AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OVERSIGHT OF THE STATE DEPARTMENT: TECHNOLOGY MODERNIZATION AND COMPUTER SECURITY

HEARING

BEFORE THE

COMMITTEE ON INTERNATIONAL RELATIONS HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JUNE 22, 2000

Serial No. 106–171

Printed for the use of the Committee on International Relations

Available via the World Wide Web: http://www.house.gov/international_relations

U.S. GOVERNMENT PRINTING OFFICE
68–288 CC WASHINGTON : 2000

COMMITTEE ON INTERNATIONAL RELATIONS

BENJAMIN A. GILMAN, New York, *Chairman*

WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
HENRY J. HYDE, Illinois
DOUG BEREUTER, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
PETER T. KING, New York
STEVE CHABOT, Ohio
MARSHALL "MARK" SANFORD, South Carolina
MATT SALMON, Arizona
AMO HOUGHTON, New York
TOM CAMPBELL, California
JOHN M. MCHUGH, New York
KEVIN BRADY, Texas
RICHARD BURR, North Carolina
PAUL E. GILLMOR, Ohio
GEORGE RADANOVICH, California
JOHN COOKSEY, Louisiana
THOMAS G. TANCREDO, Colorado

SAM GEJDENSON, Connecticut
TOM LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
MATTHEW G. MARTINEZ, California
DONALD M. PAYNE, New Jersey
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
CYNTHIA A. MCKINNEY, Georgia
ALCEE L. HASTINGS, Florida
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
JIM DAVIS, Florida
EARL POMEROY, North Dakota
WILLIAM D. DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
BARBARA LEE, California
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania

RICHARD J. GARON, *Chief of Staff*
KATHLEEN BERTELSEN MOAZED, *Democratic Chief of Staff*
KRISTIN GILLEY, *Professional Staff Member*
MARILYN C. OWEN, *Staff Associate*

CONTENTS

WITNESSES

	Page
Fernando Burbano, Chief Information Officer, U.S. Department of State	4
Jack L. Brock, Jr., Director of Government and Defense Systems, U.S. General Accounting Office	6
Mark T. Maybury, Ph.D., Executive Director, Information Technology Division, The MITRE Corporation	9
Wayne Rychak, Deputy Assistant Secretary for Diplomatic Security, U.S. Department of State	17

APPENDIX

Prepared statements:

The Honorable Benjamin A. Gilman, a Representative in Congress from New York and Chairman, Committee on International Relations	40
Fernando Burbano	43
Jack L. Brock	88
Mark T. Maybury, Ph.D	108

OVERSIGHT OF THE STATE DEPARTMENT: TECHNOLOGY MODERNIZATION AND COMPUTER SECURITY

THURSDAY, JUNE 22, 2000

HOUSE OF REPRESENTATIVES,
COMMITTEE ON INTERNATIONAL RELATIONS,
Washington, DC.

The Committee met, pursuant to notice, at 10:12 a.m. in room 2200, Rayburn House Office Building, Hon. Benjamin A. Gilman (Chairman of the Committee) presiding.

Chairman GILMAN. This meeting will come to order. I want to thank our panelists for joining us this morning and thank our colleagues for being here.

I am pleased to convene this hearing on Oversight of the State Department, Technology, Modernization and Computer Security. This is the fourth in a series of oversight hearings that this Committee will conduct relating to the Overseas Presence Advisory Panel, the OPAP.

We began these hearings back in February when we heard from the panel's members. At that time, and today, I believe the panel highlighted some very important issues. This Committee supports many of the recommendations made as a basis of maintaining a more effective and efficient State Department.

We are asking our panelists to provide the Committee with a comprehensive review of the condition of the State Department's information technology program, the safeguarding of its information and prospects of developing a common platform to facilitate communication among the agencies at posts. Along with the efficiencies of high tech systems comes a breadth of possible vulnerabilities. These systems demand continual security evaluations and resources that should be dedicated to this activity.

Personnel at the State Department must have the capacity to communicate quickly and precisely with a variety of people. The Overseas Presence Advisory Panel observed that the Department's current infrastructure does not provide the means either to acquire information from a full range of sources or to disseminate it to a full range of audiences.

Inefficient information systems leave the Department impotent in the conduct of foreign affairs. The Department and other agencies sharing the overseas platform have taken steps to bring their systems up to private sector standards, but much more is needed to be successful on an interagency basis. Our private sector pan-

elist, Mr. Maybury, will address the problems associated with that issue.

An overriding concern as modernization proceeds is to make certain that appropriate, usable systems are procured and that security elements are addressed up front. The taxpayer is providing an enormous amount of money over time for the worldwide upgrades, and this Committee needs to be assured that the right decisions and cost effective procurements are being made.

With recent cyber attacks against web sites in both Federal and congressional computer systems, serious questions arise about computer systems' vulnerabilities. Investigation of hacker assaults revealed that the techniques used over the past months were fundamentally very simple. In May 1998, GAO reported that State's computer systems were very susceptible to hackers and to unauthorized individuals.

Given the important data bases that the Department possesses, it would be a disaster if hacker penetration were to occur in the State Department; to name just a few, the passport system, the visa system, class systems. If a hacker were to succeed, it would have a devastating effect on the functioning of these items, not to mention the effect on commerce. The Department takes in an enormous amount of revenue per day on the issuance of those items.

I believe that in creating a modern infrastructure, utilizing a common platform and spending the nation's money wisely are certainly critical elements on the road to successful information technology management. We will find out today if our State Department is on the right road or if they have hit a dead end.

Now I would like to turn to our other colleagues, the Vice-Chairman of our Committee, the gentleman from Nebraska, Mr. Bereuter.

[The prepared statement of Chairman Gilman appears in the appendix.]

Mr. BEREUTER. Thank you, Mr. Chairman. I have no comment. I look forward to the testimony.

Chairman GILMAN. Judge Hastings.

Mr. HASTINGS. Mr. Chairman, I have no opening statement at this time.

Chairman GILMAN. Thank you.

Mr. Rohrabacher.

Mr. ROHRABACHER. Just a very short statement for the record. I am very concerned, Mr. Chairman, over reports that the Chin Wa news agency, a Chinese agency that has ties to the Communist Chinese government in Beijing—in fact, it is known as having an intelligence connection with the government in Beijing—has purchased a building in Arlington with the State Department—at least with no protest from the State Department, overlooking the Pentagon. This building is a 12 story building that has very serious implications to electronic intelligence operations, especially in relationship to a direct overview of the Pentagon.

I understand the State Department had no objection to this, raised no objections to the Chinese taking over this building, and I just think that there is—I do not know if this panel is the one who could explain it. Probably not, but for the record I would like to say that this is very unsettling news.

It seems to me that somebody has got to have the responsibility when things like this happen, and having an intelligence arm of the Beijing government setting up a spy nest, an electronic spy nest, you know, just in this position overseeing the Pentagon is something that deserves our attention. I thought I would put that on the record.

Chairman GILMAN. Thank you very much, Mr. Rohrabacher. I hope some panelists will comment on it as we proceed.

Today we welcome Mr. Fernando Burbano, the chief information officer of the State Department. Mr. Burbano assumed the position in May 1998, is responsible for the Department's information technology policy and operations. He oversees a budget of more than $500 million and the activities of more than 2,000 employees who are engaged in information management. He holds advanced degrees from the American University and Syracuse University.

Our second witness, Mr. Jack Brock, is director of the government wide and defense information systems in the issue area at the General Accounting Office. He is responsible for information management, evaluations and reviews of computer security issues for several agencies, including State, and he has testified several times on these issues.

The General Accounting Office [GAO] has developed guidance for improving responses to computer security threats. Thank you for putting our system back in operation. He holds advanced degrees from the University of Texas and Harvard. Welcome.

Our third witness is Dr. Mark Maybury. Welcome, Mr. Maybury, of is it MITRE Corporation?

Mr. MAYBURY. MITRE.

Chairman GILMAN. MITRE Corporation. Dr. Maybury comes to us highly recommended because of his experience in the field of worldwide system upgrades. He is the director of MITRE's information technology division responsible for the advanced research and development of intelligence and defense systems supporting several government agencies.

Dr. Maybury has taken a look at what it takes to build a common platform, collaborative computing and knowledge management within the foreign affairs community. He holds several advanced degrees, including a Ph.D. from Cambridge in artificial intelligence. We certainly appreciate his willingness to come down from Massachusetts and educate us in this highly technical field.

We appreciate all of our witnesses being here today, and we ask you to proceed with a summary of your statements. Without objection, your full statements will be made part of our record.

I also want to welcome Mr. Wayne Rychak, a Deputy Assistant Secretary in the Diplomatic Security Bureau at the State Department. He is a member of the Senior Foreign Service, and his positions with Diplomatic Security have included being regional security officer in Islamabad and Pakistan.

Mr. Rychak is here to respond to questions regarding information security.

Please proceed, Mr. Burbano.

STATEMENT OF FERNANDO BURBANO, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF STATE

Mr. BURBANO. Thank you, Mr. Chairman. Good morning, Mr. Chairman and distinguished Members of the Committee on International Relations.

As the CIO for the State Department, I am pleased to report significant progress managing the Department's information technology resources. This morning I will focus on actions we have taken to, first, strengthen our computer security; second, improve the integrity and quality of our IT strategic planning, our IT capital planning and our management of IT resources; and, third, to achieve compliance with the Overseas Presence Advisory Panel, OPAP, recommendations.

Since my testimony is limited to 5 minutes, I have provided a more detailed written report for the record.

Computer security. In the past 2 years since I was appointed CIO, the State Department has taken significant steps in strengthening our computer security and the security of our global communications networks. For example, we now have in place a corporate information system security officer and computer security incident response teams.

Our systems are protected with an extensive array of electronic firewalls, intrusion detection systems and a comprehensive antivirus program. We increased system security training, conducted extensive independent network penetration testing and installed a web based geographic information system to collect cyber threat information.

As additional examples of the Department's commitment to computer security awareness, I have hosted the CIO Council Security Awareness Day, Critical Infrastructure Protection Day and a hacker briefing presented by an industry expert. All of these are open to the entire Federal IT community.

With our improved security posture, we have successfully withstood numerous cyber attacks such as those that have damaged other agencies and private sector web sites. For example, we were successful in defending against an attack after the NATO bombing of the Chinese Embassy in Belgrade when we were bombarded with over 10,000 messages an hour for several weeks.

However, despite significant improvements in our cyber security, we realize that the cyber underworld continues to improve its weapons. We routinely assess our presence on the internet, and so far we have been successful in adjusting our protection measures to meet the continuing and ever changing challenges.

I also established a security infrastructure working group known as SIWG to proactively oversee our enterprise infrastructure and coordinate an integrated, department wide security response. The SIWG is chaired by the Deputy CIO for Operations and has representation from Diplomatic Security and other bureaus.

Let me briefly highlight our accomplishments in our IT security over the last 2 years. We achieved 100 percent completion of the 72 technical findings and the eight management recommendations identified in the 1998 GAO computer security audit. We achieved closure on Federal Managers Financial Integrity Act, FMFIA, issues open since 1984.

We revised the foreign affairs manual to include security related policies. We globally deployed a computer security self-assessment software tool known as Kane Security Analyst. We conducted vulnerability assessments on our classified, sensitive but unclassified and internet networks.

In a joint effort with the NSA, we have begun a pilot program using public key infrastructure to implement strong identification and authentication processes. We are implementing the risk management cycle as recommended in best practices published by GAO and OMB and are implementing a robust certification and accreditation program incorporating the recently released national information assurance certification and accreditation process known as NIACAP. My written testimony describes these achievements in more detail.

Now turning to Overseas Presence Advisory Panel recommendations, particularly the actions we have taken to address the challenges to obtain interagency coordination and cooperation and to insure quality and cost effective program management. To insure that all foreign affairs agencies are partners in developing solutions to the OPAP recommendations, we have convened the OPAP interagency technology subcommittee. This subcommittee, which I chair as the representative of the lead agency, consists of the CIOs of the principal foreign affairs agencies.

To date, the cooperation between all of the foreign affairs agencies in developing solutions to the OPAP report recommendations has been outstanding. This reflects the fact that over the past 2 years, through the CIO Council and its various subcommittees, the CIOs had already established strong relationships and had worked collaboratively on issues of common concern.

Specifically, we are progressing in our plans to deploy an interoperable infrastructure accessible to all agencies to improve communication and collaboration. Our OPAP architecture approach emphasizes interagency connectivity and collaboration, minimizing technical risk and leveraging internet and web technologies.

The intent is to build a browser based environment such that agencies need not change their architectures to connect to and use the OPAP facilities, and a range of connection options will be accommodated. To provide the right information to the right people at the right time, we are designing a knowledge management system to share information across agency boundaries. Security of the infrastructure will be addressed through the use of technologies such as public key infrastructure, data encryption and use of firewalls.

In order to insure quality and cost effective program management and avoid excessive cost overruns, we are following a disciplined, standard project management methodology which we have used successfully in our Y2K worldwide remediation program, IT modernization program known as ALMA and the global emergency radio deployment program. I should point out that this methodology includes regular interagency project review and approval points, such as control gates and check points, and prototype and pilot tests and assessments.

Accordingly, in fiscal year 2001, conditional on the availability of timely and adequate resources, we plan to implement a pilot pro-

gram at two posts to test the interagency developed solutions to the OPAP unclassified technology recommendations. Mexico and New Delhi are being considered as the pilot posts. Our goals and the effective participation of other Federal agencies are achievable only with your support in providing us the resources to continue.

Turning to IT management and planning, the last section, in the time remaining I will address our progress in responding to the 1998 GAO report which raised issues about our modernization program being at risk absent implementation of best practices. We have made significant improvements in the management, policy, planning and governance of our IT resources as we demonstrated in our success at turning our Y2K program from an F to an A, closing FMFIA issues and completing of a large scale, global IL modernization project.

Demonstrating the Department's compliance with the GAO's management improvements recommendations, we have adopted an enhanced capital planning process that involves all the key stakeholders, including the CFO and other senior management, Assistant Secretaries, to comply with the mandates of Clinger Cohen and OMB Circular A–11;

Created the Configuration Control Board, whose role will be expanded to further strengthen the interrelationship with the capital planning process; established the enterprise IT architecture that is modeled after guidance issued by the Federal CIO Council; included output and outcome measures in our IT tactical plan linking the relationship of those measures to mission effectiveness and efficiency;

Instituted a disciplined life cycle management process known as Managing State Projects to help insure a consistent approach to all aspects of project manager; and, last, we continued to focus on well articulated goals that are presented in our new IT strategic plan published in January of this year.

Mr. Chairman and distinguished Committee Members, I would like to conclude my testimony here today by assuring you that the State Department, including senior management, is committed to confronting the continuing challenges, including those which will cogently be addressed by GAO today.

We will work in partnership with your Committee, the GAO and other agencies and other bureaus in the Department, including Diplomatic Security, to provide exceptional IT support to American diplomatic activities in the twenty-first century.

Thank you, and I would be pleased to answer any questions.

[The prepared statement of Mr. Burbano appears in the appendix.]

Chairman GILMAN. Thank you, Mr. Burbano.

Mr. Brock, GAO.

STATEMENT OF JACK L. BROCK, JR., DIRECTOR OF GOVERNMENT AND DEFENSE SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE

Mr. BROCK. Thank you, Mr. Chairman. Thank you very much for inviting us here today.

We first met with your staff several months ago about the Overseas Presence Advisory Panel [OPAP]. The main concern was we

do not want to have a hearing in 2 or 3 years and find out that the Department has wasted $300 million or $400 million. We want a return on investment. We want to make sure that the goals and the objectives that were set out in the OPAP report are in fact and that they are met efficiently.

I think a concern that the staff had was based on a couple of GAO reports on the IT environment at the State Department and on the poor computer security, this concern was well founded. Could in fact the Department spend the money wisely? Could in fact the Department bring about the common platform that is needed to support OPAP?

Our work in computer security showed that the State Department was highly vulnerable to both inside and outside threats. We were able to pretty much walk around the Department. There was generally a lack of oversight at the management level.

Chairman GILMAN. Let me interrupt. You say there is a lack of oversight in management at State?

Mr. BROCK. Oh, absolutely. Yes.

Chairman GILMAN. Thank you. We are curious about that because we are working on the possibility of creating a new management office. Thank you.

Mr. BROCK. The same thing on looking at major investments, IT investments in the Department. There were a lack of management controls and a lack of management processes.

Both of those reports were done in 1998, and since then the Department has made impressive strides in establishing good management processes that should allow them, if implemented correctly, to control their investments, to control their computer security. I am a firm believer that good results come from good processes. If you do not have good processes, good results may or may not follow, but they are pretty much sporadic.

The Department has now laid a foundation for having a better opportunity for achieving good results, and in fact when we are looking at the OPAP project, which the early planning stages are still underway, they in fact have a disciplined process that they are following in determining what the requirements of the platform will be, how much it should cost, what sort of technology should be in place, etc. They are doing a number of things that make sense, and they are pretty much on target by the end of this fiscal year to have a detailed implementation plan.

While the Department I believe is well situated to move forward into a planning process, we believe they also face I think reasonably significant challenges in moving forward. I would like to just spend a few moments discussing those challenges.

First of all, they have to work with eight or nine agencies on this common platform, and that is difficult to do. I mean, on paper they have the agencies in place. They all meet together. They have regular meetings. Nevertheless, they have different objectives. They have different needs, and in order to optimize the common platform some of the individual needs of various agencies might have to be suboptimized.

It is this process that is difficult to negotiate and achieve. We think that it is likely that many agencies may want to continue op-

erating their own technology, particularly if they have systems that were recently acquired or upgraded.

Second, no one agency by itself has the authority or the ability to dictate a solution to insure the implementation of a mutually developed solution. Third, although negotiations are ongoing, details are still being worked out as to who will manage and administer the new collaborative network.

These challenges are answerable. They are doable, but, nevertheless, they are challenges that have to face the Department. This really has nothing to do with the Department's status now in terms of good information over technology, but I think a challenge that any organization would face trying to bring together eight other organizations.

The second challenge is on the matter of an architecture. Right now the State Department has a level of architecture, but it does not have a detailed architecture.

If I could just briefly describe an architecture in more common terms, if you have a Rand McNally atlas and you open up the front page and you see the map of the United States, it shows the major interstates going from the east coast to the west coast and from the Gulf of Mexico to Canada. Well, you sort of know how to get there and where you are going, but it is only until you turn to the detailed maps inside the atlas that you really know the best route to take from state to state to state.

I think right now the State Department has a pretty good overview map, but they do not have those detailed maps that are really necessary to dictate where the State Department wants to go in terms of matching business solutions with technology. The danger of not having an architecture in place is that sometimes you in fact let technology dictate business needs, or you let business needs dictate the wrong kind of technology, so you really need to merge those two things.

The danger of continuing or the risk of continuing in the OPAP project while the architecture is still underway is that there is a risk that the eventual OPAP architecture could influence the State Department's final architecture in a way that may not be optimal. Now, this is a risk I think they are aware of and something that they need to follow throughout the development of both the architecture and the project.

The last challenge that the State Department faces is computer security. This is a challenge that we found every agency faces. Our recent reports have indicated that the 22 major Federal agencies all have significant computer security problems. The findings that we had at State Department a couple years ago, they are not unique to the State Department. They are true everywhere on a government wide basis.

The State Department has implemented our recommendations. They have changed their management structure. They are in a better position to deal with these problems. One of the things that they have done at our recommendation is to begin to do vulnerability assessments at key places. These vulnerability assessments continue to find problems.

I think a difference now is the State Department is finding these problems, and they are fixing them, but I think it is indicative that

computer security is an ongoing concern. You are going to have a new network, a new platform, new opportunities for intrusion, and I think that the diligence and the level of effort that the State Department will have to exercise to this is going to be considerable, so that is a significant challenge.

The advantage is that you have now as an oversight body and in fact an advantage that is also shared by the State Department and the other agencies that are participating in the OPAP project is that the planning for this is just now seriously getting underway, and you have many excellent oversight opportunities over the coming year.

First of all, the State Department is developing a detailed project plan, and they are going to be testing the concept at a couple of pilot locations. This is a good opportunity to take a look at the detailed project plan, to take a look at the results of the pilot projects and say is this an investment that is going to pay off? Does it show promise? Is it something we want to pay for? Is it something that is showing results in a couple of limited locations? Does it show promise?

Second, the development of a detailed project plan also allows the performance measures to be developed so that in fact you will be able to say OK, here is where you said you would be. Here is where you are. What is the gap? What do we need to do to close the gap? Are you still on target—and gives the State Department, the other agencies, as well as you as an oversight entity, an opportunity to take corrective actions.

The State Department is well positioned to develop a plan, and I think that again this Committee is well positioned to use this plan as a vehicle for monitoring the development of the platform over the next couple of years.

Mr. Chairman, that concludes my statement.

[The prepared statement of Mr. Brock appears in the appendix.]

Chairman GILMAN. Thank you very much, Mr. Brock. You have given us a lot of food for thought.

Mr. Maybury.

STATEMENT OF MARK T. MAYBURY, EXECUTIVE DIRECTOR, INFORMATION TECHNOLOGY DIVISION, THE MITRE CORPORATION

Mr. MAYBURY. Thank you, Mr. Chairman, distinguished Members of the Committee.

As executive director for the Miter Corporation, I oversee all collaboration computing activities at the corporation, and for the past 5 years I have served and worked with the Department of Defense very closely to develop a common operating environment specifically responsible for the collaboration and multimedia elements thereof.

I will summarize my prepared statement, but I have provided a lot of details that I would like to make part of the formal record.

Chairman GILMAN. Without objection, it will be made part of the record.

Please proceed.

Mr. MAYBURY. Thank you.

Just a comment on the requirements for, the impediments to, the costs of and the lessons learned from using collaboration computing in knowledge management and other activities across the government. I have attempted to address each of these issues in detail, but I would summarize my statements.

The first point I would like to make is that to create a common operating platform for the Department of State and the other agencies is a challenge, but it has great potential. By common platform, I mean those infrastructure and applications that are basic to long distance and cross agency collaboration, things like directories, electronic mail, file sharing, desktop video teleconferencing, skills or expert data bases and shared applications.

I believe secure collaboration and knowledge management solutions have promised to directly address some of the fundamental problems outlined in the November, 1999, OPAP report, including increased global complexity, dealing with reduced overseas staffs, the need for increased global engagement and influence.

For example, if we take a look at the intelligence community and the Intelink, classified internet, which MITRE helped engineer, it has become the primary method for intelligence distribution throughout the intelligence community.

Another example. In my written statement I detail how collaborative technologies have fundamentally changed the way the Air Force operates by creating virtual air operations centers. Another example. The Navy and the Joint Forces have been able to put Tomahawk cruise missiles on target faster and more accurately during war.

At the MITRE Corporation, as I have also submitted in my materials, there are several CIO magazine articles outlining our internal internet which has been used to share knowledge globally. These systems have improved the timeliness and quality of operational processes. For example, in a major exercise last year, the Air Force was able to improve their efficiency of operations by 50 percent. With focused effort, the foreign affairs community can enjoy these same benefits.

My second point is that the success of the common platform for the Department of State will require both knowledge management and collaboration technologies. I will not detail these, but, in short, collaboration technologies are those that allow people to share information across time in both different times, as well as across different places.

For example, if you want to support a team working at a different time and a different place, you could use electronic mail, or if they are working at the same time, but in different places, you could use technologies like instant messaging, technologies like desktop video conferencing.

In contrast, knowledge management can be enabled by collaboration, but it is distinct, and it refers to processes that allow us to find experts, to map the knowledge in an enterprise or across enterprises, to integrate knowledge and to disseminate knowledge.

My third point. Because of the difficulty of predicting how people and organizations will use collaboration tools and the rapidly changing underlying communications, networking and computing

infrastructure, it is essential that the creation of these systems be done in what is called an incremental spiral acquisition process.

This is in contrast to the traditional waterfall approach where development of a system follows a strict sequential process from requirements to design to implementation to testing and in contrast is more of an iterative process in which these things are done in parallel.

Accordingly, the government needs to depart from its normal lengthy purchasing process to build a little, test a little, learn from mistakes and be willing to adapt to change. Planned obsolescence is part of this process, and these systems can be very costly. In fact, when you cost these systems you must look at full life cycle costs to include the cost to acquire the system, the cost to implement it, steady state costs, as well as indirect costs, including intangibles such as down time and user satisfaction.

Incidentally, I have included in these articles the cost analysis that MITRE has utilized that was highlighted in the February CIO article where we invested $7 million and were able to show over $50 million in return on investment.

While a spiral development process does not guarantee an inexpensive solution, it does minimize the risk that money will be wasted. Success in creating a secure common platform for the Department of State and other agencies requires clarity of vision, buy in from the foreign affairs community, explicit and measurable business outcomes, but flexibility in technology, schedule, budget and specifications.

Mr. Chairman, I have a few more points. I do not know if you would like me to stop or finish.

Chairman GILMAN. Well, we are going to be called for a vote. Why do we not dig into the questions, if you would?

Mr. MAYBURY. That is fine. Thank you.

[The prepared statement of Mr. Maybury appears in the appendix.]

Chairman GILMAN. I want to thank all of you for being concise is your presentations.

We will continue right on through the vote with the questioning. I am going to ask my colleagues if they would want to go, and we will continue so we will not have a delay.

First of all, Mr. Burbano, last week Undersecretary Cohen stated that various technology systems were still out of date, even though the Department has replaced all of its Wang systems. When can we expect the needed reorganization to be achieved that is so sorely needed? Which systems are top priority, and do we have the appropriations that are needed to do what you are seeking?

Mr. BURBANO. Mr. Chairman, the answer to that question I think goes right to the heart. It is the funding. We do not have the funding to completely overhaul the systems.

The majority of the unclassified systems have been modernized. The classified system is where we still have a lot——

Chairman GILMAN. How much will be needed, Mr. Burbano?

Mr. BURBANO. Approximately close to $200 million.

Chairman GILMAN. I understood from my staff that there is $500 million available for information technology. Is that fund available to you?

Mr. BURBANO. We are using it. I mean, it is not a fund that is available for things we have not used it for. Believe me, we are making use. Our budget is, you know, as stated earlier, $500 million.

Chairman GILMAN. So you are limited in the appropriations available to you?

Mr. BURBANO. Yes. Absolutely.

Chairman GILMAN. And what is the shortage?

Mr. BURBANO. For the classified systems, close to $200 million.

Chairman GILMAN. You need another $200 million?

Mr. BURBANO. Yes.

Chairman GILMAN. Mr. Brock, your statement noted the State Department networks remain highly vulnerable to exploitation of unauthorized access. That is based on four computer security evaluations of its unclassified networks.

What do these findings suggest for efforts to develop a common platform? Both Mr. Brock and Mr. Burbano, has any corrective action been taken? Have such risk assessments been made on the classified system? I direct that to both of you. Mr. Brock?

Mr. BROCK. First, I do not think that it is unusual that every time you do one of these vulnerability tests that you continue to find holes. One of the reasons that we advocate a continuing of vulnerability assessment is in fact to find holes because they always creep up. If you are not constantly vigilant, you will end up with a serious mess on your hands.

We did not go in and evaluate the repairs that the State Department made. We did note that they did take corrective action in the four reports that we examined. The fact that reports, though, continue to show vulnerabilities, which again I do not find particularly surprising, indicates that there is still a need for constant vigilance.

The thing the Department has done differently since our original report, though, is put in more centralized management and in fact established a control. Before our initial report they never did their own vulnerability studies. At least now they have the capability of determining on their own where they have weaknesses and then being able to take corrective action on a more timely basis.

But again, that just points out that when you are putting in a new platform, as I mentioned in my oral statement, that in fact you are assuming a certain risk. You need to determine what that risk is. You need to determine the appropriate controls that should be in place to minimize that risk, and those controls are going to cost you some money. That has to be factored into the life cycle cost of the overall project.

Chairman GILMAN. Mr. Brock, you noted that the panel reported the condition of U.S. post submissions abroad as unacceptable, and the panel found the facilities overseas had deteriorated, human resource management practices are outdated and inefficient, and there is no interagency mechanism to coordinate overseas activities or manage their size and shape. What is your recommendation to correct that?

Mr. BROCK. Well, we did not specifically go over and evaluate those conditions, so we have made a general assumption based on

other material that those conditions were reasonably and accurately reported.

In fact, the process that the State Department is leading now is supposed to address those conditions and make improvements, which is one of the challenges that we mentioned. In fact, to get all eight or nine agencies to agree to make certain changes is going to be a difficult task.

Chairman GILMAN. I am going to reserve my questions. Mr. Bereuter has another engagement. I am going to pass the time to Mr. Bereuter.

Mr. BEREUTER [presiding]. Thank you, Mr. Chairman. I appreciate that courtesy.

One of the difficulties for some of us is that you gentlemen use terminology which is not always clear to us, and I am sure we do the same, but, as I understand it, you are preparing or are you updating information architecture, a plan for information architecture for the State Department.

Is it an update would you say realistically, or is it the first time you are comprehensively attempting to look at and develop an architecture? Mr. Burbano.

Mr. BURBANO. We have developed already, as in a written testimony in April 1999. We put out our first high level, as Mr. Brock stated. It is high level architecture that brings the State Department into the modern age, and we are developing right now the details of that IT architecture, so we came out with the first published IT architecture.

There was a default one, you know, because you always operate with one, but it was not necessarily a formally published architecture prior to that one.

Mr. BEREUTER. Mr. Burbano, you heard the analogy used by Mr. Brock about the Rand McNally overall front page map, and he suggested that what is lacking to some extent——

Mr. BURBANO. Is the details.

Mr. BEREUTER [continuing]. Are the details within that overall framework.

You have a good framework in place, as I understand your comment, Mr. Brock.

How far do you intend to go in Mexico City, and where is the other pilot?

Mr. BURBANO. New Delhi.

Mr. BEREUTER. New Delhi. Are these picked because you think that they will be good models for you to work with, to make an assessment on?

Mr. BURBANO. Yes. In fact, you know, those models were picked with the whole interagency group; not just the IT interagency group, but the interagency group for OPAP that is overlooking the right sizing and the buildings/ facilities and the IT portion, the three groups underneath that. They are the ones that decided along with the three groups underneath that those were the best sites.

The reason they are the best sites is because of the representation there from the other agencies, which is what you want to do for the collaboration.

Mr. BEREUTER. Now, what I am looking for is some reassurance that the plan that you are developing or refining for the information technology for the State Department will survive changes in technology.

Mr. BURBANO. Yes, it will, and that is one of the key points. It is a refresh. We are doing that right now with our very successful ALMA program, which is another logical modernization program that we have that replaced all these Wangs on the unclassified system. That was very successful.

We have a refresh program, which is part of our Managing State Project management system that Mr. Brock spoke about that has been successful, and that includes a refresh to make sure we stay up to date. We are doing that right now with the ALMA system, and we did that also with the very successful Y2K system and also with the global overseas radio program.

Mr. BEREUTER. Thank you very much.

Mr. Brock, I want to have some assurance that what is being developed in fact will survive upgraded technological changes that are brought to bear in terms of new equipment, new software, things that perhaps we do not even anticipate at this point.

I want to understand that this plan is going to be survivable, that it will be credible, that it will reach beyond the current technology and that we will not find ourselves having to start all over picking up the pieces as a result of changes in technology.

Do you have anything you can say to me about the plan as being developed?

Mr. BROCK. Well, I cannot offer you those assurances because the plan is not complete, but what you have really done is laid out a very basic expectation that is true of any architecture. That is one of the very first things that you need to do is to use this to provide some assurance that the dollars you are going to be spending are in fact not going to be wasted.

The disadvantage of not having an architecture is that every investment that you make may or may not fit into the overall structure, so you have incompatible systems. You have—in other words, they do not talk to each other. You know, you buy Macs one place and PCs another place, and you cannot exchange software.

We have numerous examples of where a lack of a defined architecture has caused agencies billions of dollars in wasted money, so I think the answer to your question, and I apologize for going on, is that right now I cannot provide you that assurance. I can provide you an assurance that they do have a high level architecture that makes sense.

They are developing the necessary artifacts, the individual Rand McNally pieces, and those need to be examined as we go through the process to see if in fact they will provide that richness that you are asking for.

Mr. BEREUTER. I will just make one more statement really before I turn it over to Mr. Rohrabacher as I go to vote.

I understand how difficult—I think I understand in part how difficult this interagency process might be to develop an agreement as to what is appropriate in taking secondary levels of benefits perhaps in order for the uniform effort to move ahead.

I believe I understand that the intelligence community and the State Department have just basically decided they cannot be as compatible as the Congress had hoped they would be and that there is something in an appropriation bill, in an intelligence authorization bill, which suggests that that is the case, so I hope perhaps you might be able to address that in your comments for the record here. If I have given you enough information to proceed, I am asking any of you after I leave.

Mr. Rohrabacher, are you ready to take over?

Mr. ROHRABACHER [presiding]. Thank you.

Mr. BEREUTER. Thank you.

Mr. ROHRABACHER. Oh-oh. I am in charge now.

Doug, you left a question on the table?

Mr. BEREUTER. If they care to address it.

Mr. ROHRABACHER. Please feel free.

Mr. MAYBURY. Yes. I would like to address that. The intelligence community is part of my IT subcommittee, interagency subcommittee. John Dams, who is the IC CIO for all the intelligence community, is a member, and he also has representation in the other groups.

As far as I have seen directly, along with my other two subgroups, there has been excellent cooperation. There is buy in. The only statements that I have personally heard and also my group leaders has been that, you know, you have to make sure that we do not lower our security standards, which I totally agree, and nobody has said that we are going to lower them.

In fact, the opposite. We are upping our security requirements because we know that the internet, you know, has holes like Swiss cheese, so we want to make sure that we strengthen our security. We are doing that, as I stated in my oral and written statements.

You know, we are going to be using industrial strength firewalls, PKI, digital certificate and signatures and also encryption, anti-viruses, every available tool that is out there to properly do and transact business on the internet in a secure manner.

As far as my relationships, and I am also a member, by the way, of the intelligence community CIO Council. I sit on the executive council. I work closely with John Dams, and as far as I know the intelligence community is, you know, on board with us. I have talked to John. As I mentioned, he is the representative for the intelligence community, and he is on board.

Mr. RYCHAK. May I add to that?

Mr. ROHRABACHER. Yes. Sure.

Mr. RYCHAK. I think it is also important that we make the distinction between our classified systems and the interconnectivity, the proposal to interconnect classified, and what is being done right now, and that is looking at our unclassified systems and interconnecting with the other agencies.

Certainly the classified interconnectivity is a goal, but that is much longer term, and indeed there are some strong opinions as to how that could be done securely in the long run bringing in agencies that have very different backgrounds and sensitivities as it relates to information. The effort, though, that is ongoing right now deals with unclassified systems.

Mr. MAYBURY. If I could make a comment? Two comments. One on the architecture point and one on the interoperability point.

In my written statement with respect to the Department of Defense, we have been working for the past 5 years with many architectures, and I would strongly urge that there not be one architecture; there be several architectures that are tightly coupled.

Just as you would not use the same map for a pilot as you would for somebody who is driving a truck as you would for somebody who is walking through a historic district in a city, you similarly will not use the same architecture in an information system for people who have different tasks or who are looking at different levels.

To be specific, it is important to have a functional architecture, what you want to do with the system; a systems architecture, what are the components, what are the connections; and a technical architecture, that is one that specifies the standards, if you will, the rules of the road that show how these systems are going to work with one another. If you only have one of those, you have an incomplete architecture.

With respect to technical standards, I have included in my written testimony the standards we use, which are international standards. They are not government standards. They are standards such as the International Telephony Union, such as the Engineering Task Force. These are standards bodies that build or, if you will, that specify the building codes to which commercial tools are created.

It is essential that we have standards in interoperability that comes from those because if we want to protect ourselves from our investment and to insure interoperability in the future, those kinds of, if you will, building codes will help us do that.

Mr. BURBANO. If I can, I would like to add a point to that since the architecture is a very key point.

To show you how committed and a firm believer I am in the architecture, we have actually gone beyond the Clinger Cohen requirements for IT architecture. We have also developed a business architecture and a security architecture, which will be a requirement in the near future, which is not a requirement right now, and we have those in draft. We are working with GAO on that.

In terms of the collaboration, I would just like to say, because that was an issue that was brought out also in an earlier question. As I stated, because of Clinger Cohen I think that the OPAP implementation is going to be a lot easier than prior to Clinger Cohen because there is now a CIO Council, and the CIOs of the top 24 and also the other 50 CIOs or so of the small and medium agencies get together on a monthly/quarterly basis.

That has produced a very strong collaboration that will spill over and is spilling over to the OPAP. That would not have existed prior to the Clinger Cohen, so I think we have excellent collaboration.

Mr. ROHRABACHER. Thank you very much.

The Chairman is back, but I will, with the Chairman's permission, proceed with my 5 minutes.

Chairman GILMAN [presiding]. Please. Please.

Mr. ROHRABACHER. Which I have not had yet.

Chairman GILMAN. By all means.

Mr. ROHRABACHER. Let me just say, first of all, I stated something for the record at the beginning, and I just want to followup on that 1 minute, but let me just say that from my perspective it seems like we are starting this effort that you are talking about really late in the game here. This is near the end of this Administration, and all of a sudden we are talking about security.

Quite frankly, Mr. Chairman, this Administration does not have a very good track record in terms of security in the operations of our Federal agencies. One need only look at the ongoing crisis, for lack of a better word, surrounding Los Alamos and what has been going on there for what appears to have been going on for years and years and years. I realize you folks are not responsible for that. Maybe you will have some responsibility for that or parts of that. I do not know.

Then we hear stories about missing laptops. Now, where does this missing—I mean, I understand there is at least one missing laptop that dealt with top secret security information. Where does that fit into what you are doing here?

STATEMENT OF WAYNE RYCHAK, DEPUTY ASSISTANT SECRETARY FOR DIPLOMATIC SECURITY, U.S. DEPARTMENT OF STATE

Mr. RYCHAK. Sir, to answer your first question, security is not a new issue. The comments that Mr. Brock made regarding the improvements, and there have been substantial improvements within the information and security program at the State Department. Those have been occurring over the course of the last 3 years.

When the GAO issued their report in the fall of 1998, frankly it was a wake up call for many of us that are in the operational side. We have focused great effort and attention in enhancing processes, as Mr. Brock has pointed out; processes such as security awareness training, vulnerability and risk assessments, evaluations, audits, network monitoring.

Mr. ROHRABACHER. Let me interrupt you for one moment.

Mr. RYCHAK. Yes.

Mr. ROHRABACHER. And I respect all the procedural things and the descriptions of the type of—I mean, you are going through this in a systematic way and saying how can we make things better in relationship to a GAO report.

It is difficult for me to understand how to instill a security consciousness among professionals like we have at the State Department who work for the government when we have an administration that is claiming that America's most severe potential enemy, America's worst potential enemy, is a strategic partner.

I mean, for 2 years, for 3 years, we had the State Department over here, of course, doing what they were told to do because the President of the United States was making the policy that the Communist Chinese should be referred to and the operating words were strategic partner.

It is difficult for me, frankly, to sit and to listen to a very serious discussion, which you are having here, about your procedures when it is done under an umbrella of or an atmosphere that is being created by an administration insisting on calling our worst potential

enemy a partner, and not only just a partner, but a strategic partner.

Now, I am not going to ask you to attack the Administration because you would not be diplomats if you did, but I just wanted to note that for the record.

Let's go back. Let me go back to that first issue that I raised in my opening statement. Here we have, and I think rational people have to—I think rational people all along understood that Communist China was not our strategic partner, but was instead a potential enemy. I am not saying that they are an enemy, but at least our worst potential adversary.

Here we have what almost everyone recognizes as our most dangerous potential adversary buying a building right across from the Pentagon with obvious electronic capability, spying capabilities. Has there been any discussion? There was no apparent objection from the State Department, which would have had some say in this.

Have there been discussions with the Defense Department or the CIA concerning this potential security problem?

Mr. RYCHAK. Sir, when you first raised this question you surmised that there would probably be no one on this panel that could directly answer, and you are correct.

I will tell you that the Department's Office of Foreign Missions would be the entity that would normally deal with these types of issues, any acquisitions by foreign governments of property. I am sure that this office was involved.

I cannot speak of any of the details. I learned of this, as you did, this morning on the news. We would have to get back to you on your question.

Mr. ROHRABACHER. But would it be the FBI would then be in touch with the State Department, who would then do something official in terms of looking into that to see if the charges that this was an arm of Chinese intelligence and if it was to make the appropriate moves to prevent this from happening?

Mr. RYCHAK. It is normally——

Mr. ROHRABACHER. Is that the way it would work?

Mr. RYCHAK [continuing]. FBI, State Department and then the intelligence community. It is normally a coordinated effort to look at the potential hazards and threats that could be posed by a foreign government's presence anywhere in the United States.

Again, I cannot speak to any of the details, though, on this particular issue.

Mr. ROHRABACHER. And your role that we were talking about earlier is that when the agencies get together and they want to communicate via their computer system that you are just trying to see now that the computer system—someone does not hack into that or that that is a protected communications apparatus? Is that right?

Mr. RYCHAK. Yes. Certainly one of my roles is to do what is necessary to put into place a comprehensive and effective security program to protect that information. Yes.

Mr. MAYBURY. If I could make a comment on that?

Mr. ROHRABACHER. Sure. Go right ahead.

Mr. MAYBURY. With respect to there are a whole set of vulnerabilities that I know the State Department is aware of and they have been actively addressing via a variety of mechanisms, such as access by unauthorized users, denial of service and so on.

I think that it is important to note particularly when we talk about distributed collaboration systems that there are new classes of vulnerability that are inserted or potentially there. In fact, we are actively working with, and I cannot speak to this in this open session, but with government agencies to develop new technologies to apply to essentially protect some of these systems.

For example, one might want to have if you are communicating instead of over a phone using a computer to communicate, you may want to encrypt that kind of audio, for example. These are new functions that will be made available in the future, but we do not have them yet. There are new vulnerabilities that we do not yet have protection for that we need to either invest in or create.

Mr. ROHRABACHER. Well, I am pleased to see that we have some people who understand all of this computer. We were just discussing this. Congressman Hastings and I were discussing that we are not experts, unlike Ben, who understands all of the new computer system and the new technology. We are very happy that we have some real professionals who are involved in this, and we thank you, Mr. Maybury, and you gentlemen for spending your time and your professional expertise in this.

Just again for the record, I would like to say just again I am not doing this to be political, Al, but I just think the record of this Administration in this area has been—I worked for the White House for 7 years, and I remember what it was like, the atmosphere in the Reagan Administration concerning security issues, and the record of this Administration when you consider Los Alamos and some of these other things that we know about has just been abysmal.

This Administration should hang its head in shame in terms of the national security interests of our country in terms of this area. I am pleased, however, at this part of the game and that some professional attention is being spent in this area.

Thank you very much, Mr. Chairman.

Chairman GILMAN. Thank you, Mr. Rohrabacher.

Judge Hastings.

Mr. HASTINGS. Mr. Chairman, thank you so very much. My dear and good friend from California would not dare do anything political, nor would I.

Under the circumstances, I remind him that when he worked at the White House in the Reagan Administration a call on a cell would have been from a jail. The IBM machine was considered something forward thinking, and everybody thought they had arrived. Indeed, most of what you were doing was using dictating machines.

The problem that I have is that it seems that the technology is overwhelming, and I see that as problematical for not only our governmental agencies, but for all of us until we reach whatever the optimum condition is that it is likely to reach, and the way it is spiraling that is hard to envision taking place at some point in the not too distant future.

I would like to ask two quick questions, and then I would like to just, if I could, give you an overview of what I just said with more specifics in mind.

Mr. Burbano or Mr. Rychak, has the Diplomatic Telecommunications Services, which you know is an interagency common platform for secure communications, been a wise and effective investment from an electronic communications perspective, and how crucial do you feel the continued operation of DTS–PO as an interagency run common system to be for the success of a common computer system? Either of you.

Mr. BURBANO. OK. I will take first a first stab at it. DTS–PO, which you are speaking to, I think is important, and I think the collaboration among the agencies in the support of it is important.

I think the problems have definitely been there due to not the organization, but funding. Frankly, it has been severely underfunded, and what has resulted, the biggest problem is the lack of band width to support the overseas community. That is funds, so it is a funding problem, but we need to maintain the organization, and it needs to be, you know, collaboration between parent companies.

Mr. HASTINGS. All right. Thank you. Some years ago I had the good experience of visiting Australia for the first time, and I use this as just a metaphor, so to speak, for what I am about to suggest or ask.

I did not know the fierce rivalry between Melbourne and Sydney. Apparently at one point they disliked each other so intensively that when they were building their rail systems, they built them in a manner that when they came together they did not fit.

I am curious from your perspective whether or not we are involving enough people when we talk about collaborative networks, collaborative technology, interagency connectivity, and by that I meant this. I served in the judiciary, and we always were last to get stuff that was needed, yet we were involved in matters of security far beyond some of the things that I see here in the legislative branch.

My concern is that at some point there has to be not just for the State Department or the CIA or the FBI or the Defense Department, but there has to be some collaboration with all of them, including the legislative, executive and judicial branches of our government, and calling upon experts from each of those areas to work with the people that are developing it. In other words, the State Department may fool around and develop the best, and GAO may not have that. We have seen that happen over and over again.

Do any of you have that concern, or if I am talking about breadth as it pertains to security including all of government is that too much to ask?

Mr. BROCK. No, it is not. It gets back to a question Mr. Rohrabacher was going into.

We have testified many times over the past year. The government has overall very poor computer security. There is no central leadership or management or limited central leadership and management. Some of the things that you are talking about such as the building overlooking the Pentagon going to threat assessment, the

United States is not well equipped to do threat assessment. Information is not shared freely among agencies.

The "I LOVE YOU" virus, which the State Department was internally successful at resisting, was not successfully resisted by many other agencies. The National Infrastructure Protection Agency at FBI did a very poor job of sharing information on the virus and coming up with relevant information.

Earlier this year, the President released the national plan to protect the critical infrastructure. The key element of that plan was to say that the government will be a model so that the private sector will want to participate, and they acknowledge in that that the government is not a model; that there is a long way to go.

So the issues you are talking about are much broader than the State Department.

Mr. HASTINGS. Right.

Mr. BROCK. They do encompass other agencies, and they need to be looked at as part of a whole cloth.

Mr. HASTINGS. Right. The other thing, Mr. Chairman, that I raise, and this will be my final question on this round, has to do with what I think is just good sense, and that is that, for example, on the criminal side of matters totally unrelated to the State Department.

When a 17-year-old hacker is discovered that is brilliant and they take him to court, a lot of times they give him a job—do you understand what I am saying—so they can decide to use this kid. Now, that raises the question that I have.

I listened to you all this morning, and just generally everyone that I have heard, from encryption all the way back across to all of the agencies that I have been faced with in my responsibilities as a policymaker, I have heard over and over and over from extraordinarily competent individuals like yourselves, and I do not mean that patronizingly. I do not know what either of you make. I suspect from my point of view you are underpaid by comparison to what happens in Silicon Valley and other places.

I guess, Mr. Burbano, since you have the highest budget as I heard the Chair announce, do you feel that in an effort to accomplish just inside your agency the things that you need to accomplish that you would—a special category of funding to give to exceptional individuals to keep them on board or to bring in bright people? Would that be helpful?

In other words, you have a GS whatever—I never have known; GS–14, GS–15—when you need to be paying somebody $200,000 to do what needs to be done. Am I off the mark here?

Mr. BURBANO. No. No. You are right on target. In fact, one of the things that I addressed besides computer security and Y2K was the work force issue was a priority of mine, and that was in fact what you were saying. Not only to recruit, but also train and also retain——

Mr. HASTINGS. Retain.

Mr. BURBANO [continuing]. IT workers in security and all the other areas.

What we in fact have done as a first step—I call it a first step because we need long term steps. We created the first agency in the Federal Government to create both a recruitment and retention

allowance and bonus program, so for recruitment we have up to 25 percent recruitment bonus, and also we worked out with OPM so we can bring them in at higher grades and steps than normal, so that is on the recruitment end.

On the training, we have added up to around $4 million extra to train our new employees, and to retain them we were certainly the first agency to come up with what we call retention allowance based on certifications like Microsoft, Oracle, Sysco, and also on, you know, whether you have a Bachelor's in Electronic Engineering or Master's in Computer Science and so forth. You can get up to 15 percent in retention pay, so we can keep those employees and not just bring them in the pipeline.

We have done that. What still needs to be done, though, for the long term is we are still working with the ceiling, so you are very right. What we need to do, and the CIO Council and the State Department is working with the CIO Council to try to create a new IT pay scale across the whole Federal Government, not just State Department, that will be competitive with private industry.

The National Academy for Public Administration [NAPA], has actually been chartered to do that study, which as you well know was chartered by Congress and is independent of the executive branch, is doing a study at the request of CIO Council and working with the CIO Council and OPM to look at the IT pay scale.

Mr. HASTINGS. Well, I thank you all, and I thank you, Mr. Chairman.

Mr. MAYBURY. Could I add a comment to that if it were useful? Just some facts for the record again in industry perspective.

Seven out of the top ten fastest growth, according to the Department of Labor statistics, job categories are information technology job categories. Several years ago that was only about two or three. The average annual attrition rate of IT professionals in this country is roughly 14½ percent.

Mr. HASTINGS. Would you say that again?

Mr. MAYBURY. Fourteen and a half percent is roughly the average turnover rate nationally in terms of——

Mr. ROHRABACHER. Per year?

Mr. MAYBURY. Per year. That means if you have 10 employees, all right, 1.4 of them will leave every year.

Fifty thousand new graduates, both undergraduate and graduates, according to Education's statistics, will graduate every year. The annual growth rate in the IT industry is about 130,000 jobs added every year. So you do the math, and, yes, there are the disciplines that people can come from, but there are not that many. You do the math, and there is a huge shortfall.

We have been tracking this actually very closely in Defense obviously in the private sector, and I strongly concur with the activities that State and others have been doing in this area, and it will only get worse.

Mr. HASTINGS. Thank you very much.

Chairman GILMAN. Thank you, Judge Hastings.

Gentlemen, I have a few questions. Mr. Rohrabacher, if you have any additional questions.

Dr. Maybury.

Mr. MAYBURY. Yes, sir?

Chairman GILMAN. Your statement addresses the recommendation that State and the embassies have greater internet access, acknowledging the expansion of the internet can provide more pathways for intruders.

How does one balance the need for a safe and secure system and yet greater access to the internet?

Mr. MAYBURY. Well, I think one needs to do a business case analysis and to sort of have a managed approach to security. One needs to understand the risks and the vulnerabilities within those systems and then come up with a very specific understanding of what the costs, either those that are financial, national security or potential human life loss if it is a rather serious set of information, and one has to measure the associated reactions or preparations one can engage in to respond to those.

In my testimony I give some specific examples of particular approaches, some of which State has already employed, to address those vulnerabilities.

Chairman GILMAN. So what you are saying is you can make any system secure. It is just how much you are willing to pay for it. Is that right?

Mr. MAYBURY. Well, I want to be careful because, you know, there is no absolute security. Security includes personnel security, physical security, as well as electronic digital security.

There are areas where we simply today do not have answers because, as I mentioned before, there are new technologies, new functions, including new vulnerabilities that are introduced into the infrastructure every day.

What that means is if the risk is constantly changing, you have to be vigilant. You have to have a process that continually looks at those literally on a daily basis and comes up with corrective technologies, procedures, policies to address them.

Chairman GILMAN. Mr. Brock, in examining security aspects of all of this, is State Department doing something about making security a priority amongst its personnel?

Mr. BROCK. I think the State Department has made it a priority, but I think, as Dr. Maybury was alluding to, it has to be ongoing. It has to be constant.

If I could just add a bit to his response? Most of the problems that we see on computer security when you are doing the tradeoffs between security and how much you want to spend is based on the absence of any sort of risk assessment; that you should not establish controls until you know what your risk is, and risk is a function of the threat and of the vulnerability of the system. So if you had a system with very limited threat and not very vulnerable, you do not need to spend much on control.

Chairman GILMAN. Who at State has the authority or the oversight on risk assessment?

Mr. BROCK. That would be Mr. Burbano.

Chairman GILMAN. Mr. Burbano, is someone doing the risk assessment?

Mr. BURBANO. Yes. In fact, it is a joint effort with my colleague, Wayne, in Diplomatic Security.

We have established a very strong program. As an example, when I first came on board I worked with the Assistant Secretary

for Diplomatic Security to bring in the first outside penetration testing, Lawrence Livermore, NR systems or unclassified systems.

Since then we have done about three or four other penetration tests on not only the unclassified, but the sensitive but unclassified, classified systems. DS has done those.

We also brought in Secure Computing Corporation to do penetration tests prior to the Y2K rollover when it was predicted there were going to be hundreds and thousands of hackers out there. We did that in November.

We not only do the penetration vulnerable assessments and the risk management, but, more importantly, we do the remediations and make sure that whatever was found as holes that they are plugged up. As was stated earlier, you are always going to find holes, but we keep on plugging them. I feel we have done an excellent job of that.

Not only have we done penetration tests, but we have also, as Mr. Rychak has stated, we have done an excellent outreach training program to make sure that the employees are cognizant of that such as I stated earlier with the Security Awareness Day, Critical Infrastructure Day, Hacker Day and individual training sections.

You cannot log on to the internet without getting some DS training. You have to be certified to get that training for the internet in order to log on to our RICH internet access system. We have implemented the intrusion detection boxes, anti-viruses. You know, I can go on and on.

Chairman GILMAN. I am trying to understand, gentlemen, the division responsibility for computer security matters between DS and the CIO shop. Can you explain the division and why it makes sense?

Mr. Rychak, do you have any special concerns about the splintering of responsibilities between the Diplomatic Security office and the chief information officer?

Mr. RYCHAK. Sir, I would be happy to give you a background as it relates to the split of responsibilities.

There are—there have been—overlapping authorities. The Diplomatic Security Act, going back to 1985, vested the Bureau of Diplomatic Security with a broad range of responsibilities. The Clinger Cohen Act and other Acts vest the CIO also with a broad range of security responsibilities as it relates to information and computer systems.

Beginning about 2 years ago, the CIO's office, NDS, worked to identify the strengths and the operational capabilities of each of our organizations so that we could put together a clear delineation of roles, of responsibilities.

Chairman GILMAN. Are you satisfied with that delineation today?

Mr. RYCHAK. The delineation I think is working well. Mr. Burbano and I may have some differences in opinions ultimately in perhaps who should be the senior lead authority, but let me say that that decision has been made. Our Undersecretary for Management has made the decision that the CIO is the lead authority for that.

You are aware that the Secretary has proposed the creation of an Undersecretary for Security in an effort to further consolidate and establish senior level accountability for security.

Computer security/information security I think will be reviewed in that context, and I do not know how that will come out, but I have to say that the system is working I think quite well, and it is collegial. It has been a partnership arrangement between the CIO and DS.

Chairman GILMAN. Let me interrupt you a moment.

Mr. RYCHAK. Yes.

Chairman GILMAN. Between the two of you, who is responsible for the maintenance and computer security at the overseas posts and at main State office? Can you tell us? Between the two shops, how much money does State spend for security, and is there money dedicated to security for the information technology fund?

Mr. RYCHAK. I can speak for my side. For the programs that DS administers, we are expending roughly $11.2 million this fiscal year for computer security related programs, and that deals with security awareness and training and vulnerability assessments, intrusion detection capabilities, and this is a program, frankly, we are very excited about that we are in the process of implementing on a global perspective.

That is one piece of the puzzle. There are other programs that the CIO and IRM administer, and I am sure Fernando would like to address it, everything from virus protection to implementing these policies, etc.

Mr. BURBANO. Yes. I think one easy way at a high level to differentiate DS and IRM is DS is involved in the development of policy and also in the evaluations, assessments and so forth. IRM is involved, the CIO, in the implementation of that policy and so, I mean, that is one high level way of looking at that.

Chairman GILMAN. Are you pretty much both working collaboratively in main State and overseas?

Mr. BURBANO. Yes. Absolutely. I would like to reinforce what Mr. Rychak said. We have an excellent relationship. We work together. We created the matrix, and ever since we have had that I think things have gone very smoothly, and in fact we understand each other's areas, and we collaborate on all decisions.

Chairman GILMAN. Mr. Burbano, Mr. Brock's report at GAO pointed out that computer security lacks a focal point within State to oversee and to coordinate its security activities.

Do you have the expertise available in your shop to manage the responsibility for computer security?

Mr. BURBANO. Yes, and in fact I think that was May, 1998. We are in 2000, and that has changed over the last year so that is no longer—I think Mr. Brock stated that that in fact was true when they did the assessment, but that was 2 years ago. That is not——

Chairman GILMAN. You have dedicated security——

Mr. BURBANO. Yes. Absolutely.

Chairman GILMAN [continuing]. Personnel.

Mr. BURBANO. We have computer incident response teams just like DS has that works around the clock, 7 by 24, in not only monitoring, but also in——

Chairman GILMAN. So it is not left up to non-professionals?

Mr. BURBANO. No. No. These are computers that carry specialists that are dedicated and trained in the field just like DS. DS and

IRM and the CIO both have computer security staffs that are professionals.

Chairman GILMAN. Mr. Burbano, I understand Diplomatic Security sends out teams to audit security of computer systems at the various posts overseas, and they produce reports and recommendations.

Who is responsible for seeing that any recommendations are carried out? Does Washington followup on those reports or supply technical experts if a post requests assistance to make a proper review?

Mr. BURBANO. Yes. IRM is responsible, along with the post and the bureaus, in implementing those changes because the posts are underneath the bureaus. So it is a joint effort, but the responsibility for implementing those recommendations do fall to IRM and the bureaus and the posts, and we do implement the changes.

We work very closely together on these teams. In fact, we send out IRM computer security specialists along with DS on some of these assessments.

Chairman GILMAN. Mr. Brock, how would you characterize the effectiveness and the improvements that State has made in their computer security program today as compared to 2 years ago? Do you have any plans to reexamine the Department's security program?

Mr. BROCK. We believe that the organizational changes that have been made are very positive, and one of the key concerns that we had was the bifurcation of computer security responsibilities throughout the Department.

When we have gone out and done our best practices work, even in highly decentralized organizations computer security was centralized. I think it is appropriate in an organization like State that you may have multiple entities carry out tasks, but it is clear that one person or one organization needs to be overall responsible, and that is something that we would like to continue to examine within the State Department.

Chairman GILMAN. Do you have any recommendations with regard to that?

Mr. BROCK. Well, at the present time, no. We currently are engaged in a number of agency reviews, and we do not have a request, if this is what you are moving toward. We have not had a request to go back in and do a thorough computer security review of the State Department.

Chairman GILMAN. Mr. Rychak or Mr. Burbano, who is responsible for investigating computer security violations, and who resolves the intrusions or attacks in the Department? Who conducts the followup?

Mr. RYCHAK. I can address that. The response to an incident actually takes two different forms. DS has what is called a CIRT, a computer incident response team. It is a 24 hour operation of personnel, largely investigative, that would respond from an investigative standpoint.

In sync with that, the CIO has a CERT, a computer emergency response team, that deals with the operational issues relating to mitigating any problems that would develop in our system.

Chairman GILMAN. Are they able to react very promptly to those?

Mr. RYCHAK. Yes. Actually, those terms work together and often do it jointly.

Mr. BURBANO. If I can add, during the Y2K rollover we had our two teams sitting together in the same room sharing the monitors, sharing the times and everything, and it worked extremely well. We were not hacked during the Y2K rollover.

Chairman GILMAN. Mr. Burbano, is computer security training mandatory at State——

Mr. BURBANO. Yes, it is mandatory.

Chairman GILMAN [continuing]. For all State employees?

Mr. BURBANO. For all State employees, and that is not just recent. As I mentioned earlier, in order to connect to the RICH internet access system you have to have DS, you know, training, and you have to get certified first before you can log on.

Chairman GILMAN. How long a period of training is there? How extensive is it?

Mr. BURBANO. We have various levels. Since DS does them, I will let Wayne talk about it.

Mr. RYCHAK. Well, the internet training is a briefing that would last maybe an hour, an hour and a half. It presumes that the employee already has the background of security procedures and requirements.

There is a new training program that was begun about 18 months ago that was the result of the GAO audit that I would just like to comment on, and that was training for our information systems security officers. We did not have a program in place prior to 18 months ago to train the people who worked on a day to day basis to insure that computer security policies were being carried out.

We did put that program into effect. We have trained hundreds and hundreds of personnel. It has gotten excellent reviews. We have more senior level training that also is available to these personnel, and——

Chairman GILMAN. Mr. Rychak, are you satisfied that all of the important employees that use secure computers have been properly trained now?

Mr. RYCHAK. No, I cannot say that I am completely satisfied. You may recall that the Secretary of State announced a directive following the discovery of the laptop computer that it would be mandatory for all employees of the Department of State, all cleared employees, to annually receive a briefing.

We are in the process of a very intensive effort to do just that, and every day that goes by we have formal briefing sessions that are ongoing in our auditoriums at the Department.

Chairman GILMAN. How extensive has this program been, and how many have been brought in at this point? What percentage of the employees?

Mr. RYCHAK. Sir, I think we are somewhere in the neighborhood of 8,000. Now, that is not addressing our overseas operations, which are being done individually by our professional regional security officers.

Chairman GILMAN. So what percentage of people who should be brought in have already been brought into your briefing session?

Mr. RYCHAK. On the latest exercise since the Secretary's directive, I would say we are probably at about 30 or 40 percent with the goal of completing this by the end of August or first of September. In other words, 100 percent.

We are taking a role and roster of everyone that receives the briefings, and we will be able to identify anyone that has not. It is again a firm directive of the Secretary that this be done.

Chairman GILMAN. Dr. Maybury and Mr. Brock, does the Federal Government need a Federal chief information officer?

Mr. BROCK. Yes. When the Clinger Cohen bill was first introduced, it really established the framework for management of information technology from the agencies. At that time we testified that a national CIO was needed to in fact identify both opportunities and challenges across government that needed to be explored in a collegial manner, and we still support that position.

Chairman GILMAN. Have there been any steps undertaken to do just that?

Mr. BROCK. Yesterday I read an article that apparently both Mr. Gore and Mr. Bush support a national CIO, and one of your colleagues, Mr. Turner, has introduced legislation calling for a national CIO.

Chairman GILMAN. Mr. Burbano or Mr. Rychak, have you seen any progress made with regard to that proposal?

Mr. BURBANO. Other than what Mr. Brock just mentioned, no, but I would like to say that my personal opinion is I agree that one needs to be done, and I think one model could be right across the river here.

In the State of Virginia, the Governor has created, you know, a Secretary of Technology to look both within the state government, but also outside for IT management. That is one model you might want to take a look at.

Mr. MAYBURY. If I could suggest one other model would be a cross agency CIO would be the intelligence community CIO, Mr. John Dams' office.

Chairman GILMAN. Dr. Maybury points out that the success of instituting a collaborative system requires clear objectives that can drive change. Mr. Burbano, has the interagency working group identified such objectives?

Mr. BURBANO. At the high level, as Mr. Brock mentioned. We are getting down to the detail level, but for right now it is at the high level. Those were submitted in the written testimony both for the IT common platform and the knowledge management system. Some other detailed documents have been delivered to GAO and the Committee.

Chairman GILMAN. Dr. Maybury says one of the values of a collaborative environment is it can reduce the number of forward deployed personnel. That is, jobs can be done back home.

Mr. Burbano, are you examining that kind of a prospect, and do you think that technology will in fact allow for fewer personnel to have to be stationed overseas, and would those jobs be mostly administrative?

Mr. BURBANO. The answer to the first part I would say is that the right sizing committee is the committee that is actually examining that. That is the right sizing committee.

My committee, the IT, will support that effort, but, you know, will not be, you know, making the recommendations or the decisions on actually, you know, reducing or shifting staff. That is the right sizing committee.

Yes, IT will support the right sizing efforts fully and can, but there are other issues other than technology when you are trying to make decisions. Right sizing does not automatically mean reduction of staff. It means shifting to, you know, proper support where you need that staff.

Chairman GILMAN. Dr. Maybury, the Committee is concerned about the risks involved in developing an overseas common information technology platform and whether State Department is positioned to lead that kind of a project.

In your view, what can our Committee do to effectively oversee that kind of a project as it enters development and requires additional funding?

Mr. MAYBURY. Well, I think, Mr. Chairman, regular oversight expectations have explicit objectives. I know in my testimony that the organization that does this needs to have a set of key characteristics that include excellence in acquisition, systems engineering experience, technical expertise in not only security, but in collaboration, knowledge management, cleared staff, especially if we are talking about secure and unsecure systems, domain knowledge of overseas activities, perhaps personnel overseas.

That is another risk is do you have the IT talent or the infrastructure overseas, and do you have a strong contractor base or contractor oversight. I think having explicit plans, these blueprints or these maps we talked about before, these architectures, at various levels of detail and monitoring those activities, monitoring the investments and looking for actual outcomes, looking for specific measurable impact, business outcomes, of the investments.

Chairman GILMAN. Have you had an opportunity to discuss those proposals with Mrs. Cohen, Assistant Secretary for Management?

Mr. MAYBURY. No, sir, I have not.

Chairman GILMAN. I hope you might take advantage of trying to do just that so that she would have the benefit of your thinking.

One last question before I call on Mr. Sherman. Mr. Burbano, several U.S. Government agencies with global operations are seeking funding for separate communications systems. Different agencies want their own system.

What are we doing to persuade those agencies that a single connected system designed on an interagency basis is probably much more preferable?

Mr. BURBANO. What we are doing is with the OPAP I think that gets down to the heart of this because those agencies are represented on the various OPAP committees. Also with the CIO Council we have an interoperability committee that works with the various CIOs of the various agencies, and then you have the IC, intelligence community, as was just stated earlier by Dr. Maybury, and I also sit on that, on the executive committee for the intelligence CIO committee, so we are all sitting in each others' committees and so we are well aware of all the things that are going on.

I think OPAP is bringing to the forefront because the President's mandate and OMB and also the congressional leadership of want-

ing to implement OPAP that for the first time we actually have more than just, you know, intentions, but we actually have a mandate to implement these government wide systems.

These are the same agencies that you are talking about, and there is a lot of collaboration going on, and I think it is beginning to take an effect. As we stated, first we are working on the unclassified first in the first 18 months, and then after that we work on the classified systems.

Chairman GILMAN. Well, we hope you can convince all of these competing agencies to work together. I think it is extremely important.

Mr. Sherman.

Mr. SHERMAN. Thank you, Mr. Chairman.

I think we are all concerned with security of our information. Some recent problems experienced by another Federal department have highlighted that recently. I want to commend the Chairman for holding these hearings, which I think focus on information security, but I think others will ask questions about our national security information, and I want to focus my questions on the visa process.

This is a process that has flabbergasted me because I did not think that governments could be this inefficient, and it takes really bad computers and bad management to achieve some of the problems that we have experienced in this area, and yet my hope is that the information technology system as it gets better will begin to solve some of those problems.

One of the many areas of problems are difficulties in communicating via computer between the INS and the State Department. Have those been worked out?

Mr. BURBANO. I think we have worked some of them out, especially during the Y2K rollover. We had to make sure the systems, you know, communicated. There are other issues, and, you know, those—Consular Affairs, CA. You know, if you got to particulars I guess we could address them with Consular Affairs.

Mr. SHERMAN. Well, I mean, first the Y2K thing. There are a number of countries in the world that thought the whole Y2K thing was a crock, invested nothing and tried to solve it and did just fine.

We in Congress provided billions to try to improve our computer systems and deal with Y2K. I am glad the sky did not fall, but we paid an awful lot of money to keep the sky from falling, and it did not fall elsewhere.

As to particular problems, when I hear from my district that a fiance visa is taking 2 years in some places and 2 days in other places and that the State Department will not reallocate resources to be fair to Americans, one who decides to marry a Filipino and another who decides to marry and English woman, that is bad management.

When I am told that we do not have any records on whether a particular visa officer by visa officer as to their success rate—which visa officers are rejecting 30, 40, 50 percent of the requests? Which visa officers are seeing over stays or violations of U.S. immigration laws in 5 or 10 or 15 percent of the visas they grant?

The problem with information technology is that you would provide accountability and require good judgment or spotlight bad

judgment. When I have suggested various actions that would privatize these decisions by allowing people to get bail bonds, you know, we have the same—virtually an analogous issue on whether somebody will over stay in the United States and whether somebody will over stay their period of freedom before their trial.

In the private area, in the domestic area, we have turned to bail bondsmen who privatize that decision and put their money where their mouth is. We refuse to do that in the State area because total capricious power unaccountable through any technology system seems to be the goal.

I have been told that this continues only because it does not affect American citizens. Once the DMV in California was about 10 percent as bad, and the whole state demanded that it get better. It never reached these levels.

What information technology do we have with regard to how long it takes from application to grant in visa matters in the various consulates and embassies around the world? Do we have that information?

Mr. BURBANO. No, but I can get it for you because that is in the Consular Affairs Office, in that bureau, and they have that.

Mr. SHERMAN. Have you spent much time looking at their information system?

Mr. BURBANO. I would not say a tremendous amount of time because I have been dealing with the security and all these other elements, and they——

Mr. SHERMAN. I cannot tell you that it is more important than national security, but——

Mr. BURBANO. Right.

Mr. SHERMAN [continuing]. If you have some time, that is where you ought to deploy it because it is a bad system, and all the questions I have asked have come back, and just basic questions we ought to have.

No accountability by person. The accountability works two ways. What I am worried about is that every visa officer will strangle our tourism industry if they feel oh, we will be held accountable for how many over stays. We ought to hold visa officers accountable for under grants and for excessive rejections, but we cannot because we do not have a system that will tell us.

I do not know if you have anybody on the panel who is familiar with these issues. I see people shaking their heads.

Chairman GILMAN. We do not have people here from Consular Affairs. Do you have anything, Wayne?

Mr. RYCHAK. No.

Mr. SHERMAN. It surprises me to have a hearing on information technology, to have a distinguished panel of four and a back up group of several more and not to have anybody familiar with information technology in this area, but that shows that this is kind of a stepchild.

We recently did receive a report. It was produced at my request. We have not been able to review it thoroughly, but it provides averages that I know are false because I have talked to people out in the field. When I complained that it took 2 years to unify an American family I was told gee, that is standard. That is kind of what

we do here in the Philippines. Then I get a report that says the average is 20 days, 30 days. I know it is not accurate.

I realize none of you have come prepared to talk about these subjects. I hope that we would develop a visa system and perhaps, Mr. Burbano, you could let me know whether we are on the way,

Mr. BURBANO. Yes. I would be happy to get back to you.

Mr. SHERMAN. That would keep track of how long things last, if things are lasting too long why, whether there have been congressional inquiries and how those have been resolved.

I mean, I am dealing with a part of the State Department where I have been told that congressional involvement is detested and will also result in intentional delays, so this is an area where we need a good information system and appreciate your attention to it.

Mr. BURBANO. Yes. We will get back to you.

Chairman GILMAN. Thank you.

Mr. SHERMAN. Thank you, Mr. Chairman.

Chairman GILMAN. Gentlemen? Dr. Cooksey? Gentlemen, I am going to have to go to another meeting, and I am going to ask Dr. Cooksey if he would lead further discussion in our subcommittee.

I want to thank our panelists for your excellent testimony. You have given us a great deal of food for thought of what we arguably should be doing in our oversight capacity and even suggested some legislation that we will take a good, hard look at.

We wish you continued success in what you are doing. Thank you very much.

Mr. COOKSEY [presiding]. Thank you, Mr. Chairman.

It is great to be here. It is great to be here with people of your educational background. There are too many politicians in this city, and there are not enough scientists and computer experts.

I do not have but about 35 questions. We should be through by 5 or 6 o'clock. Dr. is it Maybury?

Mr. MAYBURY. Yes, sir.

Mr. COOKSEY. Yes. We have been together in a committee, and I forget which one. You have a Ph.D. in artificial intelligence I understand. Is that correct?

Mr. MAYBURY. Yes, sir.

Mr. COOKSEY. What do you think about Kakoos' book, Visions? Have you seen the book? He is a theoretical physics professor in New York.

Mr. MAYBURY. I have not seen the book, sir.

Mr. COOKSEY. It is really a good book, but he says we have a ways to go in artificial intelligence and robots, but it is fascinating some of the things that he proposes.

Mr. MAYBURY. I would agree with that statement.

Mr. COOKSEY. Yes. He is very well documented. He talks about who is doing the good research and who is doing the other research.

Along those lines, what do you think about change in the biometric system? I am a physician. I am an ophthalmologist. Change the password system from whatever you use now to a biometric system; for example, retinal patterns?

Mr. MAYBURY. In fact, actually I referred in my oral testimony that there are a couple of technologies like fingerprint detection,

like biometrics that, of course, can enhance security specifically for authentication. One could think even if you wanted to go so far as DNA testing to determine that you actually had the individual that you knew was accessing the system.

I think authentication is an important area. I think that—I am not a biometric expert, but certainly those technologies have been used in secure facilities to control access.

Mr. COOKSEY. And they work?

Mr. MAYBURY. Unfortunately, I cannot speak specifically to the performance. Obviously there are both probably precision and recall measures, technical measures, in terms of their performance. Perhaps others can.

Mr. RYCHAK. Sir, I can address part of that.

Mr. COOKSEY. Yes?

Mr. RYCHAK. There is a tremendous amount of research that is going on in the whole biomedical/biometric area. I think what you will find throughout the government and throughout the private sector is that no one countermeasure by itself is adequate, but used in combination and layered with other things you do—you can end up with a high level of security.

We have a pilot program, for example, in the State Department right now of looking at combining biometrics with SMART card technology—you are probably familiar with SMART card and its capability—and combining those two to allow access into highly restricted areas to include highly restricted information systems.

We really think that that probably is the future here, as opposed to simply relying on a password that obviously can be easily duplicated or in some cases found out about, you know.

Mr. COOKSEY. The passwords that we have used since the 1970's.

I helped a company in Boston design electronic medical records from ophthalmology. We have updated a lot of my technology, but still some of the passwords are old. It is very old technology.

Yes, Mr. Burbano?

Mr. BURBANO. Yes. I wanted to add a comment. I agree. I think the biometrics systems are excellent, but it is a question of funding. That is the problem, you know. These systems are——

Mr. COOKSEY. Do you mean Congress will not give you enough money?

Mr. BURBANO. Well, that, but more importantly, the system, wherever the money comes from. What I am saying is it is very expensive compared to the password, so it is always a question of funding, to be honest with you. I mean, I think there are good systems, but you have to have the money to do them.

As Mr. Rychak said, you know, we look at other alternatives. SMART card, you know, does not have the—necessarily. Somebody else could pick up the SMART card, PIN number or whatever, but you cannot pick up your eye, but it is a lot cheaper than that system, so it is a question of funding.

Mr. MAYBURY. If I could say something? It is also obviously a question of technology. We at MITRE Corporation and many other companies have for years been using SMART cards with PINs to control and to authenticate users.

In the future we can expect, among other things, for example, video cameras to be built into laptops, for example, so the oppor-

tunity to do facial ID, which is another area, also, potentially retinal scans cheaply is something that certainly, I cannot predict or give you a year, but it is certainly going to be cheaper in the future than it is presently.

Mr. COOKSEY. Kakoos says that computer chips will cost between 1 and 5 cents apiece. He says they will be in the drapes, and——

Mr. MAYBURY. Right.

Mr. COOKSEY [continuing]. They will be able to sense weather changes, body temperature changes.

Mr. MAYBURY. They will be built into your clothing.

Mr. COOKSEY. Clothing. Right.

Mr. MAYBURY. Sure.

Mr. COOKSEY. He also said that they will use DNA instead of computer chips. That is a fascinating concept to think about. There is research being done on that.

Mr. MAYBURY. Yes. In fact, we have some research on micro electronics. DARPA has a large program and specifically atonic level storage devices, computing devices and the like, so that is actually——

Mr. COOKSEY. That is an ongoing research.

Mr. MAYBURY [continuing]. A new wave of computing technology.

Mr. COOKSEY. Well, it is exciting to think about, and that is the reason, that when you design an information system you have to think about the future and be able to move to it.

Mr. Burbano, you had indicated in your testimony that your systems are protected with intrusion detection systems, that you will know if someone has intruded into the State Department system.

Now, Mr. Brock said in his testimony that the State Department's automated intrusion detection system does not cover all of the domestic and overseas posts. Who is right?

Mr. Rychak, you get to referee.

Mr. BURBANO. Actually, he is the one.

Mr. RYCHAK. I probably can answer it.

Mr. BURBANO. Yes. He should answer it. I just wanted to make an initial statement and then I will turn it over, and that is that we are in the midst of implementing it so, I mean, he is right. We are not finished implementing it.

Mr. COOKSEY. Because your testimony basically—you contradicted each other.

Mr. BURBANO. No. I do not think so. It is a matter of implementation.

Mr. COOKSEY. You are not finished.

Mr. BURBANO. I will let Mr. Rychak give you the status of that.

Mr. RYCHAK. Yes. We started the intrusion network program in December of this past year. Our goal is to have it completed by the second quarter of next fiscal year. Essentially what it encompasses is installing hardware/ software on every system at every embassy around the world to include our domestic facilities.

As we speak, we have it in place at about 60 locations. The majority of our domestic sensitive but unclassified systems have coverage. Our financial centers overseas have coverage. The majority of our posts in South America have coverage, and we are systematically going through it in terms of the implementation.

We do have a 24 hour by 7 monitoring operation that is fully in place, but, as Fernando says, we are not there yet. We are aggressively implementing this, but given the scope of what we are trying to do it just takes time to do it right.

Mr. BURBANO. Also the funding.

Mr. RYCHAK. And the funding, although the funding for the first——

Mr. COOKSEY. Another appropriations matter.

Mr. RYCHAK. Well, that is a good point because the funding for the first phase is covered. In other words, we have enough funding to continue the installation of the systems on our unclassified but sensitive systems.

The second phase is to put identical protection for our classified systems. That is important. It has not been as critical in terms of our priority because the State Department's classified systems were not as interconnected as our unclassified systems. Frankly, we benefited from the fact that we had and continue to have a fair amount of antiquated technology out there.

The unclassified systems were becoming increasingly vulnerable as we got into internet and as we became much more interconnected, so that became our first priority.

Mr. COOKSEY. Mr. Brock.

Mr. BROCK. One of the issues that has come up at other agencies where we have looked at automated intrusion protection programs is, first of all, this technology is fairly new. It is not very mature, and lots of advances are being made.

You get an incredible amount of information. In some organizations it has literally overwhelmed the organization's capability to do the analysis, and as a result we have gone into some agencies where they made a good faith attempt initially to handle the information coming in, but then ultimately it began to stack up and pile up in back rooms and was not looked at, so a tool that is turned on but not used is pretty useless.

I think a challenge that the State Department has in rolling this out is to make a decision or series of decisions on what kind of information they really want and how are they going to do the analysis because it is fairly people oriented. Even though the tools are automated, a lot of the analysis is not and does require trained personnel.

Mr. COOKSEY. Needless to say, that is a potential problem. Of course, you get into the issue of one big system that serves all needs. The IRS did not do very well. I think they spent $3 billion or $4 billion and gave up. I think CSC has a contract now to do the IRS' work.

Mr. BROCK. Yes.

Mr. COOKSEY. Another question. I understand that the State—this is for you, Mr. Burbano. Does the State Department use a bulk e-mail system whereby the e-mails are held up until enough are collected, and then they are sent in bulk to reduce cost?

Mr. BURBANO. To reduce cost?

Mr. COOKSEY. Do you do bulk mailing of e-mail? If I sent an e-mail or let's say you sent an e-mail from Foggy Bottom to Bangkok and then there are ten other people on your staff that send e-mails

there, are they all sent at one time in bulk, or are they sent—do they each go individually?

Mr. BURBANO. My understanding is that they go as they go. They have to go through Washington for the most part, but, I mean, they do not get bulked or anything.

Wayne, do you have anything to add to that?

Mr. RYCHAK. Yes. I am sorry. I cannot. I do not know.

Mr. BURBANO. I can look into it, but, I mean, the e-mail does not sit there. In fact, we have made a lot of improvements in our e-mail system in the last 6 months not only for security, but for speed wise where we have actually improved response time tremendously as a result of getting rid of a lot of the overhead that these e-mail systems have by implementing X.500, that type of technologies, directory type systems.

Mr. COOKSEY. Well, today I would like to ask everyone who is not here representing the PRC or Russia to stay and have all the rest of you leave, but I am afraid we still would not know who was here.

I just assume. Every time I come to one of these meetings, I assume that there is someone here from some of our potential adversaries that I hope will become allies, but, you know, that is part of the intelligence game. They are here, and we have a democracy.

Hopefully those countries will move to—until we have this perfect world where we trust all of our former adversaries and they trust us, intelligence is going to be necessary. We are going to spy on them, and they will spy on us.

I just think it is absolutely mandatory that you maintain your diligence in having security in the information systems because people's lives are at stake, and there are people's lives probably that have already been lost or compromised just because of some less than perfect security measures in this country.

You can look at what has been going on in New Mexico. I think it is really terrible that that has happened. I am still a clinical professor, and I got the feeling that there was an attitude of these professors that were involved, that were running that laboratory, that they were above having to go through all the security measures, and that is part of the reason things were lax.

I think that there was some reason to believe that there was some active information gathering by some of our adversaries, and yet we have to be diligent to make sure that we have good countermeasures and make sure that they do not get information.

I appreciate your coming. I think there are some real professionals over at the State Department. I do not always agree with the political decisions that are made there. The biggest problem we have in this city is you have too many career politicians that instead of voting first what is best for the Nation and then their state and then their district, they do what is best for their political career.

I feel that the people that are permanent in the State Department do not make those decisions, and I think some of the worst mistakes that have been made in Republican administrations, and probably they are getting ready to gavel me down. I am getting out of line. And in Democratic administrations is because people do not have their priorities right, and it causes problems.

I think that one of the most disgraceful things going on right now is what is going on in Africa. This Administration and this Congress have been so Euro centered and so centered on the Middle East. They have just totally ignored the fact that a million people were killed in Rwanda and Burundi and Ethiopia and Eritrea and Sierra Leone.

It is cowardess on the part of the executive branch and callousness on the part of the legislative branch, which is my party that is in control, and the net result is that a lot of people have lost their lives that did not need to lose their lives.

I hope you have courage of your convictions and continue to function in a very professional manner. It will be better for the nation, and what is better for our national will be better for the world.

Thank you.

[Whereupon, at 12:06 p.m. the Committee was adjourned.]

A P P E N D I X

JUNE 22, 2000

Chairman Benjamin A. Gilman
Opening Remarks: Hearing on June 22, 2000
"Oversight of the State Department, Part IV:
Technology Modernization and Computer Security"

I am pleased to convene this hearing on "Oversight of the State Department -- Technology Modernization and Computer Security." This is the fourth in a series of oversight hearings that this Committee will conduct relating to the Overseas Presence Advisory Panel(OPAP). We began these hearings in February 2000 when we heard from the Panel's members. At that time, and today, I believe the Panel highlighted important issues; and this Committee supports many of the recommendations made as a basis for maintaining a more effective and efficient State Department.

We are asking our panelists to provide the Committee with a comprehensive review of the condition of the State Department's information technology program, the safeguarding of its information and the prospects of developing a common platform to facilitate communication among the agencies at posts. Along with the efficiencies of high-tech systems comes a breadth of possible vulnerabilities. These systems demand continual security evaluations, and resources should be dedicated to this activity.

Personnel of the State Department must have the capacity to communicate quickly and precisely with a variety of people. The Overseas Presence Advisory Panel observed that the Department's "current infrastructure does not provide the means either to acquire information from a full range of sources or to disseminate it to a full range of audiences."

Inefficient information systems leave the Department impotent in the conduct of foreign affairs. The Department and other agencies sharing the overseas platform have taken steps to bring their systems up to private sector standards, but much more is needed to be successful on an interagency basis. Our private sector panelist, Mr. Maybury, will address the problems associated with this issue.

An overriding concern, as modernization proceeds, is to be sure that appropriate, usable systems are procured and that security elements are

addressed up-front. The taxpayer is providing an enormous amount of money over time for the worldwide upgrades, and this Committee needs to be assured that the right decisions and cost effective procurements are being made.

With recent cyber attacks against web sites and both federal and congressional computer systems, questions arise about computer systems' vulnerabilities. Investigation of these hacker assaults revealed that the techniques used over the past months were fundamentally simple. In May 1998, GAO reported that State's computer systems were very susceptible to hackers and unauthorized individuals.

Given the important data bases that the Department possesses, it would be a disaster if hacker penetration were to occur. To name just a few: the passport system, the visa system, class systems. If a hacker were to succeed, it would have a devastating effect on the functioning of these items, not to mention the effect on commerce. The Department takes in enormous amounts of revenue per day on the issuance of these items.

I believe that, in creating a modern infrastructure, utilizing a common platform and spending the nation's money wisely are critical elements on the road to information technology success. We will find out today if our State Department is on the right road or if they have hit a dead end.

Now, I would like to turn to the Ranking Democratic Member of our Committee, Mr. Gejdenson, for any remarks he would like to make.

Introductions

Today we welcome Mr. Fernando Burbano, the Chief Information Officer of the State Department. Mr. Burbano assumed this position in May 1998, and is responsible for the Department's information technology policy and operations. He oversees a budget of more than $500 million and the activities of more than 2000 employees engaged in information management. He holds advanced degrees from American University and Syracuse University.

Our second witness, Mr. Jack Brock, is Director of the Governmentwide and Defense Information Systems Issue Area at the General Accounting Office. He is responsible for information management evaluations and reviews of computer security issues for several agencies, including the State Department. He has testified several times on these issues, and GAO has developed guidance for improving responses to computer security threats. He hold advanced degrees from the University of Texas and Harvard.

Our third witness is Dr. Mark Maybury of the Mitre Corporation. Dr. Maybury comes to us highly recommended because of his experience in the field of worldwide system upgrades. He is the director of Mitre's Information Technology Division and is responsible for the advanced research and development of intelligence and defense systems supporting several government agencies. Dr. Maybury has taken a look at what it takes to build a common platform, collaborative computing and knowledge management within the foreign affairs community. He holds several advanced degrees including a PhD from Cambridge in Artificial Intelligence. We certainly appreciate his willingness to come down from Massachusetts and educate us on this highly technical field.

We appreciate all our witnesses for being here, and I would ask that you proceed with a summary of your statements. Without objection, your full statements will be made a part of the record.

I also want to welcome Mr. Wayne Rychak, a Deputy Assistant Secretary in the Diplomatic Security Bureau at the State Department. He is member of the senior foreign service and his positions with Diplomatic Security have included being Regional Security Officer in Islamabad, Pakistan. Mr. Rychak is here to respond to questions regarding information security.

WRITTEN TESTIMONY OF FERNANDO BURBANO,

DEPARTMENT OF STATE CHIEF INFORMATION OFFICER

CHAIR, OPAP INTERAGENCY TECHNOLOGY SUBCOMMITTEE

CHAIR, CRITICAL INFRASTRUCTURE PROTECTION SUBCOMMITTEE

Presented to

THE HOUSE COMMITTEE ON INTERNATIONAL RELATIONS

JUNE 22, 2000

Final

TABLE OF CONTENTS

Introduction 1

COMPUTER SECURITY 1

GAO Security Findings 3
Y2K Rollover 3
Responses to Cyber Attacks 3
The Foreign Affairs Manual (FAM) 4
System Security Program Plan 4
Establishment and Implementation of Key Controls 4
Improved Self-Assessment Capabilities 4
Centralized Information Security 6
The National Information Assurance Certification and Accreditation Process (NIACAP) 6
The Certification and Accreditation Program 7
Accreditation Management 8

OVERSEAS PRESENCE ADVISORY PANEL (OPAP) 9

Introduction 9
OPAP Report Recommendations 9
OPAP IT Infrastructure - Conceptual Framework 11
  Overview and Methodology 11
  OPAP IT High Level Architectural Concept 13
  OPAP IT Infrastructure - High Level Requirements 16
    Knowledge Management Requirements: 16
  IT Infrastructure Requirements 16
  IT Infrastructure - Assumptions 17
    OPAP Pilot Infrastructure - Open Issues 17
  OPAP Pilot Infrastructure Project - Minimizing, Avoiding, and Managing Risk 18
  OPAP Project Timeline and Major Milestones 19
OPAP Knowledge Management – Conceptual Framework 20
  Knowledge Management - Operational Concept 20
  OPAP Knowledge Management - Operational Concept 21
  OPAP Knowledge Management - Summary of Architectural Requirements 24
  Knowledge Management - Personnel-Related Issues 26
  Knowledge Management - Next Steps 26
Knowledge Management High Level Requirements Definition 27
  Knowledge Management - Targets of Opportunity 27
  Knowledge Management - Challenges 28
OPAP - Interagency Cooperation and Other Issues 29
OPAP Conclusion 30

CAPITAL PLANNING AND MODERNIZATION 31

The Information Technology Program Board (ITPB) 31
The ITPB Charter 31
Functions 32
Membership 32
Staff Support 32
Meetings 33
ITPB Standard Operating Procedures 33
State Department IT Strategic Planning 37
CONCLUSION OF TESTIMONY 39

LIST OF FIGURES

Figure 1. Computer Security Roles and Responsibilities 5
Figure 3. The NIACAP Certification and Accreditation Model 7
Figure 5. Interagency Committee Organizational Structure 10
Figure 7. Conceptual Collaboration Zone Architecture 15
Figure 9. OPAP Major Milestones and Timeline 20
Figure 10. Information Technology Program Board (ITPB) Structure 35

Introduction

The Department of State has undertaken vigorous activities that have resulted in significant achievements in three areas:

- Computer Security
- Compliance with the Overseas Presence Advisory Panel (OPAP) Report
- Capital planning and modernization

This report will address our initiatives and accomplishments in these areas.

COMPUTER SECURITY

The Department of State takes security matters very seriously. As examples of its commitment to Critical Infrastructure Protection (CIP), the State Department hosted the CIO Council Security Awareness Day, a CIP day and a Hacker briefing open to the entire Federal IT community. We also hosted a Cyber-threat Summit in November 1999, which featured world-renowned IT security experts and was moderated by CNN.

My focus over the last eighteen months has been threefold. First, measures have been instituted to improve our cyber security through enhanced business processes and technologies. Second, real-time tracking mechanisms to actively monitor our globally dispersed technology assets and infrastructure have been developed and deployed. Finally, we have instituted processes to continually assess the rigor and currency of our security improvement efforts through self-assessment activities including independent penetration tests, vulnerability assessments, and reviews of our controls and response mechanisms. We have successfully remediated findings of independent penetration tests conducted by the Lawrence-Livermore National Laboratory from June to August 1998, and Secure Computing in November 1999.

Assistant Secretaries of all appropriate business units have since reported 100% remediation and closure of these findings. We have remediated our UNIX based systems by developing Configuration Management (CM) guidelines, reconfiguring the Network Management Stations and Workstations, and upgrading the firewalls. All configuration anomalies in a number of our Windows NT Servers and Workstations have been remediated through training and self-assessment tools (Kane Security Monitor). We have remediated our Dial-in Access capability by reconfiguring modem connections and incorporating war dialing, which is now part of a program DS is performing on a regular basis. We have remediated our physical security, namely our handicap turnstiles, which have been upgraded to be fully compliant with both security requirements and the Americans with Disabilities Act. All routers have been brought into centralized management.

Summary of State Department Security Accomplishments

The Department of State accomplishments pertaining to IT security are summarized as follows:

1. Completed all actions recommended in the GAO security audit (GAO 98-145).
2. Achieved closure on FMFIA issues dating back to 1984.
3. Operated at full and uninterrupted capacity through Y2K.
4. Operated with minimal disruption through recent virus attacks.
5. Revised the Foreign Affairs Manual.
6. Drafted a System Security Program Plan based on guidance from GAO, OMB, and NIST, which is in review as we speak and is expected to be finalized no later than June, 2000.
7. Established and implemented an aggressive anti-virus program
8. Established continuous internal monitoring using an intrusion detection system.
9. Established and implemented a Computer Incident Response Capability (DoSCIRC) to respond to operational incidents, including a Computer Incident Response Team (CIRT) to respond to security incidents, including law enforcement issues. These teams are available around-the-clock.
10. Globally deployed a self-assessment COTS software tool, the Kane Security Analyst, under an enterprise license to all Information System Security Officers (ISSOs) and alternate ISSOs around the world. 400 copies of this are being deployed via DS. This deployment includes 233 foreign sites.
11. Established a continuous and rotating post and bureau evaluation program.
12. Initiated risk assessments of our classified, Sensitive but Unclassified, and Internet networks.
13. Initiated a joint effort with the NSA on a Public Key Infrastructure strategy to implement strong identification and authentication processes.
14. Initiated implementation of the risk management cycle as recommended in best practices published by GAO and OMB.
15. Inaugurated action to comply with the Chief Financial Officers Act of 1990 and the Paperwork Reduction Act of 1995 to ensure internal controls and security accountability for IT throughout the Department of State.
16. Initiated implementation of a robust certification and accreditation program incorporated within the recently released National Information Assurance Certification and Accreditation Process (NIACAP) embodied within the GAO recommendations.

Further details of the above items are disclosed in the following paragraphs.

GAO Security Findings

- COMPUTER SECURITY Pervasive, Serious Weaknesses Jeopardize State Department Operations, GAO/AIMD-98-145, May 1998, disclosed details of a GAO audit and recommended remedial measures. The GAO audit, which included an independent penetration test of our systems, identified 72 findings in 6 categories. Since my arrival at the Department of State we have addressed the eight management recommendations.

Federal Managers Financial Integrity Act (FMFIA) issues

We have achieved closure of Federal Managers Financial Integrity Act (FMFIA) issues encompassing contingency plans, mainframe security, and information systems security. These issues are summarized as follows:

Contingency Plans	Open	1984	Closed 1999
Mainframe Security	Open	1987	Closed 1999
Information Systems Security	Open	1997	Closed 2000

Y2K Rollover

The Department of State remained fully operational throughout the Y2K rollover. I directed the development of an ISSO Security Monitor (ISM) web site to handle cyber-based threats during the Y2K rollover. This web site is being revised to incorporate PKI, NIACAP, PDD-63, and Certification and Accreditation (C&A) links. We have successfully conducted and completed Sensitive But Unclassified (SBU) network penetration tests, a vulnerability assessment in agreement with PDD-63, and Y2K cyber penetration testing.

Responses to Cyber Attacks

The Department of State has also successfully repulsed numerous adversarial cyber attacks, including the May 2000 "Resume virus". Following NATO air strikes in Kosovo and Serbia, which included the accidental bombing of the Chinese Embassy in Belgrade, The Department of State encountered millions of e-mail assaults and approximately 250,000 hacking attempts. The Department of State maintained operations at full capacity. More recently, the "Love Bug" virus and variants thereof caused an estimated $10 Billion in damages globally. The Department of State did not experience any virus-inflicted data loss. Mission-critical operations were impacted only to the extent that any work-around activity, if needed, would have delayed the normal flow of business. From May 4, 2000 to May 8, 2000, a total of 99,570 hacking attempts were stopped at our firewalls.

The Foreign Affairs Manual (FAM)

We have updated the FAM Volumes 1 and 12 to reflect our security enhancements, modernization efforts, changes in roles and responsibilities, and compliance with GAO-recommended organizational structure

System Security Program Plan

We have also drafted an agency-wide System Security Program Plan, which will provide high-level guidance for program managers and users. This Systems Security Program Plan identifies and documents the diverse components comprising the Department's IT security program, identifies the functional bureaus responsible for development and implementation of the IT security program, and summarizes the guiding principles that serve as the foundation for IT security in the Department of State.

Establishment and Implementation of Key Controls

The Department of State has worked to establish and implement key controls which include an aggressive anti-virus program, continuous internal monitoring using an intrusion detection system, and around-the-clock availability of a two response teams. These are the Computer Emergency Response Capability (DoSCIRC) and the Diplomatic Security Computer Incident Response Team (CIRT).

The DoSCIRC responds to operational emergencies involving the Department of State Department computer systems by providing technical support and remediation. The DoSCIRC is centrally managed and has the ability to pull cross-functional experts who evaluate reported problems and devise appropriate response strategies.

The CIRT responds to computer security incidents on State Department networks. The CIRT is staffed by DS agents acting under authority of the Computer Fraud and Abuse Act of 1986, and is part of the Diplomatic Security/Analysis and Certification Division/Evaluation and Audit Branch (DS/ACD/EAB). The CIRT functions as a central reporting point that coordinates incident resolution with operational managers, outside computer security entities, and law enforcement entities as appropriate.

Improved Self-Assessment Capabilities

To improve our self-assessment capabilities, we have globally deployed the Kane Security Analyst (KSA) software tool under an enterprise license to strengthen the security posture of our offices. Kane Security Analyst (KSA) is a client/server security assessment tool that provides a fast, thorough analysis of client/server security for Windows NT and Novell NetWare. The KSA compares the client/server security

guration with industry best practices or the local organizational security policy. In tes, the client/server's areas of vulnerability can be discovered and corrective action . The KSA includes customizable reports that can be compiled into an attractive presentation for management. A global deployment of 400 copies of KSA has been ted, including deployment and training to 233 foreign sites as well as domestic sites. deployment is being carried out via the Diplomatic Security (DS) training office.

ave implemented a system to continually assess and evaluate our security policy and ures, which provides the capability to systematically improve our security posture. xample, we have established a continuous and rotating post and bureau evaluation am and are conducting risk assessments of our classified, Sensitive but Unclassified, nternet networks, and we are working with the National Security Agency (NSA) on lic Key Infrastructure strategy to implement strong identification and authentication sses. The roles and responsibilities of our post and bureau evaluation program are n in Figure 1.

U/S M
- **Accrediting Official**

CIO
- **Accreditation Management**

DS
- **Certification Authority**

Data Owner
- **Functional Responsibility**

- **Site Manager**
  - **Resource Executive**
- **System Manager**
  - **System Resource Management**
- **ISSO**
  - **Security Advocate**
- **User**
  - **Resource Operator**

Figure 1. Computer Security Roles and Responsibilities

Centralized Information Security

I established a Security Infrastructure Working Group (SIWG) to proactively oversee our enterprise infrastructure and coordinate an integrated department-wide security response. The SIWG is chaired by the Deputy CIO (DCIO) for Operations, and has representation from all Department Bureaus. The SIWG has achieved closure of the GAO Computer Security Audit by establishing a Tiger Team to remediate the findings and recommendations.

In December 1998, I established a centralized information security unit, the Corporate Information Systems Security Office, to oversee our enterprise infrastructure and coordinate an integrated department-wide security response. The CISSO, under the CIO, is responsible for managing and implementing the Department's computer security program. In this capacity the CISSO oversees accreditation management and infrastructure compliance functions within the Department.

The National Information Assurance Certification and Accreditation Process (NIACAP)

I have also initiated involvement in the National Information Assurance Certification and Accreditation Process (NIACAP), which is defined by National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000. NIACAP establishes the minimum national standards for certifying and accrediting national security systems. NIACAP provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. NIACAP is designed to certify that the IT meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle. This model serves as a standard boilerplate for the development of a comprehensive certification and accreditation process.

The basic NIACAP certification and accreditation process model is shown as follows in Figure 2.

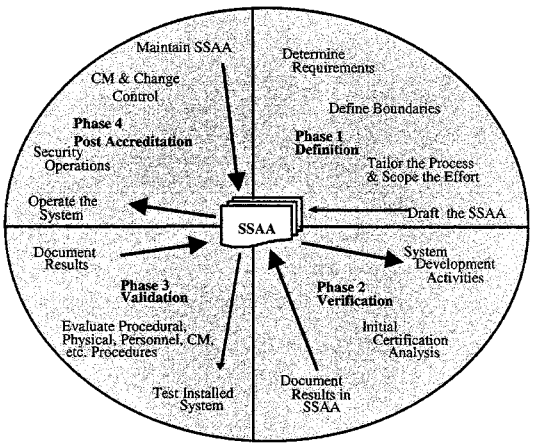

Figure 2. The NIACAP Certification and Accreditation Model

The Certification and Accreditation Program

The Department of State has initiated a strong Certification and Accreditation (C&A) program as recommended by GAO. The C&A program was established to ensure compliance with NIACAP requirements and specifically addresses the areas of policy, testing, and control. Within the context of the C&A program, certification and authentication are defined as follows.

- Certification - the comprehensive evaluation of technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

- Accreditation - Formal declaration by a Designated Approving Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable risk.

C&A involves four processes, the major components of which are summarized as follows:

1. Definition - Identify system roles, responsibilities, and security requirements; develop a C&A plan and determine level of effort; document negotiated items; incorporate existing documentation.

2. Verification - Analyze system architecture and software design; analyze network connection rule-compliance; analyze integrity of integrated products; analyze life

cycle management requirements; develop validation procedures, and conduct a vulnerability assessments.

3. Validation - Conduct a Security Test and Evaluation (ST&E); conduct penetration testing; verify TEMPEST compliance; validate COMSEC compliance; perform a system management analysis; conduct a site accreditation survey; perform a contingency plan evaluation; conduct a risk management review, document results.

4. Post-accreditation - Monitor physical, personnel, and management security practices for changes to security posture/profile; continue to verify TEMPEST and COMSEC compliance; maintain contingency plan; conduct risk-based management reviews.

Accreditation Management

The certification and accreditation process adopted by the Department of State consolidates the security mandates under the Computer Security Act, OMB A-130, and PDD-63 into a comprehensive life-cycle security process. This process simultaneously achieves the related goals of computer security and critical infrastructure protection. Through post-accreditation activities, including network monitoring and real-time configuration management tracking, the process continually verifies compliance with Department of State standards.

Throughout the process, close coordination with DS, OIG, and GAO, ensure that the key internal controls mandated by the Chief Financial Officers Act, Government Performance Results Act, and OMB A-11 are implemented in an effective manner. These controls ensure management responsibility and accountability for security and critical infrastructure protection requirements. As part of this process, vulnerabilities identified through the evaluations of auditing agencies will be incorporated into post-accreditation compliance activities to ensure that issues raised are resolved in a timely manner.

OVERSEAS PRESENCE ADVISORY PANEL (OPAP)

Introduction

To successfully advance our national interests, the foreign affairs community must be positioned to exploit the expansive access, speed, and analytical capabilities that information technology and rapid communications now afford. The leadership role of the United States in international affairs demands that we develop an integrated, responsive and secure IT capability, including systems and tools that enable us to access, manipulate, and share up-to-date information and to collaborate with others in addressing foreign policy issues. The Overseas Presence Advisory Panel (OPAP) report is the visionary blueprint for the future – one in which our interagency staff, wherever they are located, will have immediate access to the information, tools, and services needed for the conduct of e-Diplomacy in the Information Age.

The Department of State is heading the interagency effort to improve the information technology installed at our diplomatic missions around the world. As CIO for the Department, I had, in fact, already begun the planning to address many of the issues raised in the OPAP report. The Department of State's Information Technology Strategic Plan for first five years of the millennium describes five strategic IT goals as : 1) a secure global network and infrastructure; 2) ready access to international affairs applications and information; 3) integrated messaging; 4) leveraging IT to streamline operations; and, 5) sustaining a trained productive workforce. These five goals are consistent with the interagency OPAP IT goals. Thus, implementing the recommendations will build on work begun previously to meet agency specific goals.

Prior to issuance of the OPAP report, I had designated a Chief Knowledge Officer and initiated the creation of the Foreign Affairs System Integration Office (FASI) to plan for interagency connectivity. Under my direction, the Chief Knowledge Officer and Foreign Affairs Systems Integration Office are now dedicated to implementing the OPAP IT recommendations and are leading interagency groups in developing solutions.

The Department of State, in consultation with other Foreign Affairs agencies resident in our missions overseas, is planning for OPAP IT implementation at pilot posts in FY 2001. The pilot program will address the three IT-centered recommendations: 1) deploy an unclassified common, interoperable platform; 2) apply Internet and Internet-like technology to support interagency collaboration and streamline business processes; and, 3) provide a knowledge management system to share information between all Foreign Affairs agencies, wherever they are located.

OPAP Report Recommendations

On February 10, the Department of State Under Secretary for Management, Bonnie Cohen, convened an interagency Overseas Presence Committee to address OPAP report concerns. Three interagency subcommittees have been established to deal with the

specific report recommendations concerning overseas facilities, interagency rightsizing of the total foreign affairs staff, and information technology. As CIO for the Department of State, I chair the OPAP Interagency Technology Subcommittee and membership includes the CIOs of the principal foreign affair agencies (recommendation 5.2). Two interagency IT working groups were also put in place: one for implementing Knowledge Management systems and the second to design the IT infrastructure and platforms (Figure 3, graphically depicts the organizational structure of the various committees.)

To date, the cooperation between all of the foreign affairs agencies in developing solutions to the OPAP report recommendations has been outstanding. Through the CIO council and its various subcommittees, the CIOs have established strong relationships and have worked collaboratively on issues of common concern. The same spirit of cooperation has been brought to the OPAP Interagency Technology Subcommittee and associated working groups.

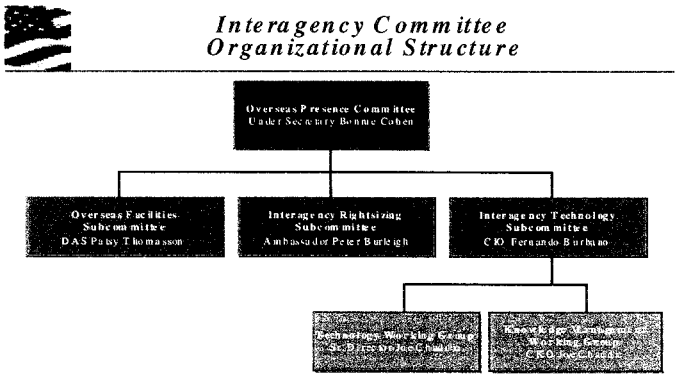

Figure 3. Interagency Committee Organizational Structure

The OPAP Interagency Technology Subcommittee will define: 1) a concept for an interagency, interoperable IT infrastructure; 2) a project plan to include development and testing of a prototype, along with field testing of the concept at two or more pilot posts as funding allows; 3) a cost model, which will be used to develop estimates for the two pilots; 4) a requirements survey; 5) preliminary design, architecture, standards and security proposals; and 6) a concept and design for a Knowledge Management system.

The upgraded information technology will improve interagency knowledge sharing and communications to enable regionalization and collaboration. Thus, the work of the Interagency Technology Subcommittee is being driven by requirements defined by the Rightsizing and Knowledge Management initiatives. The IT subcommittee has been

meeting regularly to collaborate, research, analyze, plan, and design the IT infrastructure and systems to comply with technology centered recommendations.

Six posts were identified as possible pilot sites for the OPAP rightsizing initiatives: Mexico City, Mexico, Paris, France, Tbilisi, Georgia, Amman, Jordan, New Delhi, India and Bangkok, Thailand. The chairman of the Interagency Technology working group accompanied members of the Rightsizing Subcommittee as they visited and evaluated the six posts. Based on trip findings, Mexico and India are recommended as primary candidates to pilot and test the OPAP IT solutions, conditional on the availability of timely and adequate funding.

The initial focus will be on the unclassified environment to support interagency connectivity for e-mail, safe Internet-like services to all foreign affairs agencies. Once the unclassified platform is tested, validated and fully deployed, we will progress to the classified platform, using the unclassified design as a model. We plan to utilize COTS products and existing agency platforms to the extent possible.

We have made significant progress in developing the concepts and frameworks for both the technology infrastructure and the knowledge sharing system. Specific recommendations of the intragency group regarding the infrastructure and knowledge management framework are being finalized. Thus information below is preliminary and relates to our approach for use of FY 2001 funding request by the Department for OPAP IT initiatives. The following provides a high level overview of the proposals to address the IT recommendations For the purposes of the pilot project:

OPAP IT Infrastructure - Conceptual Framework

Overview and Methodology

The OPAP Interagency Technical Study Group is studying an initial approach to implement a pilot infrastructure needed to enable all agencies, regardless of their location, to exchange e-mail and have an interoperable platform for knowledge sharing. A standardized project management approach is being be used to mitigate risk and to achieve IT recommendations presented in the Nov 1999 America's Overseas Presence in the 21st Century OPAP Report. Key items in our management approach to the project are:

- Establishment of formal Memoranda of Understanding between agencies;
- Consideration of Service Level Agreements;
- Formation of Interagency Governance Boards;
- Identification of Control Gates and interagency reviews;
- Tracking project milestones with appropriate reporting procedures including monthly status reports;

Implementation of a pilot program to test and validate the concept of operations and various technical alternatives;

- Evaluation of the pilot program and refinement of designs as necessary before proceeding with further deployment overseas;

OPAP IT High Level Architectural Concept

The Department of State has had some success with IT architectures, although we have more work to do. Our A Logical Modernization Approach (ALMA) platform, which represents an operational overseas, unclassified architecture, has been extremely successful. In addition, we have developed a high level IT Architecture (ITA) document to begin the process of establishing an architectural framework and a set of evolving standards to guide IT projects. In addition, we implemented a Configuration Control Board (CCB) and developed a high level IT Architecture (ITA) document to begin the process of establishing an architectural framework and a set of evolving standards to guide IT projects. The end result of these efforts is a remarkable level of consistency throughout the Department and around the world in terms of IT environment, especially for unclassified processing. This has resulted in increased ease of use for end users and technical support staff, and is enabling us to move forward with a global enterprise management initiative. We are now beginning to develop a parallel classified architecture.

We have been applying our architectural experience to the OPAP work, and have developed the high level pilot architecture presented below. Some key architectural principles we are planning to pursue are simplicity, flexibility, standards, and security. These principles greatly increase the chance of success, while reducing costs and risks. The high level OPAP architecture we have developed so far conforms to these principles. Key elements are that agencies need not change their architectures to connect to and use the OPAP facilities, and a range of connection options will be accommodated. Agencies need not install any special software, as a standard Web browser will be the primary common interface to the OPAP Collaboration Zone. We are modeling the pilot architecture on the Internet, where people can communicate from virtually any type of desktop or network connection. Internet like practices and tools that have so well enabled businesses and individuals to collaborate will be our model. We will refine this architecture as requirements and technical solutions become better understood.

Based on an initial set of requirements derived from the OPAP final report and information collected from the Foreign Affairs agencies, the proposed high level concept will allow all agencies access to an unclassified "network" through their existing LANs. The pilot concept proposes to create a number of "collaboration zones", which might be compared to AOL with robust security features to minimize vulnerabilities and risk of intrusion. The collaborative zone is the Foreign Affairs Community's network to share information and communicate via e-mail. The servers located in the Collaboration Zone would provide access to shared Knowledge Management data. Just like the Yahoo portal on the Internet, the collaborative zone allows users to search and interact with shared databases and applications belonging to any agency and located at any site.

The OPAP concept for interagency e-mail would provide quicker and more reliable delivery of messages and attachments than exists today. One approach to overcome the difficulties of interfacing with the current stovepipe systems is to provide robust e-mail service through a collaboration zones. This type of service would resemble an Internet

Hotmail account, making e-mail accessible from any location, using existing LANs and PCs.

By using Internet technologies, the Internet Browser at the desktop can be used to access the network and thus becomes the common platform called for in the OPAP IT recommendations. Agencies can continue to use their existing LANS, regardless of the operating system (MS NT, Banyan Vines, Apple, Novell, etc.); users will have access to the shared network with their desktop browser. Thus we do not expect agencies will have to make changes to their existing architecture. Our proposed pilot solution should be cost effective and achievable to comply with the OPAP recommendation of a common platform. We hope that in most cases agencies will not need to replace existing equipment.

To ensure a secure environment, the pilot architecture would include security-enabling technology, such as Public Key Infrastructure (PKI) for user authentication, data encryption, and firewalls at access points. The Department of State's Bureau of Diplomatic Security and the IRM Office of System Integrity will coordinate with other agencies' security elements to develop appropriate security requirements. A risk analysis and assessment will be conducted after a prototype test and prior to the pilot program deployment.

A depiction of the high level architectural concept for a pilot project is presented below in Figure 4, emphasizing the flexibility of connectivity options and the range of services to be provided by the proposed collaboration zone. The "behind the scenes" systems and security engineering that will be required to sustain the new IT environment is not represented in the diagram, but will be part of the more detailed system concept documents.

OPAP
Conceptual Collaboration Zone Architecture

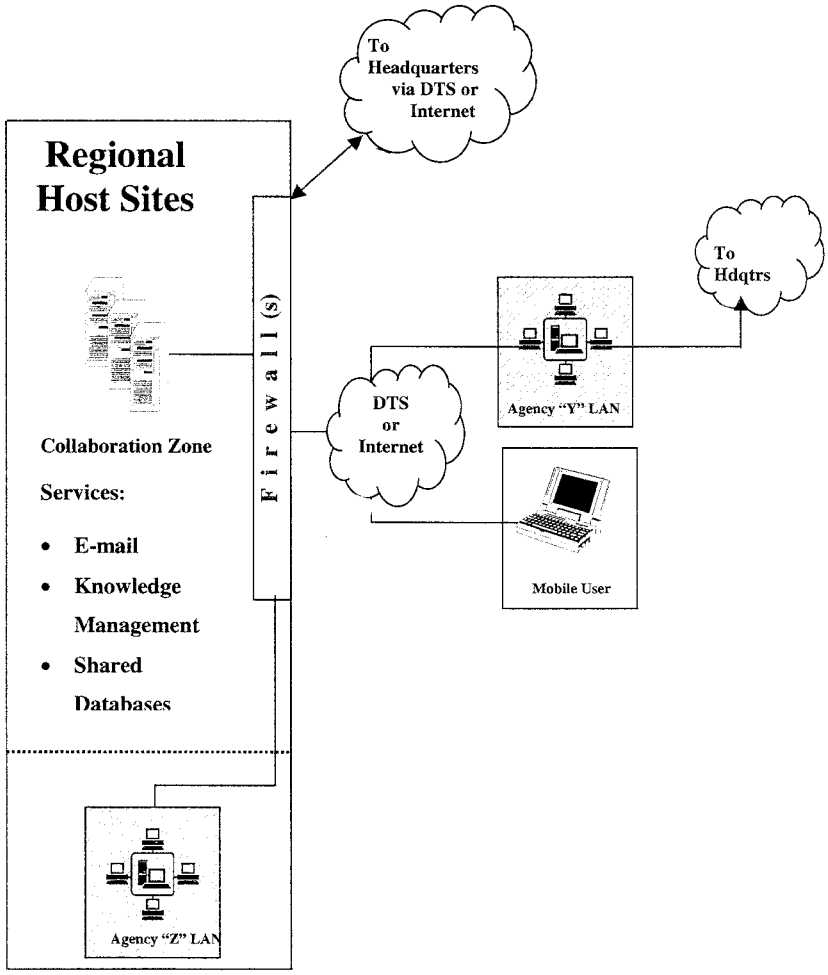

Figure 4. Conceptual Collaboration Zone Architecture

OPAP IT Infrastructure - High Level Requirements

Based on interagency discussions pertaining to Knowledge Management requirements and the common platform and Information Technology infrastructure to support knowledge sharing, the following is a synopsis of the high level requirements identified by the interagency working groups:

Knowledge Management Requirements:

Unclassified E-mail

Issue specific databases

Skills and Expertise Database

Workflow Applications

Discussion Groups Among Communities of Interest

Shared Applications

Information Repository for document sharing and collaboration

IT Infrastructure Requirements
Improve overall cost and quality of IT across the foreign affairs community

All agencies, wherever located, must be able to access the Collaboration Zone

Agencies can access the Collaboration Zone using Diplomatic Telecommunications Service – Program Office (DTS-PO) as a transport mechanism. Also able to access via Internet, dial-up, or other viable option.

Agencies cannot lose current functionality

Desktop system should be able to run TCP/IP stack and have a PKI capable web browser

Easily maintainable
- Low maintenance (minimum support staff needs)
- Remote management
- Low cost to implement

High availability
- Acceptable application performance
- Bandwidth available to meet needs

Applications must be web enabled on the front-end and PKI capable

Message Integrity

Data Confidentiality

Non-repudiation and Authentication

Security Hardware/Software Needs

Scaleable and extensible to include future expansion of Internet services where appropriate.

IT Infrastructure - Assumptions

Design for Sensitive But Unclassified[1] while allowing for unclassified.

Data owners to control access as needed.

Two possibilities exist for e-mail. These include: using existing agency e-mail systems and adding e-mail services to the collaboration zone.

Take advantage of existing Web Enabled applications.

Each agency must be able to establish connection to transport mechanism.

Connection standards will be developed.

Users will not have to be physically located at the post site.

OPAP Pilot Infrastructure - Open Issues

Availability of timely and sufficient funding for pilot posts.

Establishing and maintaining an organization process to manage the development, implementation and ongoing support of the collaboration system solution.

Clear policies and guidance on data security.

[1] Describes information which warrants a degree of protection and administration control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act.

Service levels for network, systems and applications.

Strategy for domain names and IP addressing.

Policies for providing remote access.

Current applications may not be web and PKI enabled.

Agreement on the PKI certificate process.

PKI technology is still in the pilot phase.

Configuration management.

Agency headquarters access and integration.

Integration with emergency action plans.

Agreement on Internet access policy.

OPAP Pilot Infrastructure Project - Minimizing, Avoiding, and Managing Risk

We are very comfortable dealing with the risks of large-scale overseas IT projects. We successfully deployed the ALMA IT infrastructure, Y2K modernization and remediation, and the overseas wireless modernization. We successfully addressed the numerous risks inherent in such an effort.

Some of the risks associated with OPAP are common to any IT project -- for example, delivering solutions on time and within budget. The Department of State has in place several processes for managing these types of risks. However, this effort also creates unique risks, due primarily to the interagency nature of the effort and the unclear functional scope. Unlike most IT projects, the potential scope is extraordinarily broad, and we must take aggressive steps to manage the scope, so we can deliver successfully.

We have taken several steps to address the major risks. General risk mitigation steps we have taken are:

1. We are developing a risk mitigation plan, identifying all known risks and establishing a disciplined process for monitoring these and other risks that may arise, and for addressing these risks to mitigate their impact.

2. We have limited the scope of initial efforts to unclassified systems, greatly reducing the security complications.

3. We are emphasizing commercial-off-the-shelf (COTS) solutions, reducing the need to develop high risk custom software.

4. We are proceeding incrementally, beginning with a prototype, then pilot implementation in two countries.. We will test and refine along the way, ensuring that risks are identified and resolved.

5. We will apply the disciplined IT project management process that The Department of State has been using successfully for all internal projects. This process, called Managing State Projects (MSP), will ensure that all phases of the OPAP effort go through appropriate control gates and decision points, and enabling management and the Interagency working groups to monitor progress and ensure success.

We need the support of Congress to help us address some of the most important risks. The schedule we are operating under is very aggressive, and we are currently developing a comprehensive project plan with milestones. In the course of developing this plan, it has become clear that one key variable affecting project success is timely availability of funds. There is virtually no slack in the schedule and, in fact, many tasks must be performed in parallel to achieve the deadlines. Accordingly, we can tolerate no delay in funding. We must be able to initiate procurements for the prototype as early in October as possible, and must have the funds to do so.

OPAP Project Timeline and Major Milestones

A standardized project management methodology is being employed. The project is currently in the "Study Phase." This phase will consider all viable deployment alternatives, select options based on a cost benefit analysis, develop and test prototype(s), and ultimately deploy pilot sites by September, 2001.

Milestone dates are dependent on adequate and timely availability of funding

Project Milestones

Conceptual Framework	May-00
Initial Project Plan	May-00
Requirements Document	Jun-00
Organizational Process Architecture	Jun-00
Preliminary Security Requirements	Jun-00
Cost Benefit Analysis	Jul-00
Concept of Operations	Jul-00
Formal Project Plan	Aug-00
System Acquisition Plan for Prototype	Sep-00
Prototype Implementation Plan	Oct-00
System Integration Plan -- Prototype	Dec-00
Complete Prototype Testing	Apr-01
Formal Security Risk Analysis	Apr-01
Revised Concept of Operations/ Project Plan	Apr-01
System Acquisition Plan for the Pilots	Apr-01
System Integration Plan -- Pilots	May-01
Site Training Plan	May-01
Pilot Post Deployment Plan	Jul-01
Complete KM Prototype Testing	Sep-01
Deployment of IT Pilots Completed	Sep-01
Deployment of KM Pilots Completed	Dec-01

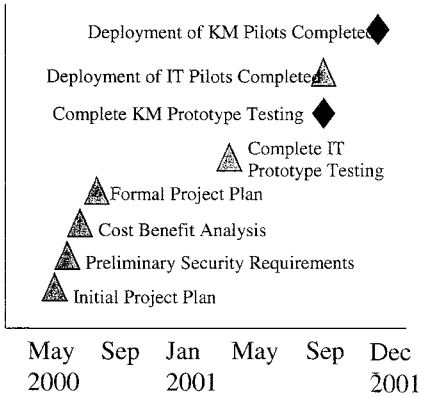

Figure 5. OPAP Major Milestones and Timeline

OPAP Knowledge Management – Conceptual Framework

Knowledge Management - Operational Concept

On April 4, the OPAP Knowledge Management Working Group published Initial Findings, including a prioritized listing of business functions at post which could accrue benefits from application of knowledge management tools and methods. Knowledge management tools are important components in the successful movement of post operations to a more collaborative, streamlined approach in line with the OPAP recommendations. The following is a high-level operational concept of the way that knowledge systems could support employees at the prototype and two pilot posts.

Knowledge Management - Scope

Organizations: The organizational scope for the knowledge management prototype and pilot projects will be the agencies participating in the right-sizing portion of the foreign affairs response to the OPAP Report. This includes the Departments of State, Defense, Commerce, Agriculture, Treasure, Justice, Transportation, the Peace Corps, the U.S. Agency for International Development, and other independent agencies.

Knowledge Systems Users: Participants in the Knowledge Management Prototype and Pilot Projects will be professionals representing their agencies at overseas posts or in Washington. At posts, the participants will be those employees who are working toward achievement of some aspect of the Mission Program Plan (MPP). It should be noted that the participating agencies vary widely in the statutory requirements and policies governing their overseas presence. Accordingly, each organization (and, hence, the users of knowledge systems) will approach joint knowledge systems differently. The material in this report represents a first draft of composite requirements across all participating agencies, not to suggest that all agencies at post would necessarily use all of the described functions. Future definition of detailed requirements will address these agency differences explicitly and will incorporate them at that time.

Classification Level: All requirements presented herein apply to Sensitive But Unclassified (SBU) information and SBU information systems.

OPAP Knowledge Management - Operational Concept

The Knowledge Management Prototype/Pilot Systems will seek to provide appropriate staff at post the following capabilities and functions:

1. Access to timely, reliable email service between agencies.
Employees will have the ability to send and receive unclassified email, including attachments, reliably and within a reasonable period of time. The first priority is to achieve this level of service between all organizations at post (includes organizations associated with the Embassy in country). In addition, that capability should extend outside the post environment, to the region and worldwide. Remote access capability (the ability to send and receive email, securely, from remote locations) is also highly desirable.

2. Access to news and information of interest to the post and the wider community.
Current news is the lifeblood of American overseas presence. The availability of late-breaking news on local and world issues allows employees at post to respond to events occurring in the host country and region as well as world issues. Equally important is access across the post community of news specific to the post.

a. Calendars: A calendar of events of general interest to the post will be available. Schedules of senior officials will be available for coordination, on a more limited basis.

b. Post/agency notices and announcements: Announcements and notices affecting the entire post will be available. Employees will be able to tailor the knowledge system to present notices from other selected organizations of interest.

c. Telephone directory: A post telephone directory will be available, and updateable by the individual. Department/Agency worldwide directories will be available in cases where such an on-line directory exists.

d. News services: All employees will have access to current local and world news and weather reports, with immediacy that is equivalent to availability of CNN. The news capability of the knowledge system will be tailorable by the employee to present the news of greatest interest either passively (with headlines on the "front page") or via "push" capability (the employee receives a tone or some other indicator that there are new headlines in their area of interest).

3. Ability to collaborate electronically across agencies on a wide range of issues.
The ability for professionals to collaborate electronically to achieve post objectives supports key aspects of the OPAP recommendations. This ability would allow workers to make the best use of their limited time and resources, and facilitates the participation of specialists regardless of geographic location. In addition, electronic collaboration improves the documentation of group activities, speeding up the learning process for those who are working on similar activities or joining the collaborative activity after it is underway. Knowledge system collaboration would allow teams of any level of formality or duration to develop "team rooms" wherein team plans, products and discussions can be developed and stored for future reference. The virtual nature of this capability allows teams to be comprised of any set of employees, located anywhere in the world. The following are examples of some areas in which this type of collaboration would be beneficial:

a. Crisis coordination: The knowledge system will support the rapid coordination needs of crisis situations, by providing the virtual "space" for crisis teams to compile plans and products and hold discussions. Crisis teams will be able to pull in expertise from other locations, as needed.

b. Support for Mission Performance Plan (MPP) "clusters": Agency representatives who are participating on issue teams aligned with the MPP will be able to meet and share products with other team members within virtual team "space". This capability will also allow the team to create repositories of information about cluster group activities for access and use by the wider community.

c. On-the-fly development of "space" for teams to use for coordination on a wide array of issues: Project or issues groups of any size will be able to create tailored "space" to meet their needs for discussion, development of products and repositories, research and consultation. Depending upon the level of technical support available at post, this process could be performed independently by team members, or by support staff located at the post or regionally.

4. Access to knowledge databases and repositories, both agency and community-owned.
current information systems environment does not support access to Department

databases and repositories by other Departments or Agencies. The knowledge systems will be designed so that Departments and Agencies may make available relevant databases and repositories of interest at post to a wider audience. The owner of each database/repository of information will define criteria for access to their information.

a. Existing databases and repositories: Each participating organization currently owns electronic research sources that could be of broader interest at post. The employee will be able to use these sources for research in cases where there is legitimate need and agreement by the owner of the resource that it is shareable. The originating organization must be able to specify the appropriate target audience for the information, and protections must be in place to assure that sharing the resource does not put the resource in jeopardy.

b. Sources developed as a result of collaboration: Products of working groups will be available to others working within the area of interest for research purposes. Team members will be able to identify work that was done on similar projects and issues within the post, the region or worldwide. This encourages use of lessons learned and development and use of best practices across the community.

c. Skills and expertise: Employees will be able to identify those within the foreign affairs community who have specific skills and expertise for purposes of consultation. Knowledge systems will be capable of capturing areas of skill and expertise based upon direct input as well as product publication and participation on virtual teams. This information will be available worldwide, allowing consultations to take place with sources of expertise quickly and with minimal cost.

d. Country or region-specific: All employees will be able to quickly and easily access information about products and issues organized by country and region. This capability will be particularly useful for orientation of employees recently arriving at post.

e. ICASS: Information about ICASS products and services as well as information currently contained within ICASS applications will be available for research. This capability will improve the ability of participating organizations to manage their ICASS activities.

5. Ability to use workflow applications to increase efficiency.
Workflow applications are computer programs which capture work transactions as they occur, streamlining the work process while organizing the captured information in ways that allow analysis, processing and distribution of the work being conducted. The result is reduced time to complete work processes, fewer instances of lost or mishandled transactions and greater efficiency of workflow. In addition, work processes accomplished this way are more easily quantified and analyzed, supporting trend analysis and decision-making. Employees will be able to "self-service" more often for both routine transactions and resource-related activities. The following are some examples of the areas where a workflow approach could be used to advantage:

a. Personnel: Offices at post will be able to process position classification requests, develop position descriptions, develop and manage performance plans and handle a wide array of personnel-related items electronically. It is important to note that the electronic nature of the transactions reduce the importance of the physical location of the specialists needed to complete the activities – work flows to the people who must work on the transaction no matter where they are located..

b. ICASS: ICASS service requests and a variety of other ICASS transactions will be available electronically, allowing representatives of each participating agency to know the status of ICASS work immediately.

c. Other administrative: Other areas suggested for workflow process include travel planning and management, training requests and feedback, financial and budget activities, procurement processes.

d. Contact management: Employees will have access to information about host country contacts, relationship history and links. Participants will be able to schedule meetings, conferences and other events, document contacts and add to the knowledge store. Options will be available to create mailing and distribution lists, and perform other work functions organizing contacts within the host country.

e. Motorpool scheduling: Post personnel will be able to interact with the motorpool office to schedule service.

f. Re-allocation of physical resources: Posts will be able to manage their excess property virtually, advertising availability of excess resources between agencies.

OPAP Knowledge Management - Summary of Architectural Requirements

The concept of operations outlined above infers a number of characteristics for the information technology architecture hosting the knowledge systems. Listed below are those characteristics. While the characteristics appear challenging when considering the current environment, they are necessary to support a robust interagency knowledge management environment.

1. The handling of email traffic must be changed to a method that allows more direct routing of email within the post and region. While some participating agencies have implemented methods to improve email flow between their personnel and the post (principally through using Internet email), this is not true across the board. In addition, several participating agencies noted the growing need for email access from remote locations (from example, from residences or while traveling).

2. Collaborative tools must be in place to support the functions outlined above. Discussions must be possible both asynchronously (meaning all parties do not need to be on-line at the same time) and synchronously (similar to the "chat" capabilities of

commercial on-line services, but using both voice and text). Capability must exist for group development of products and creation of data stores of a variety of types. It must be possible for groups to quickly develop team "space", either independently or with the support of a technical specialist at post or within the region.

3. The capability must exist to link to Department/Agency information sources that do not exist within the knowledge system. These information sources exist within the systems environments of the authoring Department/Agency. There must be capability to control access to the information per the requirements of the authoring organization, and in keeping with SBU security guidelines and practices. In all cases, access to this information is the prerogative of the authoring organization, and access rules are defined by that organization. Availability of this link must not jeopardize the information source.

4. The capability must exist to archive and manage the products and information holdings of the knowledge system(s). For example, collaborative activities, including discussions, plans, products and data stores should all be captured in a method which supports eventual archiving of the material.

5. The technical architecture must be able to support development and use of applications common to the participating agencies (to support workflow applications). The capability must exist to transfer work products between locations for workflow purposes.

6. Timely access to public news services must be available.

7. A key factor in design of architecture to meet these requirements is the low level of systems support resources available within most agencies at post. Remote administration should be considered, and to the extent that local administration can be simplified to not require involvement of systems professionals, this approach should be taken.

8. Participating agencies do not have financial resources to replace network operating systems or add substantial investments in hardware and software to their inventories. To the extent possible, information technology solutions should allow interface between the existing network and systems resources of participating agencies and the target architecture. Agencies should be able to exercise the option of fully integrating this solution into their existing networks or maintaining the knowledge systems as a stand-alone capability.

9. One candidate technology that holds promise to serve as a desktop interface to the listed capabilities is "portal" technology. One aspect of portals that make them particularly attractive for this application is the ability to tailor portals to the specific functional requirements of each worker, assuring that the information that they most need to see is presented quickly and in a manner that best suits the needs of the user.

10. Many of the listed requirements infer a method of populating the knowledge systems which is known as monitored self-posting. For most functions, professionals should be able to add information to the system, viewable by others, without requiring the assistance of a technical specialist. Monitoring capability should be available to allow oversight of the information being posted and editing of that information by an oversight organization. Particularly in the early stages of this program, it is important that there be a single point of accountability for the knowledge systems within the post, and that this entity be given responsibility for monitoring the content of the knowledge systems. It is important to provide guidance to first-time knowledge system participants regarding what is and is not appropriate content.

11. Operation of knowledge systems meeting the criteria contained herein will require telecommunications bandwidth beyond the level currently available to a large percentage of overseas posts. Bandwidth issues must be considered in the selection of knowledge tools and must be a key consideration in the development of the underlying technical architecture.

Knowledge Management - Personnel-Related Issues

1. FSN Classification
   Full implementation of the described knowledge capabilities will change the day-to-day responsibilities of many personnel at post. Several participating agencies employ Foreign Service Nationals (FSNs) in key positions requiring contribution to and interaction with the knowledge systems. This has at least two implications requiring further action. First, it is recommended that, as this program proceeds, classification standards for FSN positions be reconsidered in light of the increased sophistication of the knowledge work required in their positions. In addition, the Working Groups must analyze the impact of this situation on security requirements for a Sensitive But Unclassified systems environment.

2. Training
   Successful implementation of knowledge systems will require significant investments in training. Of particular importance is orientation of personnel to new expectations regarding the way they work and the way they think about the use and management of information sources.

Knowledge Management - Next Steps

In preparation for development of prototype and pilot knowledge systems, several near-term steps are required:

1. Further analysis of requirements. Using the requirements contained herein as a baseline, the Working Group plans to convene a focus group of senior professionals with extensive recent experience in overseas posts, to further define the requirements

for knowledge systems to support posts. The results of this analysis will drive the design of a prototype knowledge system to serve as a test bed.

2. Development of comprehensive project plans. Structured project plans must be developed to support both the development and deployment of the prototype knowledge system as well as the development and deployment of two pilot knowledge systems at posts. These plans will include criteria for measuring the impact of these systems on business operations.

3. Involvement of the designated pilot posts. The two posts designated as pilot sites will become involved as soon as possible in the process.

Knowledge Management High Level Requirements Definition

The Knowledge Management Working Group was chartered to address recommendation 4.6 of the Overseas Presence Advisory Panel (OPAP) report. In summary, the OPAP report recommends that the foreign affairs agencies view the management of knowledge as a key function, and develop systems to allow development and sharing of knowledge resources.

Knowledge Management - Targets of Opportunity

The Knowledge Management Working Group met on four occasions during March 2000, and, as of March 30, has established the following list of Targets of Opportunity for implementing knowledge management at posts (i.e., identification of business requirements at a very high level). Note the list is in a priority order as determined by the working group.

1. Ability to communicate electronically among organizations at post, sharing email, files, notices, correspondence and other work products.
2. Wider availability of issue-specific databases at post. Examples are: INS Country Team Database, USAID Research Data (CDIE), Worldwide Refugee Database, Trade Issue Search Engine, Economic and Social Data, Enforcement-related Data
3. Greater use of workflow applications to allow employees to increase productivity. Examples are: travel processing, country clearance processing, procurement requests.
4. Wider access to ICASS information.
5. Development of a skills and expertise database for the foreign affairs community to allow identification of potential consultants by issue or skill area.
6. Easier access to sources of information in Washington, both within and outside headquarters organizations.
7. Universal access to the MPP process.
8. Support for crisis coordination (evacuations, alerts, health and safety)
9. Availability of expanded information about the post and the host country.
10. Expansion of the enforcement information available to that community at post.
11. (The above items were prioritized by the working group; items below were not

for knowledge systems to support posts. The results of this analysis will drive the design of a prototype knowledge system to serve as a test bed.

2. Development of comprehensive project plans. Structured project plans must be developed to support both the development and deployment of the prototype knowledge system as well as the development and deployment of two pilot knowledge systems at posts. These plans will include criteria for measuring the impact of these systems on business operations.

3. Involvement of the designated pilot posts. The two posts designated as pilot sites will become involved as soon as possible in the process.

Knowledge Management High Level Requirements Definition

The Knowledge Management Working Group was chartered to address recommendation 4.6 of the Overseas Presence Advisory Panel (OPAP) report. In summary, the OPAP report recommends that the foreign affairs agencies view the management of knowledge as a key function, and develop systems to allow development and sharing of knowledge resources.

Knowledge Management - Targets of Opportunity

The Knowledge Management Working Group met on four occasions during March 2000, and, as of March 30, has established the following list of Targets of Opportunity for implementing knowledge management at posts (i.e., identification of business requirements at a very high level). Note the list is in a priority order as determined by the working group.

1. Ability to communicate electronically among organizations at post, sharing email, files, notices, correspondence and other work products.
2. Wider availability of issue-specific databases at post. Examples are: INS Country Team Database, USAID Research Data (CDIE), Worldwide Refugee Database, Trade Issue Search Engine, Economic and Social Data, Enforcement-related Data
3. Greater use of workflow applications to allow employees to increase productivity. Examples are: travel processing, country clearance processing, procurement requests.
4. Wider access to ICASS information.
5. Development of a skills and expertise database for the foreign affairs community to allow identification of potential consultants by issue or skill area.
6. Easier access to sources of information in Washington, both within and outside headquarters organizations.
7. Universal access to the MPP process.
8. Support for crisis coordination (evacuations, alerts, health and safety)
9. Availability of expanded information about the post and the host country.
10. Expansion of the enforcement information available to that community at post.
11. (The above items were prioritized by the working group; items below were not

OPAP - Interagency Cooperation and Other Issues

While securing the active cooperation of the approximately 40 agencies operating overseas is a major challenge, we have to date received excellent cooperation. Clearly, the most important way to obtain agency cooperation is to develop IT systems and tools that they value, and we are making good progress in that direction. We are working to ensure interagency participation in the decision-making process and in promoting the value of the OPAP approach.

The Department of State is experienced in coordinating overseas interagency efforts and in managing large, globally implemented projects. We have been leveraging that experience to the OPAP initiative. We are also finding that our own recent IT successes have increased our credibility with the other agencies and this will go a long way to achieving cooperation. We have received broad recognition for our success with several very complex projects, especially the successful worldwide deployment of the ALMA global infrastructure. We had remarkable success in our Year 2000 initiative, going from a grade of F to an A in a very short time, and have put in place a sound IT governance process. This gives other agencies confidence that working with The Department of State can yield effective IT solutions.

The Interagency subcommittees have been working collaboratively to define requirements for a pilot OPAP Collaboration Zone and for the Knowledge Management System. We are conducting a comprehensive survey of all agencies to capture functional and technical requirements for the infrastructure. The Knowledge Management Working Group will be hosting a facilitated workshop to develop more detailed business requirements for the Knowledge Management System. We have enlisted agency representatives to work together with in leading our efforts, thus giving ownership to the entire group, not just to the Department of State as the lead agency.

We learned early on in the OPAP process that flexibility is vital. We must offer agencies different options for connectivity to the OPAP network and a flexible array of functional capabilities that meet agency needs. In collaboration with all foreign affairs agencies we are working to understand and accommodate individual agency functional and business requirements as well as technical constraints. We are also working to design solutions that have no negative impact on existing systems, and that enable agencies to leverage assets already in place, thus reducing overall costs and the need to change.

The OPAP Technology Working Group is designing a pilot architecture that minimizes risk and focuses on best value for all agencies. I am working to leverage my very active involvement as a member of the CIO Executive Council, using established relationships with other agency CIOs to help promote the OPAP initiative and enlist cooperation and enthusiasm. This fits well with the Council's focus on improving interagency efforts.

The friendships and working relationships of CIOs that have been built through the Federal Agency CIO Council are evident at the meetings of the Interagency Technology Subcommittee which I chair. It is clear all agencies agree that providing a modern

accessible and interoperable infrastructure to ensure that all employees of U.S. government agencies working overseas can communicate and collaborate with each other efficiently is a worthy goal.

While I am pleased with the level of interagency cooperation and participation displayed to date in developing solutions to the OPAP report IT-centered recommendations, I am concerned that we may not achieve full participation during the pilot program due to resource constraints. The President's FY 2001 budget includes $17 million in support of the recommendations for a common information technology platform overseas and a knowledge management system. If appropriated by the Congress, the Department of State will fund the design, development and pilot program deployment for all agencies represented at the pilot sites.

As the OPAP report noted, the technology to put in place the OPAP report recommendations is available. However, each agency has its own unique procedures and regulations governing the information placed on the systems, process for changing configuration of systems, and administering systems. Interagency agreement on security processes and procedures concerning risk mitigation and minimizing of system vulnerabilities are being addressed in the early phases of the project. Implementation and operation of shared IT infrastructure and systems may also require a change in the nature of IT current operations.

OPAP Conclusion

OPAP presents a challenge and an opportunity to succeed. The Department of State has the talent and the management skills tois lead the interagency efforts to conclusion. We were successful in conquering the Y2K bug due to our management and technical expertise combined with Congressional support provided us. We also completed the worldwide deployment and implementation of ALMA at all of our overseas posts. These two examples were large complex projects very similar to potential worldwide application of OPAP solutions. . Given continued support and the cooperation of the other agencies, the foreign affairs community will be successful in implementing the OPAP recommendations.

Information Technology is just one concern highlighted by the OPAP report, but IT can enable the Foreign Affairs Community to redesign America's overseas presence. I have witnessed the willingness of my CIO colleges in the Interagency Technology Subcommittee to work together to remove the technical barriers impeding interagency communication and collaboration and move toward an e-diplomacy business model.

CAPITAL PLANNING AND MODERNIZATION

We are taking steps to ensure compliance with the Chief Financial Officers Act of 1990. The Chief Financial Officers Act of 1990, also known as Public Law 101-576, contains principle provisions to establish:

- CFO organizations in OMB and each agency;
- Improved accounting, reporting, and auditing practices;
- Improved financial systems;
- Improved asset management policies

The CFO Act of 1990 also mandates a government-wide Chief Financial Officer's (CFO) Council, and requires agencies to produce an annual progress report which is used by OMB to produce a government-wide financial management status report.

We are taking steps to ensure compliance with the requirements of Clinger-Cohen and OMB's A-11 guidance. This process was developed jointly by the Chief Information Officer, the Chief Financial Officer, and other senior management. In 1999, the Department inaugurated a new IT Capital Investment process that allocates all Central Fund resources. This process is chaired by the Under Secretary for Management to:

- Meet requirements of Clinger-Cohen and OMB A-11; and

- Establish and Maintain effective working relationships with key stakeholders, giving them active roles in IT capital planning and investment.

The Information Technology Program Board (ITPB)

Under this arrangement the senior management group, the Information Technology Program Board (ITPB), advises the Under Secretary for Management on funding allocations for the Department's IT activities. The CIO is the second chair of the ITPB and members of the ITPB are at the Assistant Secretary level representing the Department's regional, functional, and management bureaus.

The ITPB Charter

The Information Technology Program Board (ITPB), an advisory entity to the Under Secretary for Management, is the highest-level body that addresses Information Technology (IT) issues in the Department of State (DoS). The ITPB has two primary purposes: to assess and determine needs for IT resources to support DoS strategic missions, and to ensure that IT resources available to DoS are used effectively and efficiently in support of those strategic missions.

Functions

Specific functions of the ITPB are to:

- Approve and issue DoS IT Strategic and Performance Measurement Plans, ensuring that they are fully supportive of the DoS Strategic Plan.
- Approve DoS budget requests for IT resources, ensuring that initiatives being undertake are consistent with the current IT Strategic and Performance Measurement Plan.
- Allocate available IT resources on the basis of sound management and investment practices, and in particular, such factors as furtherance of DoS missions, favorable returns on investments, and the ability of IT project groups to make effective use of resources.
- Approve and issue DoS capital management procedures for initiating IT projects, implementing IT systems, and evaluating the cost and effectiveness of those systems over their entire life-cycles.

Membership

The Under Secretary for Management serves as the Chair of the ITPB. The Department's Chief Information Officer (CIO) serves as the Deputy Chair. Members of the Board include:

Executive Secretary of the Department
Assistant Secretary for Consular Affairs
Assistant Secretary for Administration
Assistant Secretary for one Regional Bureau (rotated periodically)
Assistant Secretary for one Functional Bureau (rotated periodically)
Chief Financial Officer (CFO)

Staff Support

The ITPB has no full-time staff. It is supported by staff members of FMP, IRM, and A as needed.

The ITPB depends heavily on two lower-level IT groups, the Management Review Advisory Group (MRAG) and the Technical Review Advisory Group (TRAG), for preliminary evaluations of IT issues, projects, and budget matters. The MRAG and TRAG continually evaluate IT projects, systems, and resources and provide the ITPB

with joint recommendations regarding those projects, systems, and resources, along with proposed solutions to enterprise-wide IT problems.

Meetings

The ITPB meets several times each year to support the Department's regular budget and capital planning cycles. These and other ITPB meetings, as required, will be called by the Under Secretary for Management.

ITPB Standard Operating Procedures

Scheduling Meetings – In general, the time and place of ITPB meetings will be announced at least a week in advance. Meeting announcements will be accompanied by planned agendas and background documentation pertinent to the subjects to be considered.

Attendance at Meetings – Members of the ITPB are expected to participate in each meeting or, if that is not possible, to send the person officially acting in that position. Depending on the size of the meeting room, members or designated representatives may bring other persons to ITPB meetings, if necessary; however, those persons may not participate in the ITPB discussion unless specifically asked to do so by a member of the ITPB.

Meeting Chair – The Under Secretary for Management will chair ITPB meetings. In absence of the Under Secretary, the Chief Information Officer (CIO) will chair the meetings.

Information/Presentations – To conserve the time of the ITPB, most of the information presented to it will have been pre-evaluated by the Management Review Advisory Group (MRAG) and the Technical Review Advisory Group (TRAG). In addition, most of the presentations to the ITPB will be made by members of the MRAG or TRAG. However, managers of major IT projects or other IT projects of special significance or interest may be called upon to provide direct input to the ITPB. Also, at the discretion of the Under Secretary for Management, bureau sponsors may be permitted to make presentations about their proposed projects to the ITPB.

Recommendations – The ITPB is an advisory function for the Under Secretary for Management. It provides a broad representation of Departmental interests and a variety of viewpoints helpful in decision-making. ITPB recommendations will be presented to the Chair in the form of decision memoranda.

Documentation – The staff of FMP and IRM will have responsibility for documenting decisions made by the ITPB and for distributing this documentation to members of the ITPB. The ITPB structure is shown as follows in Figure 2.

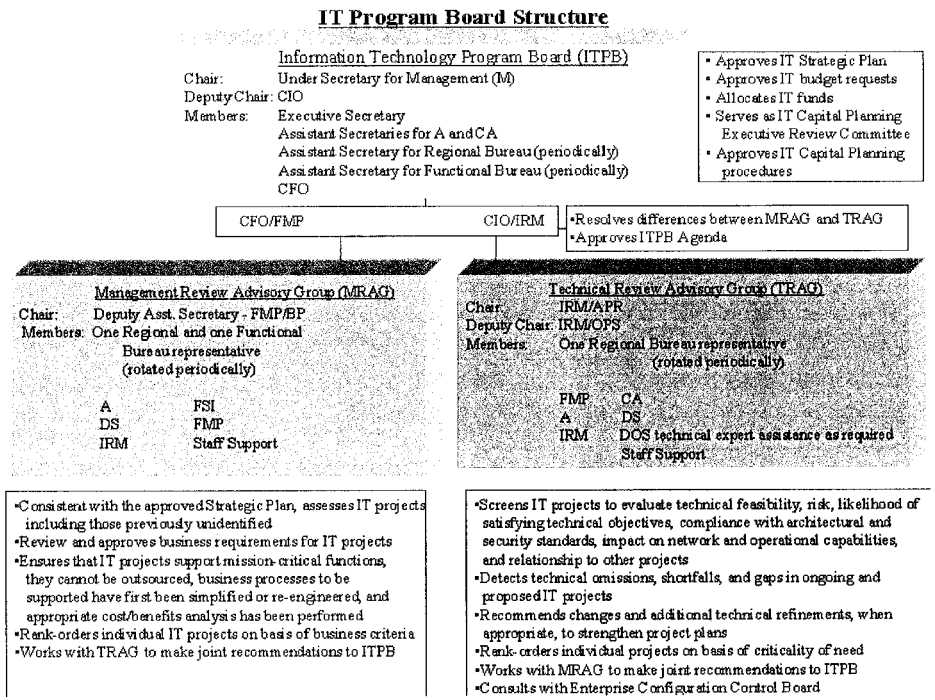

Figure 6. Information Technology Program Board (ITPB) Structure

The ITPB is supported by two advisory groups: 1) the Management Review Advisory Group (MRAG) that evaluates the investment potential of IT projects and their ability to support the Department's IT Strategic Plan; and 2) the Technical Review Advisory Group (TRAG) that assesses the technical merits of IT projects and their potential impact on the infrastructure.

Together, the ITPB, MRAG, and TRAG ensure that IT projects and systems:

- Support the mission of the Department of State;
- Represent sound investments;
- Are carried out in the most cost-effective manner possible; and
- Present managed technical risk.

Specific formats for project plans have been defined that tie to our established project management methodology – Managing State Projects – a methodology modeled after a successful approach used by the CIA. Project plans include such sections as:

- Return On Investment;
- Benefit Cost Analysis (for all major projects);
- Security Plan;
- Alternatives Analysis;
- Outcome and Output Performance Measures;
- Two year cost estimates with associated Milestones; and
- A five-year life cycle cost estimate.

A subset of this information is published in our well established IT Tactical Plan.

These project plans are provided to MRAG and TRAG members and to an IT Configuration Control Board that determines the impact on the infrastructure. In addition, change requests made to the CCB can initiate action to the ITPB if the change(s) requested are determined to have a significant impact on the architecture or infrastructure, or will require significant resources to implement or maintain.

These entities review projects against the Department's Strategic Plan, the IT Strategic Plan, and the Information Technology Architecture (ITA). The ITA was published in April of 1999, and provides a framework for mapping business requirements to technical solutions and provides a framework for specifying IT architectural components and standards. The framework of the ITA was based on guidance published by the CIO Council in late 1998. We are continually enhancing the ITA to ensure that it remains current with our plans and advances in technology.

Based on the project plans and decisions taken by the ITPB, the IT Tactical Plan presents the estimated funding requirements. However, we recently published our new IT Strategic Plan in January 2000, and are currently working to refine our cost estimates based on our updated Goals and Objectives.

The Department has a robust IT Planning and Management process currently in place. We have a series of key IT planning documents including our new IT Strategic Plan, IT Tactical Plan, and Information Technology Architecture that link to, and are driven by, the International Affairs Strategic Plan and the Department Strategic Plan. These planning documents guide and drive all of our IT work and processes. We have repeatedly been asked for copies of these plans by other government agencies including the Executive Office of the President.

State Department IT Strategic Planning

Our IT Strategic planning has been highly praised, and our Five Year Goals paper and recent IT Strategic Plan have been highlighted in the trade press. The National Research Council Office of International Affairs published an article titled The Pervasive Role of Science, Technology, and Health in Foreign Policy: (1999) Chapter 3, p.45, Broadening and Deepening Science, Technology, and Health Competence within the Department of State. This article praised our five-year plan and made mention of the plan's early achievements. This article also made the following recommendation: "The Secretary, the Administration, and Congress should ensure that the Department's five-year information technology modernization plan stays on course and is fully funded for its successful implementation and also for necessary ongoing maintenance and upgrades."

Additional management items were raised in a separate GAO modernization report Department of State IRM Modernization Program at Risk Absent Full Implementation of Key Best Practices, GAO/NSIAD-98-242, September 1998. These have also been resolved. With the Undersecretary for Management Cohen's support, IRM took the following steps to address the issues presented in the GAO report:

1. Working closely with the Chief Financial Officer and other senior management, we are taking steps to implement an enhanced Capital Planning Process to involve all the key stakeholders and meet the requirements of Clinger Cohen and OMB's A-11.
2. Implemented a working Configuration Control Board and are currently expanding the role of this CCB, further strengthening the interrelationship with the Capital Planning Process.
3. Published an Enterprise IT Architecture that is modeled after guidance issued by the Federal CIO Council.
4. Included output and outcome measures in our IT Tactical Plan and tie outcomes to mission effectiveness or efficiency.
5. Instituted a disciplined life cycle management process – called Managing State Projects – to help ensure a consistent approach to all aspects of project management.
6. Focused on a few well-articulated goals that are presented in our new IT Strategic Plan published in January of this year.

The CIO is actively engaged in ensuring the success of our IT Modernization projects:

- Works closely with the CFO and other senior management to develop effective budget plans, accompanying excellent technical plans, that have succeeded in greatly increasing our IT modernization budget.

- Engages peers at the Assistant Secretary level by meeting with them regularly.

- Conducts regular conferences with our overseas Information Management Officers (IMOs) to share vision, goals and current activities.

The success of these improvements in our planning processes is best exemplified in recent key projects:

1. The Department of State successfully deployed a fully modern IT infrastructure to the desktop of every employee at 233 overseas posts, providing robust office automation tools and e-mail access to the Internet. This modernized infrastructure provides the foundation for enhanced, information age communication and collaboration for U.S. diplomats.

2. As a result of the Department of State's proactive efforts to ensure that all of its IT systems would be Y2K compliant, little or no anomalies in our systems were encountered during the rollover. The Chairman of the House Subcommittee on Government Management, Information and Technologies, Congressman Stephen Horn, issued a report card raising our "F" in 1998 to an "A" in 1999. In recognition of this progress, The Department of State was also awarded a Government Computer News award for excellence in technology.

3. To ensure uninterruptible international emergency voice communications and to improve local communications, we fielded 883 satellite telephones, 106 emergency and evacuation, or "E&E" net radio systems, and some 5040 hand-held radios at overseas posts.

4. We now have a single modern e-mail package, MS Exchange, linking all Department offices and overseas posts

While we have made such significant progress modernizing our IT, we still have a lot of work ahead of us. We must

- Continue to deploy major improvements to our administrative and management systems such as GEMS personnel and our financial systems

- Continue to deploy CableXpress - a popular and effective new front end to our formal message traffic system

- We must replace our existing vintage World War II messaging system with a new system that provides a more robust and scaleable network taking advantage of today's technology.

- Continue to refresh our overseas unclassified infrastructure and modernized our overseas classified IT infrastructure. There are many unexploited security techniques and technologies that we must take advantage of to effectively secure the Department's worldwide IT and physical resources. We will create a state-of-the-art, cost-effective global network that maximizes access to worldwide information. This network will provide features like more robust world-wide secure communication, transmission of secure email and classified documents, and connectivity to DoD's classified network (SIPRNET).

- Implement the five Goals of the new IT Strategic Plan. This will require resources to address the gaps in our IT infrastructure. Our new IT Strategic Plan focuses on building a robust world-wide network, expanding the tools available to our substantive officers, revamping our obsolete messaging systems, centralization and streamlining our administrative systems, and enhancing the skills and retaining our core IT workers.

My new IT Strategic Plan presents this vision and lays out the road ahead of us for the next five years. The current focus of the OPAP pilots is on the unclassified infrastructure – an area in which we are fully modernized. The Department of State will require sustained funding in order to achieve the goals in the ITSP. Cornerstones to achieving these goals are the modernization of the classified infrastructure and sustained technology refresh of the entire enterprise – both will also be required in order to pursue the OPAP objectives into the classified arena in the future.

CONCLUSION OF TESTIMONY

The information technology requirements associated with modern diplomacy will likely increase over the next few years. Two recent studies, both conducted by prominent diplomatic experts, discuss the radical changes expected to occur in the conduct of diplomacy and international affairs[2]. As we addressed in this report, the more recent report of the Overseas Presence Advisory Panel (OPAP) demands a leadership role from The Department of State in ensuring interagency exchange of information and robust interoperability. Collectively, the changes that can be foreseen will subsequently generate a demand for far greater connectivity with other countries, Non-Government Organizatioins (NGOs), and various publics. As discussed in this report, security requirements, challenges, and demands are already increasing and will continue to do so. Likewise, there will be increased demand for information access, intelligent analytical tools, powerful search engines, and collaborative processing - within The Department of State, with other organizations, and with other technologies. The Department is committed to supporting our diplomats and the foreign affairs agencies as we move into

[2] Stimson and CSIS reports

this new information age. We are seeking to establish a robust IT environment that will support what we have termed *e-Diplomacy,* the conduct of diplomacy in the age of the Internet and other technological advances. We must continue to make the investments needed to support this vision and add value to the conduct of international affairs.

Although we have made great strides in the past two years, the Department faces significant IT challenges it has only most recently begun to address. Chief among these is providing a robust, secure global network that gives our domestic and overseas staff desktop access to the classified, sensitive but unclassified (SBU), and unclassified information required for the job. In the increasingly interconnected world in which they operate, our diplomats and other officers are severely short-changed by the technological limitations they face today. We must provide global connectivity and full Internet access at all locations. We must address the knowledge needs of diplomats in new and creative ways, giving them easy access to multiple, timely sources of information at their fingertips, facilitating sharing of best practices, and fostering collaboration across the foreign affairs community. To this end, we have published an IT Strategic Plan for FY2001-FY2005. The plan sets the direction and five goals for IT support for the Department's international affairs mission in the early years of the new millennium. The Department has adopted these goals at the highest levels. This IT direction closely parallels the two recent outside reports cited above, documenting the need for radical changes in diplomacy and associated supporting infrastructure. As previously noted, another study produced by the National Research Council (NRC)[3] highly praised our five year plan and calls for significant investment to implement The Department of State's IT Strategic Plan. This study recommends the following:

> The Secretary [of The Department of State], the Administration, and Congress should ensure that the Department's five-year information technology modernization plan stays on course and is fully funded....

To address these challenges and build the global network we need, we must address an array of security concerns, some of which are unique to the Department's role as the lead foreign affairs agency. Our systems have been repeatedly targeted by internal and external threats having ever-increasing levels of sophistication. Our overseas posts are heavily dependent on a local foreign nationals workforce. As communications capabilities increase, so do the security threats and risks associated with unauthorized access to sensitive information. As we connect our networks to the Internet, we must be sure to protect the integrity of our information assets. Accordingly, we have embarked on several ambitious and vital initiatives to devise and implement cost-effective security solutions that will enable us to manage and minimize risk, while providing our professionals with the information tools they need. In short, we are committed to deploying a viable security infrastructure that meets our business and security requirements.

---

[3] *The Pervasive Role of Science, Technology, and Health in Foreign Policy, Imperatives for the Department of State*, National Research Council, 1999.

The conduct of international affairs is highly information-intensive. To protect our vital national interests, The Department of State must have access to current and accurate information and the ability to disseminate and share that information among the international affairs community. This demands *e-Diplomacy* and the most effective information management tools, systems, and networks possible. The nation runs a grave risk if we fail to provide our overseas staff with ready access to the information they need to make informed decisions and provide the excellent analyses and advice the Department's stakeholders depend on. Accordingly, we must finish the job of modernization and position the nation for *e-Diplomacy*. We must continue to make the investments needed to support this vision and add value to the conduct of international affairs.

United States General Accounting Office

GAO

Testimony

Before the Committee on International Relations, House of Representatives

For Release on Delivery
10:00 am
Thursday
June 22, 2000

FOREIGN AFFAIRS

Effort to Upgrade Information Technology Overseas Faces Formidable Challenges

Statement of Jack L. Brock, Jr., Director,
Governmentwide and Defense Information Systems
Accounting and Information Management Division

GAO/T-AIMD/NSIAD-00-214

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss the Department of State's efforts to improve the foreign affairs community's information technology infrastructure. As you know, the Overseas Presence Advisory Panel[1] found that many of our embassies and missions are equipped with obsolete information technology systems, which prevent efficient communication and effective information sharing and storage. In particular, many systems within our embassies are incapable of simple electronic communications across department lines and most are disparate and not interconnected. When coupled with other problems, such as poor facilities and outmoded administrative and human resource management practices, these deficiencies were found by the Panel to seriously undermine effective representation of U.S. interests abroad.

My testimony today will focus on (1) State's efforts to implement the Panel's recommendations and (2) the challenges and risks it will face as it proceeds. State has already begun providing leadership and reaching out to other federal agencies with overseas presence. At this point, State is in the early stages of planning for the common platform initiative—establishing preliminary project milestones, developing rough cost estimates, and formulating a project plan for upgrading information technology systems abroad. The detailed plan, which State intends to complete by

[1] *America's Overseas Presence in the 21st Century: The Report of the Overseas Presence Advisory Panel,* November 1999, U.S. Department of State.

September 30, 2000, is intended to define project goals, requirements, benefits/costs, schedule, and approval procedures.

Devising a common technology solution that will meet the collective needs of this community remains a formidable task. Over 14,000 Americans and about 30,000 foreign nationals employed by over 40 federal agencies located in 160 countries around the world comprise the foreign affairs community. Moreover, each agency has a unique mission and its own information systems and obtaining consensus may be difficult. If the common platform is to move from concept to reality, State will have to overcome cultural obstacles and get agreement on both high-level and detailed requirements of the platform's users so it can make the best decisions on the types of systems, hardware, software, and networks to acquire. Moreover, it will need to carry out this delicate balancing act while working concurrently to define its own technical architecture and continuing to address pervasive computer security weaknesses. These challenges must be addressed not only to minimize risk of project failure but also—and more importantly—optimize opportunities for success.

STATE'S EFFORTS TO DEVELOP AND IMPLEMENT A COMMON OVERSEAS INFORMATION TECHNOLOGY PLATFORM

The Overseas Presence Advisory Panel was formed to consider the future of our

schedule, and approval procedures.

Devising a common technology solution that will meet the collective needs of this community remains a formidable task. Over 14,000 Americans and about 30,000 foreign nationals employed by over 40 federal agencies located in 160 countries around the world comprise the foreign affairs community. Moreover, each agency has a unique mission and its own information systems and obtaining consensus may be difficult. If the common platform is to move from concept to reality, State will have to overcome cultural obstacles and get agreement on both high-level and detailed requirements of the platform's users so it can make the best decisions on the types of systems, hardware, software, and networks to acquire. Moreover, it will need to carry out this delicate balancing act while working concurrently to define its own technical architecture and continuing to address pervasive computer security weaknesses. These challenges must be addressed not only to minimize risk of project failure but also—and more importantly—optimize opportunities for success.

STATE'S EFFORTS TO DEVELOP AND IMPLEMENT A COMMON OVERSEAS INFORMATION TECHNOLOGY PLATFORM

The Overseas Presence Advisory Panel was formed to consider the future of our

Overseas Presence Committee and is chaired by State's Undersecretary for Management. Three interagency subcommittees have been established to report to this committee, including the Rightsizing Subcommittee, the Overseas Facilities Subcommittee, and the Interagency Technology Subcommittee.

The area that you asked us to focus on, Mr. Chairman, involves the Information Technology Subcommittee, chaired by State's CIO and consisting of CIOs from the eight other major agencies with overseas presence, including the U.S. Agency for International Development, the Peace Corps, and the Departments of Defense, Justice, Transportation, Treasury, Agriculture, and Commerce.[2] Two working groups report to this subcommittee: (1) the Interagency Technology Working Group, which is responsible for defining operational requirements, selecting specific enabling strategies, identifying required funding, and establishing standards for the common platform and (2) the Knowledge Management Working Group, which is charged with making the right information available to the right people. Knowledge management is a very important component of the Panel's recommendations. The Panel's intent is that our overseas agencies be able to not only communicate with each other and back to their respective headquarters, but also to obtain and share the information and knowledge that already exists among agencies and around the world, but is currently fragmented and not readily accessible.

[2] These agencies represent nearly 99 percent of our overseas presence. State and Defense together represent almost 80 percent.

State In Early Stages Of Project Planning

State is in the process of developing a structured project plan for the lifecycle of its common platform initiative. In doing so, State intends to define user and system requirements; identify risks and assess technical feasibility; identify the major work elements that will be accomplished over the life of the project; analyze costs and benefits; establish project goals, performance measures, and resources; assign responsibilities; and establish milestones. It expects to complete this plan by September 30, 2000.

Given the risks, complexities, and potential costs involved in the common platform initiative, it is critical that State carefully scope the effort, anticipate and plan for risks, and establish realistic goals and milestones. Experience with similar undertakings has shown that poor project planning can cause agencies to pursue overly ambitious schedules, encounter cost overruns, and/or find themselves ill-prepared to manage risks.

To date, State has developed high-level preliminary project milestones and decided to pilot a prototype common system, from April through September 2001, at two posts, Mexico City, Mexico and New Delhi, India. It has also decided to follow a methodology

for managing the project called Managing State Projects, which provides a structured process for planning, applying, and controlling funds, personnel, and physical resources to yield maximum benefits during a project life cycle. The methodology focuses on a number of key factors critical to ensuring the success of any large, complex information technology effort, including (1) clearly defining what users need, (2) determining what the system will ultimately cost, and (3) defining how management will monitor and oversee progress, and ensure that the project stays on track.

State is already in the process of taking the first step—defining requirements for the overseas common technology platform. System requirements include such things as system functions, communication protocols, interfaces, regulatory requirements, security requirements, and performance characteristics. State officials responsible for managing the development of the common platform effort told us that they have developed high-level preliminary requirements and are in the process of further defining user requirements. Given the range and number of agencies and employees involved in foreign affairs, this task will need to be carefully managed. Requirements will have to be agreed upon by, and have the same meaning for, each of the participating overseas agencies, and they will need to be fully documented and sufficiently detailed so they can be used to determine what systems will be acquired and what standards will be used.

Cost estimates—the second step--cannot be finalized until user requirements are

system will cost. The Panel estimated that the ultimate cost of a common solution for both classified and unclassified information will be over $300 million. The President's FY2001 budget includes $17 million in support of the recommendation for a common information technology platform for overseas offices. State officials characterized the $17 million as a "down payment" on the total anticipated investment. If these funds are appropriated, the department intends to use them on its pilot project. State is now developing preliminary cost estimates for the pilot; however, State officials told us that these estimates will be rough given that detailed user requirements have not yet been fully defined and target systems, hardware, and networks have not yet been identified.

State officials also plan to address the third step--instilling the management oversight and accountability needed to properly guide the common platform initiative. The methodology provides a formal approval process with "control gates" to ensure that user needs are satisfied by the proposed project, timetables are met, the risks are acceptable, and costs are controlled. If effectively implemented and adhered to, these control gates can provide management with the opportunity to review and formally approve progress at key decision points. State expects to define the approval process in its overall project plan.

IMPLEMENTATION ISSUES

WILL PROVE CHALLENGING

As State is in the early stages of project planning, it faces considerable challenges in modernizing overseas information technology systems. First, State will need to obtain agreement among its various bureaus and the agencies in the foreign affairs community on such issues as requirements, resources, responsibilities, policies, and acquisition decisions. This will be a delicate task as these agencies have different needs, levels of funding, and ongoing agency-unique systems development. Second, State needs to complete its detailed information technology architecture--or blueprint--to guide and effectively control its own information technology acquisitions. It currently has a high-level architecture and anticipates completing the detailed layers of the architecture by next year. Third, the security of the common system must be fully addressed before its deployment to ensure that sensitive data is not stolen, modified, or lost.

Barriers to Cooperation Need to be Overcome

Obtaining the interagency cooperation and funding necessary to achieve the Panel's recommendations will be a major challenge. Each of the more than 40 agencies involved in foreign affairs has its own unique requirements, priorities, and resource constraints and many are accustomed to developing, acquiring, and maintaining their own systems. Yet State will need to overcome these cultural barriers and secure agreement on a range of issues such as which systems, hardware, and networks to acquire, how much can be spent on these assets, and who should be responsible for managing and maintaining them. In recognizing this dilemma, the Panel highlighted the need for Presidential initiative and support, the Secretary of State's leadership, and ongoing congressional oversight and support.

Addressing cultural and organizational barriers to standardization and cooperation will not be easy. First, it is likely that many agencies may want to continue operating their own technology, especially if these systems were recently acquired or upgraded. Second, no one agency by itself has the authority or ability to dictate a solution or to ensure the implementation of a mutually developed solution. Third, although negotiations are ongoing, details are still being worked out as to who will manage and administer the new collaborative network.

The department will also need to obtain cooperation among its various bureaus. Information management activities at State have historically been carried out on a decentralized basis and without the benefit of continuing centralized management

synchronized and the systems themselves not interoperable. State acknowledges that many of its systems can be described as "stovepiped" and "islands of automation," terms which describe their fragmentation and independence. In recognition of this problem, the department is working to establish a shared computing environment but progress has been slow.

State officials recognize that they will need to reach out to bureaus and to other agencies with overseas presence to achieve consensus on specific, detailed user requirements, acquisition decisions, standards, policies, and responsibilities and that this will be a difficult endeavor. They have told us that they have begun to explore ongoing common platform initiatives with other agencies and that they will address this challenge as they develop their overall project plan.

Lack of A Detailed Information Technology Architecture Increases Risks

Even though State is leading the common platform initiative which involves more than 40 other agencies, it does not have a detailed information technology architecture. However, State does have a high-level architecture issued last year in place and is now

working to complete supporting architectural layers. An architecture is essential to guiding and constraining information technology acquisition and development efforts. In doing so, an effective architecture will limit redundancy and incompatibility among information technology systems, enable agencies to protect sensitive data and systems, and help ensure that new information technology optimally supports mission needs.

System architectures are essentially "construction plans" or blueprints that systematically detail the full breadth and depth of an organization's mission-based mode of operations in logical and technical terms. In defining architectures, agencies should systematically and thoroughly analyze and define their target operating environment—including business functions, information needs and flows across functions, and systems characteristics required to optimally support these information needs and flows. In addition, they should provide for physical and administrative controls to ensure that hardware platforms and software are not compromised.

The importance of thoroughly and systematically identifying and analyzing information needs and placing them in a technical architecture cannot be overemphasized. The Congress recognized the importance of technical architectures when it enacted the Clinger-Cohen Act, which requires chief information officers to develop, maintain, and

[3] Clinger-Cohen Act of 1996, Pub. L. No. 104-106 (40 USC 1425 (b))

[4] OMB Memorandum M-97-02, Funding Information Systems Investments, October 25, 1996, and OMB

facilitate integrated system architectures.[3] Additionally, OMB has issued guidance[4] that, among other things, requires agency information systems investments to be consistent with federal, agency, and bureau architectures. Moreover, our reviews of other agencies have consistently shown that without a target architecture, agencies risk buying and building systems that are duplicative, incompatible, and unnecessarily costly to maintain and interface.

In April, 1999, State published a high-level information technology framework. State officials told us that documents will be produced later this year which further define the security, information applications, and technical infrastructure for the department. But, at present, State lacks the detailed framework needed to ensure that it does not build and buy systems that are duplicative, incompatible, vulnerable to security breaches, and/or are unnecessarily costly to maintain and interface. Specifically, State has not detailed its current logical and technical environment, its target environment, or specified a sequencing plan for getting from the current to the target environment. State officials told us they are working to develop these necessary architectural layers.

Such a framework is critically needed to ensure that the common platform is in concurrence with State's own target environment. If State proceeds with the common platform initiative before defining its own target architecture, it may well find that the

---

Memorandum M-97-16, Information Technology Architectures, June 18, 1997.
[3] Clinger-Cohen Act of 1996, Pub. L. No. 104-106 (40 USC 1425 (b))

initiative itself with its resulting decisions on standards, protocols, systems, and networks may end up driving the department's architecture. Moreover, each foreign affairs agency overseas has its own networks and systems, based on different protocols, systems, and security measures. By not having a defined and enforceable architecture, State may well perpetuate the current stovepiped, redundant, and disparate computing environment. State acknowledges that there is risk in proceeding with modernization initiatives in parallel with developing a complete information technology architecture, and it intends to begin addressing this risk as it proceeds with its pilot projects.

Computer Security Concerns Still a Challenge

As envisioned by the Panel, a common platform could provide overseas agency staff with collaborative applications and Internet access. The Panel recognized that security risks would be increased with this greater connectivity and indicated that solutions, such as the use of industry best practices and security software, would be required to mitigate these risks. In view of these added risks, I would like to discuss specific concerns we raised in a previous review of State's computer security practices. State has generally made good progress in addressing these concerns; however, issues

remain which must be paid attention to in order to ensure the integrity of the proposed platform.

Two years ago we reported[5] that the State Department's unclassified information systems and the information contained within them were vulnerable to access, change, disclosure, disruption, or even denial of service by unauthorized individuals. During penetration testing of State's systems at that time, we were able to access sensitive information and could have performed system administration actions in which we could have deleted or modified data, added new data, shut down servers, and monitored network traffic. The results of our tests showed that individuals or organizations seeking to damage State operations, commit terrorism, or obtain financial gain could possibly exploit the department's information security weaknesses. For example, by accessing State's systems, an individual could obtain sensitive information on State's administrative processes and key business processes, such as diplomatic negotiations and agreements. Our successful penetrations of State's computer resources went largely undetected during our testing, underscoring the Department's serious vulnerabilities.

Our penetration testing two years ago was successful primarily because State lacked an overall management framework and program for effectively overseeing and addressing information security risks. In particular, State lacked a central focal point for

[5] *Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations* (GAO/AIMD-98-145, May 18, 1998).

overseeing and coordinating security activities; it was not performing routine risk assessments to protect sensitive information; its information security policies were incomplete; it lacked key controls for monitoring and evaluating the effectiveness of its security programs; and it had not established a robust incident response capability. We also found that security awareness among State employees was problematic. For example, we were able to gain access to networks by guessing user passwords, bypassing physical security at one facility, and searching unattended areas for user account information and active terminal sessions.

As such, we recommended that State take a number of actions based on private sector best practices that have been shown to greatly improve organizations' ability to protect their information and computer resources. In response, State has taken a number of positive steps to address our recommendations and made real progress in strengthening its overall security program. For example, the department consolidated its previously fragmented security responsibilities and made the Chief Information Officer responsible for all aspects of the department's comprehensive computer security program; clarified in writing computer security roles and responsibilities for the Information Resources Management and Diplomatic Security offices; and enhanced its ability to detect and respond to computer security incidents by establishing a Computer Incident Response Team. In addition, the department revised its Foreign Affairs Manual to require the use of risk management by project managers and resolved the specific physical and computer security weaknesses we identified during our testing.

However, State's implementation of recommendations that are integral to successful implementation of the common platform initiative is incomplete. For example,

- State's automated intrusion detection program does not yet cover all domestic and overseas posts. As a result, State does not have a comprehensive overview of attempted or successful attacks on its worldwide systems. Lack of such a process limits State's ability to accurately detect intrusions, deal with them in a timely manner, and effectively share information about intrusions across the department.

- State lacks a mechanism for tracking and ensuring that the hundreds of recommendations made by auditors and internal vulnerability studies over the last 3 years are addressed. Again, this limits the department's ability to ensure that all relevant findings are addressed and resolved. State officials told us that action is underway to develop a tracking system.

- Lastly, even though State has formally consolidated computer security responsibilities under its CIO, its Bureau of Diplomatic Security will still be responsible for carrying out important computer security related tasks such as establishing policy, conducting security evaluations at diplomatic posts, and conducting training. As stressed in our report, fragmented responsibilities in the past have resulted in no one office being fully accountable for information technology security problems and disagreements over strategy and tactics for improvements. This new process can

work, but it will be essential for the department to ensure that the Chief Information Officer effectively coordinates these responsibilities.

Consistent with our recommendations, State performed four computer security evaluations of its unclassified and sensitive but unclassified networks over the past three years. In response to your request, Mr. Chairman, we reviewed these evaluations and found that State's networks remain highly vulnerable to exploitation and unauthorized access. Because three of the four evaluation reports are classified, we are constrained in this forum from discussing specific vulnerabilities. However, each of the reports found problems indicating continuing computer security problems at the department. Collectively, the reports indicate a continuing need for the department to assess whether controls are in place and operating as intended to reduce risks to sensitive information assets. Recent media reports highlighting State problems with physical security also emphasize the need for continued vigilance in this area.

At the time of our work for this Committee, State was unable to provide much information about security features for the common platform because its design is still underway. However, based on the fact that State's networks remain vulnerable to individuals or organizations seeking to damage State operations, we emphasize the importance of effectively addressing the significant challenge that additional external connectivity brings to securing the foreign affairs community's planned information network.

Conclusions

Mr. Chairman, in summary, maintaining an effective presence overseas absolutely requires up-to-date information and communications technology. Officials overseas must have easy access to all agencies sharing the overseas platform and the fastest possible access to all information that might help them do their jobs. State is taking steps to address this need but it faces significant hurdles in doing so. Not only must it secure agreements among a wide range of disparate users and agencies, it must do so while undertaking equally challenging efforts to develop a detailed technical architecture and address continuing computer security issues. As a result, as it completes it project plan over the next few months, it is critical that State

- Carefully scope the initiative, identify and mitigate risks, analyze costs and benefits, and establish realistic goals and milestones.
- Instill the management and oversight accountability needed to properly guide the effort and secure agreement on who will manage and maintain the systems once they are implemented.
- Anticipate the steps needed to overcome cultural obstacles and employ a truly collaborative approach that can effectively facilitate agreement on requirements, priorities, resources, policies, and acquisition decisions.
- Place high priority on developing a detailed systems architecture for the department that will help ensure that information technology acquired is compatible and aligned

with needs across all business areas.

- Vigorously pursue efforts to strengthen long-standing computer security weaknesses and ensure that new policies, responsibilities, and procedures being implemented are on par with best practices.

Mr. Chairman and Members of the Committee, this concludes my statement. I will be happy to answer any questions you or Members of the Committee may have.

Contacts and Acknowledgements

For questions regarding this testimony, please contact Jack L. Brock, Jr. at (202) 512-6240. Individuals making key contributions to this testimony included Cristina Chaplain, Kirk Daubenspeck, John de Ferrari, Patrick Dugan, Diana Glod, Edward Kennedy, Hai Tran, and William Wadsworth.

(511968)

A Common Platform for the Foreign Affairs Community: Collaborative Computing & Knowledge Management

Dr. Mark T. Maybury
Executive Director
Information Technology Division
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
maybury@mitre.org
www.mitre.org

Oral Statement

Committee on International Relations
United States House of Representatives

Hearing on State Department
Technology Modernization and Computer Security

22 June 2000

Good morning. My name is Dr. Mark Maybury. I am Executive Director of the Information Technology Division at MITRE where I coordinate the MITRE Corporation's work on collaboration technologies. For the past 5 years I also have served as the Chair of the Defense Information Infrastructure Common Operating Environment (DII COE) Multimedia and Collaboration Technical Working Group (MCTWG). I will summarize my prepared statement which I would like to have made part of the formal record. Thank you for the opportunity to address the Committee on the topic of a common platform for information sharing and management for the Foreign Affairs community. I was asked to comment on the requirement for, impediments to, costs of, and lessons learned from using collaborative computing and knowledge management technologies, which are key enablers of a common platform. I have attempted to address each of these issues in detail in my written testimony. My key points are:

1. **Creating a common operating platform for the Department of State and other agencies is challenging but possible with great benefits**. By common platform I mean those infrastructure and applications that are basic to long distance and cross agency collaboration such as directories, electronic mail, file sharing, desktop video teleconferencing, skills/expert databases, and shared applications. I believe secure collaboration and knowledge management solutions (which I will describe) have promise to directly address some of the fundamental problems outlined in the November 1999 Overseas Presence Advisory Panel (OPAP) report such as increased global complexity, reduced overseas staff, and the need for increased global engagement and influence. For example, Intelink, a "classified Internet" which MITRE helped engineer, has become the primary method of intelligence information sharing for the Intelligence Community (IC). In my written statement, I detail how collaboration technologies have enabled the Air Force to create virtual air operations centers, the Navy and Joint Forces to put Tomahawk cruise missiles on target faster during war, and MITRE to rapidly share its knowledge globally. These systems have improved the timeliness and quality of operational processes. For example, in a major exercise last year, Air Force users reported a 50% improvement in efficiency of operations. With focused effort, the Foreign Affairs community can enjoy these same benefits.

2. **Success of a common platform for the Department of State will require both collaboration and knowledge management technologies**. *Collaboration services* are those technologies that enable people to share information, communicate, and coordinate across the boundaries of time and space. This includes supporting teams working at different times and places (e.g., using email). It also includes teams working at the same time but in different places (e.g., using instant messaging, and desktop videoconferencing). *Knowledge management* can be enabled by collaboration services, however, it refers to a process which includes knowledge and expertise discovery (e.g., via directories and skills databases), knowledge mapping, knowledge integration and knowledge dissemination.

3. Because of the difficulty of predicting how people and organizations will use collaboration tools and the rapidly changing underlying communications, networking and computing infrastructure, **it is essential that the creation of these systems be done in what is called an "incremental, spiral acquisition process"**. In contrast to the waterfall approach where development of a system follows a strictly sequential process of requirements to design to implementation to testing, the spiral approach uses more of a process in which refinements in requirements/design/implementation/testing are accomplished in parallel. Accordingly, the government needs to depart from its "normal" lengthy purchasing process and build a little, test a little, learn from mistakes and be willing to adapt to change. Planned obsolescence is part of this process and these systems can be very costly. Costs should address life cycle costs to include acquisition cost, implementation costs (e.g., communication, training, system administration, process change), steady state costs (e.g., re-training, support), as well as indirect costs, including such intangibles as downtime and user satisfaction. While a spiral development process does not guarantee an inexpensive solution, it does minimize the risk that money will be wasted. Success in creating a secure common platform for the Department of State and other agencies requires clarity of vision, buy-in from the Foreign Affairs community, explicit and measurable business outcomes, but flexibility in technology, schedule, budget, and specifications.

4. **These networked systems pose new security challenges that the government will need to address in a comprehensive fashion**. Beyond physical and personnel security risks, risk is introduced as a result of vulnerabilities in the communications and network infrastructure as well as a lack of built-in security features in applications that run on them (e.g., directories, email, desktop video conferencing). Risks include but are not limited to:

   - access by unauthorized users
   - unauthorized personnel posing as legitimate users (called "masquerading"),
   - vulnerability to various viruses, Trojan horses, and so on (e.g., exemplified by the recent .com distributed denial of service attacks and "I LOVE YOU" virus).

   The State Department can protect its enterprise using several technologies in use today that mitigate these risks:

   - Create closed sub-networks using technologies such as Virtual Private Networks (VPN) and incorporate Secure Session Layer (SSL) enhancements for authentication and encryption of application sessions (used increasingly for electronic commerce).
   - Deploy firewalls that restrict access to our networks.
   - Enforce the use of strong authentication (as opposed to weaker user id and password schemes) that requires a Public Key Infrastructure and the generation of digital certificates.
   - As they become more reliable, make greater use of biometric devices for reading

fingerprints or performing retinal scans.
- Be vigilant about virus scanning and network scanning to uncover vulnerabilities that might make networks more susceptible to attack.

These and other strategies are in use today to mitigate some of these risks; however they are predominantly point solutions that require a great deal of time and effort to engineer and administer. Secure solutions for collaboration remains an active research topic

5. The MITRE Corporation's experience working with a broad range of government organizations is that **it is essential to work cross agency information technology governance issues up front** (e.g., possibly via the Federal CIO Council). The planning and implementation organization that creates a common platform for the Foreign Affairs Community would ideally have the following characteristics:

   - Acquisition excellence (e.g., successful experience with spiral acquisition and technology insertion)
   - Systems engineering expertise (e.g., architecture, integration, migration).
   - Technical depth (specifically in collaboration services and knowledge management)
   - Cleared staff (e.g., secret, top secret, secure compartmented access)
   - Domain knowledge of overseas presence
   - Preferably overseas presence and/or projection
   - Strong contractor base and contractor oversight

6. **The best collaboration and knowledge management systems won't make people collaborate**. To be sure, a stable, secure communications and networking infrastructure and effective applications are essential. However, collaboration is fundamentally driven by a need to solve a common problem or perform a joint task. In other words, it is mission driven and technology enabled, not technology driven. Executive level championship, including clear vision and explicit measured objectives, and a culture reinforced by incentives are necessary to foster knowledge sharing and teams. This is particularly true in this case where collaboration must occur across great distances and across agency boundaries and cultures.

7. **Finally, the true magic in collaboration is enabled by cultural change -- moving from a management style of command and control to one of coaching and cultivation ... moving from a culture of independence to one of interdependence.** Most current organizational cultures support a management style that is more akin to playing football where a single individual is in control. In contrast, collaborative and knowledge enabled enterprises are more likely to operate like soccer, a more distributed game in which individual players have positions and locations but they can each be in control of the direction of the ball at any given point. However, there is a profound difference in the style of play, e.g., the degree of dependence on the quarterback to call the plays in football vs. the interdependence of the soccer players.

So to summarize, there are a few key items for success:

- First collaboration and knowledge management technologies offer great promise for helping to create a common platform to enhance our overseas presence.
- Second, these must be secure to manage risk.
- Third, success comes from an incremental, step by step creation of a solution with measured milestones toward a clear vision.
- Fourth, you need qualified experts and organizational commitment to make this succeed.
- Finally, cultural change is required to fully realize business process improvements.

While success is hard, the results are worth it. Collaboration and knowledge management are new and complex technologies that require special attention as their success is both dependent upon and can enable positive organizational change. I believe that through the establishment of a secure, common platform we can enhance our overseas presence through prudent application of collaboration and knowledge management technologies. I thank you for your attention and would be happy to answer any questions.

6

A Common Platform for the Foreign Affairs Community: Collaborative Computing & Knowledge Management

Dr. Mark T. Maybury
Executive Director
Information Technology Division
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
maybury@mitre.org
www.mitre.org

Prepared Statement

Committee on International Relations
United States House of Representatives

Hearing on State Department
Technology Modernization and Computer Security

22 June 2000

Good morning. My name is Dr. Mark Maybury. I am Executive Director of the Information Technology Division at MITRE where I coordinate the MITRE Corporation's work on collaboration technologies. For the past 5 years I also have served as the Chair of the Defense Information Infrastructure Common Operating Environment (DII COE) Multimedia and Collaboration Technical Working Group (MCTWG). Thank you for the opportunity to address the Committee on the topic of a common platform for information sharing and management for the Foreign Affairs community. I was asked to comment on the requirement for, impediments to, costs of, and lessons learned from using collaborative computing and knowledge management technologies, which are key enablers of a common platform.

Collaboration and Knowledge Management

Collaboration technologies are those technologies that enable people to share information, communicate, and coordinate across the boundaries of time and space. The collaboration commercial marketplace has been evolving over the last ten years, initially delivering technologies that provided *asynchronous* (i.e., different time) communication such as email. In the past five years we have seen a rapid growth in *synchronous* (i.e., same time) conferencing such as (room and desktop) audio/video conferencing and/or text chat as well as shared data and/or application control, such as found in shared whiteboarding and application sharing. More recently, several commercial companies have offered *place-based collaboration environments* to support virtual meetings/virtual collocation. There are a range of adopted and emerging International Telecommunication Union (ITU), Internet Engineering Task Force (IETF) and other standards that I would be happy to describe in the future if that is of value.

In contrast, *knowledge management* relates to the process of knowledge and expertise discovery, knowledge mapping, knowledge integration and knowledge dissemination (Morey et al. 1999). Knowledge management and associated systems are very much in their infancy, although already many commercial companies have active knowledge management programs. In addition commercial products and Internet services are emerging to provide expert/skill finding (Fenn 1999; Mattox et al. 1999) as well as tools for automated knowledge mapping of corporate information. A distributed/delegated model of knowledge stewards seems to be an effective strategy.

Collaboration and knowledge management *solutions are emerging rapidly*. The Gartner group has predicted (Gartner Group, 19 July 1999) that by 2002 "synchronous collaboration technologies [are] expected to be deployed by 70% of technology driven enterprises and 30% of moderate technology adopter enterprises." They subsequently predict the explosion of real time data conferencing applications to over 10 million users by 2002 (Gartner Group, October 1999 and Collaborative Strategies, 1999).

To be successful, both collaboration and knowledge management technologies require a

cultural shift. I'm sure the Panel knows well the need to rapidly establish global, multidisciplinary teams to address growing transnational threats in ever changing, complex, dangerous world. Future teams need to be secure, fast and agile (i.e., retaskable, coordinated, precise), decisive in a dynamic, complex, uncertain world, and knowledge superior.

Most current organizational cultures support a management style that is more akin to playing football where a single individual is in control. In contrast, collaborative and knowledge enabled enterprises are more likely to operate like soccer, a more distributed game in which individual players have positions and locations but they can each be in control of the direction of the ball at any given point. However, there is a profound difference in the style of play, e.g., the degree of dependence on the quarterback to call the plays in football vs. the interdependence of the soccer players. (You might realize by now that my two sons play soccer and not football).

Planning for Success

How much planning is required before you implement a knowledge management/collaborative computing approach?

In our experience, it is perhaps more useful to have clearly stated and achievable business objectives/outcomes that will drive change than it is to have detailed requirements stated up front. It is important to start. While it is useful for benchmarking purposes to baseline current processes, one primary value of collaborative environments is their ability to revolutionize current business practices. For example, they can facilitate changing serial processes to parallel, enable time and place distant experts to work together, and reduce the number of forward deployed personnel by enabling "reachback" to CONUS. Architecting these systems requires details of the number, type and location of organizations and also the way in which they are expected to communicate and interact in the "to be" as opposed to "as is" configuration. To be sure, successful software/human systems deployments require at least: robust communications, infrastructure services that are consistent with the tasks and needs of users, enterprise security, effective user training, and sustained support. In addition, the successful deployments of collaboration environments have a number of common elements: an executive level champion, direct user engagement, rapid and iterative "spiral development" and compelling business goals that drive cooperative work.

One useful organizing conceptual framework is to think of various levels of collaboration. At the lowest level users have awareness of one another (e.g., they know who is where with what communications capabilities and/or skills, possibly via directory services and/or yellow pages) as well as situational awareness (e.g., they know what events and activities are occurring). At the next level, users regularly share information with one another. Beyond this, they may actually coordinate their actions (e.g., timing actions to occur so they are synchronized with a partner's action). Finally, they may plan

and execute efforts jointly, ultimately to alignment of objectives consistent with the commander's intent. Moving up these levels of collaboration implies increased interaction among individuals, groups, and organizations as well as the additional time and resources that increased interaction implies.

Impediments to Success

What problems (e.g. bandwidth, network management, security, etc.) might we face when applying this approach at 260 overseas posts for the 40 agencies who use the posts)?

At the DoD and Intelligence Community workshop on Collaboration and Knowledge Management in May 2000, a group of experts from industry and government identified high level leadership, security policy and procedures, and infrastructure as key impediments to the success of these systems. When we began helping the government deploy collaboration solutions several years ago we thought the challenges would be, in decreasing order of difficulty, infrastructure, security, and culture. In fact, while all were indeed challenges, the degree of difficulty was just the opposite. Additionally, scalability, training & access to expert and cleared personnel overseas, and heterogeneity of networks and users will be special challenges for OPAP.

In terms of success, we use the acronym UNITE to indicate the necessary elements for collaboration success. The "U" stands for Unified purpose. It is essential for a team (within or across organizations) to have a shared goal otherwise they will have no desire to work together. No amount of technology can undermine or overcome people's attitudes. The "N" in UNITE stands for Network security. Connecting everyone up means that it is essential we secure the network, authenticate users and audit usage. Public Key Infrastructures and Virtual Private Networks are important enablers in this regard. The "I" in UNITE stands for the Infrastructure to enable the success as well as Incentives to value team collaboration. The "T" is for creating an environment of Trust. Finally, the "E' means we need to Empower the Executive level of support. Failures in any one of these areas can dramatically effect the success of a collaboration environment. However, the rewards from success can be rather dramatic, as I will describe in a few exemplary case studies below.

Security

What are the security risks with a project of this nature?

There are several key areas of security risk in deploying a common platform for the Department of State. Beyond physical and personnel security risks, which I will not address, risk is introduced as a result of vulnerabilities in the communications and network infrastructure as well as a lack of built-in security features in applications that run on them (e.g., directories, email, desktop video conferencing).

Last month, MITRE President and CEO Martin Faga and John Woodward, Director of Information Warfare, testified at the U.S. Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities. The subcommittee meeting was held to discuss ways the private and public sectors can work together to combat cyber attacks. I refer you to the details of that testimony which outlined a number of risks and some work MITRE and others are carrying out to mitigate those risks.

Security risks include, but are not limited to, access by unauthorized users, masquerading, and vulnerability to various viruses, and Trojan horses. There are several strategies in use today to mitigate some of these risks; however they are predominantly point solutions that require a great deal of time and effort to engineer and administer. Secure solutions for collaboration remains an active research topic. For example, we can create closed sub-networks using technologies such as Virtual Private Networks (VPN) and incorporate Secure Session Layer (SSL) enhancements for authentication and encryption of application sessions (used increasingly for electronic commerce). We can deploy firewalls that restrict access to our networks. We can enforce the use of strong authentication (as opposed to weaker user id and password schemes) that requires a Public Key Infrastructure (PKI) and the generation of digital certificates. As they become more reliable, we can make greater use of biometric devices for reading fingerprints or performing retinal scans. We can be more vigilant about virus scanning and network scanning to uncover vulnerabilities that might make our networks more susceptible to attack.

A special risk is introduced by the desire to have bandwidth-efficient communications when using desktop audio and video conferencing across large enterprise networks, such as the one State envisions. In particular, networks that support multicast (one-to-many-transmissions) are recommended for efficient bandwidth use. Simply put, if the Secretary of State wants to broadcast real-time audio or video to all employees worldwide in real-time, multicasting (vs. unicasting) those packets would minimize the impact on networks that may already be bandwidth-constrained. Using a multicast approach, a collection of audio or video packets could be transmitted to each site that would then be distributed locally to the intended recipients. Sending packets in this manner would avoid the duplication of communication costs that would occur in a traditional unicast scheme. Multicasting can be implemented natively by configuring routers to support this scheme. For routers that don't suport native multicast, we can "tunnel" packets, that is, bypass network routers using specialized communications software, although this requires additional system administration. Although it is an efficient way of transmitting packets when high bandwidth applications are being used, multicasting relies on the use of the User Datagram Protocol (UDP) as the network transport protocol. Typically, firewalls are configured to block UDP as it is a connectionless protocol and transmissions cannot be managed reliably. As a way around this problem, VPNs are often used in conjunction with route encapsulation techniques to pass multicast data through a firewall with *less* risk. Connecting sites via a VPN can reduce the security of sites within the virtual network to the security level of the least secure site. That is, attackers could exploit a weak security policy at one site and use the VPN to gain access to systems at other sites

within the VPN and possibly beyond.

In summary, there remain several impediments to collaborating securely. First, collaboration standards and protocols (see Appendix B for definitions of these and other standards) are inherently insecure (e.g., ITU H.323 for conferencing, ITU T.120 for data sharing, UDP, and multicast). Second, mature, comprehensive firewall proxies for collaboration protocols do not exist (e.g., Multicast, T.120, H.323). Third, there is a lack of application-level security features that provide for strong authentication (e.g., using digital certificates, tokens), access control and privacy (encryption). Fourth, collaboration rules and policy are hard to define and enforce (e.g., coalition collaboration, inter-agency collaboration). Finally, there is the need for expert trained systems administrators. In summary, better standards, more mature proxies, security feature-rich applications and well-trained staff, and ultimately, clearer policy will be needed to mitigate current collaboration security concerns.

Real-World Collaboration Successes

Please describe some real-life experiences at MITRE or other corporations with implementing such approaches. Provide some perspectives on others (like the JIVA project or DOD's information superiority approach) who are trying this and lessons learned.

Collaboration environments have been utilized to enhance operations in multiple services and agencies, including the Army's Task Force XXI, the Air Force Expeditionary Force Experiment, the Navy's Collaborative Contingency Targeting for cruise missile planning, and in the national intelligence community. I have chosen to highlight some activities that illustrate the potential for success using collaboration solutions. These include:

(1) the United States Air Force's Joint Expeditionary Force EXperiment (JEFX) which reduced forward deployed personnel from thousands to hundreds through innovative use of VPNs to enable a secure, virtual air operations center.
(2) the Navy's activity to coordinate mission planning for targeting of cruise missiles between the Cruise Missile Support Activity, Pentagon, CENTCOM and supporting agencies in several recent conflicts.
(3) MITRE's own intranet, which won the CIO magazine Enterprise value Award and includes an explicit ROI in a business context.

The Air Force has been experimenting with place-based collaboration environments since 1996 (i.e., the "Fort Franklin" Experiment). Since the initial single site, ten user experiment, the annual Air Force's Joint Expeditionary Force Experiment (JEFX) has grown to create a distributed, collaborative Air Operations Center including 3 primary sites, 21 fixed, afloat and airborne locations, 1600+ accounts and an average of 300+ concurrent users. The virtual air operations center is used for preparation of Air Tasking

Orders (ATOs), daily Commander briefings, and coordination of Air Operations Center activities. Most dramatic has been the impact on the Forward Joint Air Operations Center (JAOC). Whereas in Desert Storm there were 1500-2000 people in the JAOC, which took 10-15 days to set up with the help of approximately 25 C-141s, the virtual JAOC requires only about 100 staff, can be set up in 24-48 hours, and requires only one C-17 load for support. The operational impact as reported by the users included a 50% improvement in process efficiency in the Attack Operations Cell, 30% time savings in the Targeting Cell and 50% - 80% increase in situation awareness by the Air Defense and Information Operations teams. The Air Force learned that a dynamic collaborative capability is indispensable to distributed operations. They also learned how important it was to incorporate collaboration into their command and control concepts of operations. Their effort was successful because of a multi-function approach incorporating system deployment/management, training/ operations, and networking and security. In December of 1999 the Chief of Staff of the Air Force directed AF/XO to institutionalize distributed operations. The AF continues to experiment with collaboration in Millennium Challenge/JEFX 2000. For more details on the Air Forces operational use of collaboration technologies, contact Col David Tillotson, ESC/FX at (david.tillotson@hanscom.af.mil).

The Navy successfully utilized collaboration services to target the Time Critical Target (TCT) threat, with Tomahawk cruise missiles, during Operation DESERT FOX (in Iraq) and Operation ALLIED FORCE (in Kosovo). Previous serial targeting was cumbersome and time intensive, prone to ambiguities and errors, lacked consensus of other participants, created confusion, and duplicated effort. To simplify the targeting process, the United States Joint Forces Command (USJFCOM) created the Collaborative Contingency Targeting (CCT) system to support the target distribution process. CCT consists of off the shelf tools such as text chat, voice conferencing, and whiteboarding together with shared mission applications (e.g., Matrix, ELT (Electronic Light Table)) and the Mission Planning Request (MPR) from CINCs to planners. The Cruise Missile Support Activity (CMSA) at USJFCOM in Norfolk, VA, used CCT to virtually connect to the United States Central Command (USCENTCOM) in Tampa, FL for Operation DESERT FOX and to the United States European Command (USEUCOM) in Germany for Operation ALLIED FORCE. All players were able to reduce targeting time of certain Tomahawk cruise missile missions from days to an average of six hours, with dramatic reductions in error. In one case, the team was able to put a missile on target in less than two hours from alert, an unprecedented accomplishment. CMSA has since used CCT to virtually connect with multiple players simultaneously, to include USEUCOM in Germany, CMSAPAC in Hawaii, Joint Warfare Analysis Center (JWAC) in Dahlgren, Virginia, the National Imagery and Mapping Agency (NIMA) in St. Louis, Missouri, and deployed aircraft carriers. For further details on this example of CCT success, please contact Captain William Dewes, USN, at (757) 836-7501 (CMSA00@hq.jfcom.smil.mil or unclassified CMSA00@hq.jfcom.mil).

Whereas the above situations address primarily the use of collaboration tools, I would like to provide an example of the deployment of tools that support knowledge

management in a distributed environment. I choose a corporate example with which I am very familiar, namely MITRE's Information Infrastructure (MII). Because nearly a quarter of MITRE's 4000 personnel operate at MITRE sites collocated with service and agency installations across the US and overseas, we have utilized our intranet, its services, and an associated corporate knowledge management initiative as a means for enhancing our efficiency, cost management and service quality. In particular, we have applied a Norton/Kaplan balanced scorecard concept of financial measures assessing customer satisfaction, internal business processes and innovation and learning. To date, our $7.1 million investment has netted an ROI of $62.1 million in reduced operating costs, improved productivity, and cost avoidance. Other cited benefits include increasing the knowledge base and sharing expertise via mechanisms such as expert locators, knowledge repositories, and shared file spaces. For example, in the past year alone, employee use of the latter has gone from 2000 to 3000 and content has increase 10% per month). Our valuation strategy has been cited in CIO Magazine (Young, 2000).

An illustration of effective knowledge management techniques used by the government is the Science and Technology Expert Partnership (STEP) program, managed by the Scientific and Technical Intelligence Committee (STIC). The mission of STEP is to "ensure that scientific and technical analysis for the intelligence community represents considered judgement by the highest caliber experts in the United States." STEP maintains a network of nationally recognized experts from a broad range of scientific and technical areas. STEP facilitates collaboration between experts and intelligence community analysts to create classified and unclassified studies that address important national concerns. This agile form of virtual organization on demand has produced a variety of cost effective results on a number of scientific and technical topics.

Finally, I would like to point out that the Intelligence Community (IC) has recognized the need to capture and learn from past experience. For example the CIA's Office of Advanced Analytic Tools (AAT) is establishing the Collaboration Facilitation Cell (CFC) to further AAT's ongoing support to the IC in the promotion of virtual, electronic collaboration as a competitive business advantage for the IC. The Cell will, among other things, be responsible for independently measuring and evaluating ongoing IC collaboration programs with an eye toward the systematic capturing and sharing of lessons learned and best practices. The Cell will provide direct support to the Assistant Director of Central Intelligence for Analysis and Production (ADCI/AP) in his leadership role for defining future business strategies for IC analysis and production. The Cell will provide support to other IC programs engaged in the proliferation of virtual collaboration, including support to some intra-CIA programs. For more information about the CFC you can contact Jill Singer at (703) 613 7885/7882 (jills@ucia.gov).

Collaboration Challenges

As the market continues to rapidly deliver collaboration offerings, organizations have yet to adopt many of these collaboration services into the enterprise. The state of the

practice in most organizations is with the use of asynchronous collaboration technologies (e.g., e-mail, threaded discussion groups, web/document servers, group calendaring). Adoption of real-time conferencing is occurring at a slower rate than initially anticipated, but is expected to grow in the next few years, with a focus on data conferencing. Gartner Group anticipates that synchronous collaboration technologies will be in use by over 10 million users by 2002. The government is ahead of commercial industry with respect to understanding requirements for virtual collocation, and the demand from commercial industry is expected to follow.

But even in the government, there continues to be more of a focus on pilot programs and limited operational deployments rather than enterprise deployment of advanced collaboration services. Reasons for the slower adoption can be attributed to technical/infrastructure, security, and cultural issues.

In order for an organization to be able to successfully use collaboration technologies on an enterprise scale, the network and systems infrastructure must be able to support the requirements of the collaboration tools. Real-time conferencing requires available bandwidth and quality of service from the network. Some tools require support for IP multicast routing. Organizations must prepare a strategy for managing large-scale rollouts, network advances, administration, training, and support.

To enable cross-organizational collaboration, security policies and security solutions must be in place. Security is often weakly addressed by collaboration tools, requiring organizations to consider additional technologies (such as virtual private networks) and flexibility in security policy and an agreed upon concept of operations to enable collaboration across organizations. This poses a great challenge to adoption of collaboration, beyond challenges we face with technology, since there are no policies in place for supporting virtual organizations.

The most difficult challenge is that of dealing with organizational culture and organizational readiness to change to support collaborative operations. Even if the systems, networks, and security policies are in place, and the collaboration technology is the most capable and robust, it will not be of impact if the members of the organizations do not see a need or do not have a willingness to share information and collaborate. Organizations must work within to create a collaborative culture in the organization and help members to understand the benefits and rewards, how they are expected to work, and how they will be supported. Organizations need to work with staff to understand how to use collaboration technology to improve the business process and realize improvement. Members of the organization should be involved from the beginning in helping to define the concept of operations, understanding the rollout and training process, and evolving organizational goals. More fundamentally, this may require organizational change to fully realize benefits. In the words of Jessica Lipnack & Jeffrey Stamps, Co-CEO's of NetAge, "We can't solve 21st century problems with 19th century organizations."

All of these challenges in implementing collaboration take time, careful planning, and come with an associated cost. Piloting and early experimentation, with a plan to build upon lessons learned and expand to more members of the organization, can help to ease the rollout process. Organizations should expect failures, but examine them closely to understand the causes, so that the next iteration can become more successful.

Cost

How much money is involved or commitment (is it short or long term; does it require a change in culture; is there a chance that costs could escalate)?

Cost and schedule overruns are unfortunately more common than not in complex software and system acquisition. The 1999 Standish Group Chaos Study of software projects discovered on average that only 16% complete on time and within budget, 31% are cancelled, and the remaining 53% have cost growths exceeding 89%. On average, the final product contains 61% of the originally-specified features. At the same time, organizations have actually been able to do far more with less.

Collaboration is a major undertaking for any organization as is evident from the above. There are a number of organizations that have successfully deployed collaboration solutions so the effort is not unprecedented, although only a few organizations have done so at the scale and complexity OPAP seeks to address. However, the opportunity cost and possible increased risks of not deploying collaboration may to be too high a price to pay.

While we are not aware of any existing government or commercial cost analyses for collaboration or knowledge management (except for the MII cited above), there is a wealth of information technology life cycle cost analyses from which we can glean effective methods for cost analysis. Notably, a costing method should address life cycle costs and ensure the cost model considers both direct and indirect costs, including such intangibles as downtime and user satisfaction. Cost models need to incorporate acquisition cost, implementation costs (e.g., training, roll out), and steady state costs (e.g., re-training, support).

New Opportunities

A networked, collaboration, and knowledge-enabled enterprise provides a number of opportunities. For example, the information security threats against our foreign installations are probably as great if not greater than the physical ones. Eavesdropping, disruption, and/or distributed denial of service attacks against our Embassy communications pose a real current and future threat. The ability to network together in-place monitoring stations to support distributed collection, centralized processing, and analysis by experts regardless of their location could enhance reporting timeliness, coverage, and quality (by supporting analysis by experts and correlation across sites for enhanced indications and warnings).

Agencies to Lead the Acquisition

While it would be inappropriate for me to make a specific recommendation of which agency should lead the creation of a collaboration/knowledge management system for the State Department and other agencies, the ideal agency would have the following characteristics:

- Acquisition excellence (e.g., successful experience with spiral acquisition and technology insertion)
- Systems engineering expertise (e.g., architecture, integration, migration).
- Technical depth (specifically in collaboration services and knowledge management)
- Cleared staff (e.g., secret, top secret, secure compartmented access)
- Domain knowledge of overseas presence
- Preferably overseas presence and/or projection
- Strong contractor base and contractor oversight

Summary

In summary, a common platform for the Foreign Affairs community needs to address collaboration and knowledge management, both in technology and organizational process. With clear objectives, effective incentives, and careful governance, a common platform can improve existing processes, moving them from serial to parallel and reducing forward footprints and the associated costs and risks. Moreover, they can enable new, joint, and agile processes that can result in reduced cost and time lines, enhanced situational awareness, and improved mission execution. However, infrastructure, security, and culture are challenging technical, human, and organizational problems that require attention, time, and resources.

I thank you for the opportunity to share with you my insight and I hope the panel will find my testimony useful in advancing our missions overseas.

References

Fenn, J. 1999. Skill Mining: An Emerging KM Technology. Gartner Group Report.

Gartner Group reports on Collaborative Strategies, 19 July 1999 and October 1999.

Hall, T. 2000. Intelligence Community Collaboration Baseline Study. CIA/AAT. http://collaboration.mitre.org/prail/IC_Collaboration_Baseline_Study_Final_Report/toc.htm

Mattox, D., Maybury, M., and Morey, D. 1999. Enterprise Expert and Knowledge Discovery. Proceedings of 8th International Conference on Human-Computer

Interaction (HCI International '99), August 22-27, 1999, Munich Park Hilton, Germany. pp. 303-307.

Morey, D.; Maybury, M. and Thuraisingham, B. editors, Fall 2000. *Advances in Knowledge Management: Principles and Practice*. Cambridge: MIT Press.

Young, D. 2000. An Audit Tale: In a post-implementation audit of its intranet, MITRE Corp. focuses on the benefits of knowledge sharing and collaboration. In *CIO Magazine*, May, 2000. pp. 151-158.

Appendix A: Resources

A couple of resources may be valuable to the committee. First, as a consequence of a recent MITRE-sponsored executive summit on collaboration, government participants asked MITRE to compile a web site, collaboration.mitre.org, that captures in an unclassified and publicly released fashion, some of our and our sponsors most recent lessons learned, in addition to pointers to collaboration resources. A special issue of MITRE's Edge advanced technology newsletter on collaboration (www.mitre.org/pubs/edge_perspectives/february_00/index.htm) and another on knowledge management (www.mitre.org/pubs/edge/april_00/index.htm) are available on line. These materials address problems and some solutions based on experiences across several services and agencies.

Second, shortly MIT Press will publish a knowledge management collection (Morey, D.; Maybury, M. and Thuraisingham, B. editors, Fall 2000. *Advances in Knowledge Management: Principles and Practice*. Cambridge: MIT Press) that includes classic papers and current organizational case studies encompassing strategy, process, and benchmarking of knowledge management solutions. Some of the state of the art KM strategies are put forward by such recognized experts as Senge, Nonaka & Takeuchi and Kaplan and Norton.

Appendix B. A Holistic Approach

This appendix outlines some hard lessons learned from many collaboration experiences – both successes and failures. One of the most important lessons to learn about successful collaboration and knowledge management solutions is that their success requires systemic attention. The range of issues that needs to be addressed has been alluded to above and includes:

Communications and Networking. Stable and reliable communications and networks are essential to effective collaborative computing and this requires continuous monitoring and intervention. Moreover, efficiency in multiparty collaboration, particularly when using bandwidth intensive services such as audio and video requires use of technologies such as multicasting to enable more efficient use of bandwidth by minimizing replication of packets. Voice and video conferencing require consistent jitter variation which

networks do not provide. Quality of service features can significantly minimize impact of bursty network congestion and permit better selective performance, although these technologies are still maturing and not yet broadly deployed.

Scalability. The above successes illustrate the need to support thousands of users, and hundreds of simultaneous users. Often solutions will work with a few participants but fail with many. Technologies such as multicasting can help, however, federating collaboration servers and other approaches are often required to ensure high performance.

Security. Impediments to collaborating securely include that fact that standards and protocols are inherently insecure (e.g., H.323, T.120, UDP, Multicast), there is a lack of firewall proxy support (e.g., for Multicast, T.120, H.323), and that most tools lack application-level security features such as strong authentication (digital certificates, tokens) and privacy (encryption). In addition, collaboration rules and policy are hard to define and enforce (e.g., coalition collaboration, inter-agency collaboration). There are a number of collaboration enablers including the use of virtual private networks to mitigate risk by enabling encrypted, authenticated communications. However, security is only as good as the "weakest link" with this approach which has lead to research in secure collaboration (for conferencing, document repositories, and data sharing) as well as better standards, proxies, and products.

Standards and Interoperability. While standards for data sharing (T.120) and conferencing (H.323) exist, not all commercial products support these standards. Standards compliance does not mean interoperability. Moreover, important standards for rooms (ITU T.137) and awareness (IETF IMPP) are still emerging and require reconciliation across standards organizations. As another example, IDC (January 1999) predicts heavier weight ITU [International Telephony Union] data conferencing standards will be challenged by lighter weight "web-friendly" approaches. Table1 below summarizes key collaboration services and standards. Also important are directory services (LDAP), certificates (X.509) and file transfer (T.127) standards.

Service	Standards	Approved	JTA 3.0	COTS
Session Management	ITU T.120	1995-	Yes	Many
Text Chat	IETF RFC 1459 ITU T.120/T.134 IETF IMPP	Defacto IRC 1998 Emerging	No Yes No	Freeware Many None
Audio/Video Conferencing	ITU H.323; V: H.261, H.263 A: G.711, G.723.1, G.729; ITU H.320 ISDN Gateway IETF draft RFC 2543 VOIP	1996 1996 1990 Emerging	Yes Yes Yes No	Many Many Many None
Shared whiteboard	T.120/T.126	1995	Yes	Several
Application sharing	T.120/T.128	1998	Yes	Several

Rooms & Context Management	T.120/T.137 (MRM) MCP	2000 Defacto	Yes No	None Freeware

Table 1. Collaboration Services and Standards

Cost Effectiveness. Pricing of collaboration tools range from free to tens of dollars per seat to hundreds of dollars per seat. The predominant costs are often hidden, however, in the communications, networking, training, and sustaining support for such tools.

Culture. Successful collaboration requires managerial incentives for information sharing, teaming and joint efforts. High level leadership support and commitment is essential. This includes training in human/group processes (e.g., shared leadership) and changes in policy, procedures, and incentives (e.g., group awards, recognition and rewards for collaboration).

Attachment C. MITRE Corporate Overview

The MITRE Corporation is an independent, not-for-profit company that provides technical support to the government. Working in the public interest, MITRE operates as a strategic partner with its sponsoring government agencies. This relationship imposes some constraints on MITRE's business practices, but permits a degree of access and a long-term perspective not available to commercial contractors who compete for government business. Within this relationship, MITRE is able to address complex technical problems of critical importance to its sponsors with a breadth and depth of expertise beyond that available inside the government. A strong information technology base and an integrated systems approach support all of MITRE's work.

The Corporation manages three Federally Funded Research and Development Centers (FFRDCs). These Centers support systems engineering and integration work for Department of Defense (DOD) command, control, communications and intelligence (C3I), systems research and development work for the Federal Aviation Administration (FAA) and other civil aviation authorities, and systems engineering for the Internal Revenue Service (IRS).

Under the primary sponsorship of the Assistant Secretary of Defense for C3I, the Air Force and Army are sponsors of the DOD C3I FFRDC. This Center supports the national security and intelligence community with technical work on command, control, communications, computers, intelligence, surveillance and reconnaissance, by applying its core competencies of "system-of-systems" engineering, systems development and acquisition, process implementation, architectures and interoperability, and technology application. In order to serve as an objective, impartial link between its government sponsors and commercial vendors, the C3I FFRDC does not compete with profit-making organizations, work for the private sector, or manufacture products.

The Center for Advanced Aviation System Development (CAASD), sponsored by the FAA Administrator, is the FAA's FFRDC. CAASD specializes in the analysis, operations, and technologies of advanced air traffic management systems. CAASD supports its clients with a unique combination of operational knowledge, state-of-the-art understanding of technology, advanced laboratory capabilities, and a top-down view of the entire national airspace system. In order to preserve objectivity and impartiality, CAASD does not manufacture products and works with the private sector only as directed by its sponsor.

Under the IRS FFRDC, MITRE provides strategic, technical and program management advice to the IRS and Treasury Department, focusing on work supporting the modernization of the nation's tax administration system.

MITRE employs approximately 4,500 technical and support staff at its headquarters in Bedford, MA, and Northern Virginia, and at more than 60 sites throughout the world.

Dr. Mark Maybury

Dr. Maybury is Executive Director of the Information Technology Division at The MITRE Corporation where for the past ten years he has created, applied, and evaluated collaborative computing and knowledge management initiatives both within the private and public sector. Since 1995, Dr. Maybury has served as the chair of the Defense Information Infrastructure Common Operating Environment (DII COE) Multimedia and Collaboration Technical Working Group (MCTWG). This group is responsible for:

1. maintaining the cross-service, cross-agency DII COE collaboration Software Requirements Specification (SRS)
2. Making recommendations to the COE Chief Engineer regarding collaboration standards, and
3. Assessing how tools and technologies satisfy these requirements to ensure an effective, affordable, and interoperable infrastructure.

Dr. Maybury is a member of the Board of Directors of the Object Management Group, a consortium of 800+ companies that collaborate to create interoperable object based software solutions. Dr. Maybury has edited or co-edited 5 books and written over 50 journal articles. http://www-i.mitre.org/resources/centers/it/maybury/mark.html

Additional References

Anderson, M., Smith, C. (1998) IEW Scenario: Virtualizing the Office. *Gartner Group*.

Brett, J.M., Rognes, J.K. (1986). Intergroup relations in organizations. In *Designing Effective Work Groups* (Ed: P. Goodman and Associates). Jossey-Bass Publishers: San Francisco, p202-236.

Davidson, J., Deus, L. (1998) A Case Study in Technology Transfer of Collaboration Tools. *The Edge*. http://www.mitre.org/pubs/edge/june_98/sixth.htm

Grudin, J. (1994). Groupware and Social Dynamics: Eight Challenges for Developers. *Communications of the ACM*, 37 (1): 92-105.

Grudin, J. (1994). Computer-Supported Cooperative Work: History and Focus. *IEEE Computer*, 27 (5): 19-26.

Harris, K. (1998) The Quest for Collaboration: How to Know When It Happens. *Gartner Group*.

Harris, K. (1998) Will Job Performance Benefit From KM? *Gartner Group*.

Orlikowski, W.J. (1992) Learning From Notes: Organizational Issues in Groupware Implementation, *MIT Sloan School Center for Coordination Science*, http://ccs.mit.edu/CCSWP134.htm

Poltrock, S.E., Engelbeck, G. (1997) Requirements for a Virtual Collocation Environment. In *Proceedings of Group 97*, p61-70.

Web References

1. Collaboration Portal - http://collaboration.mitre.org
2. Collaborative Computing Collections - http://www.csc.liv.ac.uk/~team-it/collect.html
3. International Telecommunications Union (ITU) - http://www.itu.ch
4. International Multimedia Teleconferencing Forum (IMTC) - http://www.imtc.org
5. Internet Engineering Task Force (IETF) - http://www.ietf.org
6. IP Multicast/MBONE - http://www.mbone.com/, http://www.ipmulticast.com, http://www.ipmulticast.com/community/whitepapers/
7. T.120 and H.323 Primers - http://www.databeam.com/h323/h323primer.html , http://www.databeam.com/ccts/t120primer.html , http://www-us-east.intel.com/technology/itj/q21998/articles/art_4.htm, http://www-us-east.intel.com/technology/itj/q21998/articles/art_5.htm
8. H.323 and Firewalls - http://support.intel.com/support/videophone/trial21/H323_WPR.HTM
9. Netmeeting and Firewalls - http://www.it.hq.nasa.gov/~cshenton/hq/netmeeting/