

Technologies for the Mobile User

- C. Christian, R. Denniston, G. Galloway (IRM/BPC/eDip) 25 June, 2004

Introduction

The Office of eDiplomacy (IRM/BPC/eDIP) is chartered to “*Enhance the Department's leadership in American diplomacy by promoting a knowledge-sharing culture and by putting the power of innovation in technologies and practices at the fingertips of the individual user.*” To this end, eDiplomacy works with users to identify their needs and values and broker technological solutions. One pressing area of concern is the implementation of a mobile technology program.

The mobility of Department of State (DoS) users is increasing and quickly outstripping the deployment of adequate technology to meet their demands. By placing personnel in the field without up-to-date resources and deprived of key information access, diplomats and other State employees are less productive, less effective, and, in fact, can be placed in unnecessary jeopardy. As technology implementation slows, the gap between capability and need widens. Colloquially, we know that a climate of desperation is encouraging users to find alternative means to exchange information (e.g., commercial email services, etc.). As the gap widens between resources and user needs, a far greater risk to DoS business than the perceived risk associated with remote access looms ahead.

This paper addresses eDiplomacy's method for addressing the large need for mobile technologies within the Department of State.

Defining the Business Need

The DoS deploys a significant number of employees overseas, as do other agencies. This distributed personnel costs money, involves risks, and creates a challenge in communication. To achieve State's mission: *Create a more secure, democratic, and prosperous world for the benefit of the American people and the international community*, it is important for this workforce to be distributed globally. Diplomats need to be interacting within their host countries including “getting out and about”. Alternatively, by conducting operations solely from an office, there is little justification for State employees to be located anywhere but Washington. Placing diplomats in the field without access to information puts them at risk, and dilutes the effectiveness of the diplomatic service and the Department in general.

Considering the global situation today, there exist additional possibilities that physical spaces will be vacated periodically due to weather, disasters, terrorist activities, logistics, and a host of other causes. The business of the DoS can ill-afford to halt merely because some office buildings are periodically and unpredictably unavailable. Emergency preparedness is a pressing concern at the federal, state, regional, and local level.

In addition, as a subset of the above considerations, the DoS, as other federal agencies, are bound to certify that 100 percent of *eligible* employees have the option to telecommute as per 2001 Transportation Appropriations Measure (PL 106-346). Currently the number of State employees reported as “telecommute-enabled” is less than 2%. The requirement for conformance may soon come with significant fiscal penalties, if actions in the House Appropriations Committee are carried through (c.f., S. Barr, 2004, Washington Post <http://www.washingtonpost.com/wp-dyn/articles/A1059-2004Jun23.html?nav=headlines>).

The only conclusion that can be drawn is that diplomats and many other DoS employees require mobile access to information, including human resources. It behooves the Department to join other federal agencies in enabling its workforce to continue business at “anytime, anywhere”.

Delineating Technology Needs

Typically the technologies used to provide mobile access are loosely lumped under the terminology “mobile computing”. A stricter definition of **mobile computing** is: “using a portable computing device while in transit or in a remote location”. Because our applications are broader than computing and are centered on the need to have mobile *access* to information, including human expertise, the term “mobile technologies” is used herein. Mobile technologies, therefore, enable mobile users to access the information they need when then need it. Mobile technologies include but overarch mobile computing.

The requirements for mobile technologies are derived from a user-centric point of view. Specifications must capture the work environment and needs of users, so that affordable, sensible solutions can be implemented.

Characterizing the User Environment

DoS users need to work in a variety of environments and access resources through various infrastructure. These places include:

- Specific recurrent locations away from the work place (home, second office, telework centers, etc.)
- Other random locations (hotels, meeting venues, airports, café’s etc.)
- In transit (train, car, other transportation, in the field)

Users need reliable access at random times not necessarily correlated with specific places.

Required environments may be at a variety of levels of security from insecure to highly secure.

Describing Access Needs

Users have a wide plethora of access needs, depending upon time, location, and profile of the user as well as the specific tasks being accomplished. These access needs include:

- Global access to unclassified e-mail. Access includes but is not limited to viewing information, responding to messages, modifying material and printing it
- Access to calendars, contact lists and tasks from a wide variety of computers located outside the DoS network without special equipment or software
- Access to e-mail and calendars through wireless devices
- Access to personnel through phone, video conferencing, and teleconferencing
- Access to remote events through video or audio
- Access to all OpenNet resources, including but not limited to the DoS Intranet, AIDNet and OSIS, and to network files and applications by authorized end-users from as wide a variety of computing devices as possible
- Expansion of access to ClassNet information as options become available; e.g., through SIPRNet
- Full access to ON+ from any USG-owned equipment and facilities including GSA telework centers
- Single logon identification and password for ON+ and for ClassNet that can be used from any workstation on the network without administrator intervention
- Upload/download of textual, graphical, audio, digital imagery and video to local or centralized computing services depending upon need
- Geo-referencing of materials (e.g., GPS or coordinate tagging)

The user values associated with these needs are:

- Users have ubiquitous access to information and human resources necessary for their work.
- Jobs are accomplished better and faster through appropriate software and hardware tools.
- Corporate information, including substantial legacy knowledge, is accessible when needed.
- Workflow can be streamlined through incorporation of material into a corporate or enterprise system allowing rapid, up-to-date access.
- Systems are easy to utilize, as well as stable, and robust. Solutions will not be used if they are technically or logistically difficult or cumbersome.
- Tasks are accomplished with agile systems, independent of the vagaries of the hardware device. Device independence allows different tasks with varying degrees of complexity and device requirements to be accomplished without retooling.
- Contiguous task performance is independent of network connectivity. Users need solutions that allow tasks to continue, without loss of work in spite of with intermittent network connections.

- Leverage of and access to existing corporate investments and enterprise systems occurs without custom redeployment.
- Contiguous future IT investment and evolution and improved IT support is built in to solutions from the outset.
- COTS solutions are available where possible for commonality with other agencies, private enterprises and NGOs to facilitate sharing of information and critical project resources as applicable and appropriate.
- Users are assured that growth and future demands are met with scalable solutions from the outset thereby avoiding retooling.
- Rational security solutions provide integrity and protection without seriously degrading performance.

Considering the Stakeholders

Every facet of the DoS mobile technologies program must include the interests and participation of Stakeholders and end users. EDiplomacy brokers solutions by bringing to the table various stakeholders and users to identify common needs and values. These stakeholders and users include:

- Posts and consulates: Interest from ambassadors and other personnel, especially as articulated through the New Diplomacy Task Force.
- Virtual consulates: interest from posts supporting virtual consulates
- Regional Bureaus
- The Bureau of Legislative Affairs (H): keenly interested in anytime, anywhere access and wishes to participate in pilot testing.
- Economic and Business Affairs (EB): has significant technological know-how, presses for anytime anywhere access, and strongly desires to participate in pilot testing
- Courier Service: participating in pilot testing mobile laptop/satellite connections in Central Europe. Desire less cumbersome connectivity
- Telecommuters: desire simple, responsive connectivity
- Diplomatic Security (DS/OFM): needs anytime, anywhere access as soon as practical

The Role of Diplomatic Security and Information Assurance

(DS provides information on possible risks, IA maps the matrix of risk, contingencies, likelihood and implications of acceptance of risk. They provide *information*, not approval)

Confer with Other Agencies

(discussions with other knowledgeable agencies)

Define Mobile Technologies Program
(Strategy for funding)