PUBLIC SAFETY PSWN PROGRAM WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Additional Pilot Project Compilation Report—Secure Paging Pilot for the Washington, DC Area

FINAL

MAY 2002

Table of Contents

EXECUTIVE SUMMARY **1**

1. INTRODUCTION **1**

1.1 Background 1
1.2 Purpose 1

2. SECURE PAGING PILOT TECHNOLOGY **3**

2.1 Introduction 3
2.2 Background 3
2.3 Paging Units 3
2.4 V-One Corporation 4
2.5 Qwest Communications 5
2.6 Secure Two-Way Paging Network 6
2.7 Sequence of Steps 8

3. PILOT APPROACH **9**

3.1 Planning 9
3.2 Procurement 10
3.3 Testing and Analysis 10
3.3.1 Phase I Testing 11
3.3.2 Phase II Testing 12
3.3.3 User Information Survey 14
3.3.4 Call Usage Information 14

4. KEY FINDINGS **15**

5. CONSIDERATIONS FOR FUTURE IMPLEMENTATIONS **18**

APPENDIX A – MEMORANDUM OF UNDERSTANDING **A-1**

APPENDIX B—TEST PLANS AND RESULTS **B-1**

APPENDIX C—TEST ISSUES AND RESOLUTIONS **C-1**

APPENDIX D—USER INFORMATION SURVEY **D-1**

APPENDIX E—CALL USAGE DATA **E-1**

APPENDIX F—LIST OF ACRONYMS **F-1**

EXECUTIVE SUMMARY

The U.S. Department of the Treasury (Treasury) recognized a need for secure, two-way paging within Departmental Offices, as well as within the Treasury Law Enforcement/Public Safety components. To ensure that this secure two-way paging technology adheres to Treasury's strategic and business plans, a pilot test was necessary. Treasury representatives contacted the PSWN Program to request assistance in testing this technical capability for protection and security operations, including day-to-day activities, and ultimately, with the objective of deploying the technology for use during the 2002 Olympic Winter Games in Salt Lake City, Utah.

Purpose

The purpose of the secure two-way paging pilot was to assess the technical merits and operational impacts of the V-One Air SmartGate/VPN Server and the V-One V-Client encryption software operating on Metrocall, Inc.'s paging service. V-One provides secure messaging and authentication for pager-to-pager, pager-to-e-mail, and e-mail-to-pager communications using Ron's Code 4 (RC4), a Variable-Key-Size Encryption Algorithm. Note that RC4 does not meet the National Security Agency's (NSA) standards for transmitting classified information, therefore, no classified messages were sent and received by the pagers using the V-One encryption solution. Further, some pilot participants were from non-federal agencies and did not possess the required security clearance to transmit and/or receive classified information. The V-One encryption solution is only intended to privatize messages sent in encrypted mode; thus, it is important that up to sensitive but un-classified messages only be transmitted or received.

The test evaluation was necessary to gain an understanding of the operation of the secure paging service and to determine whether this service can effectively be deployed for operational public safety use for day-to-day activities as well as for full-scale operational environments. This report highlights the two-way paging technology, describes test plans and procedures, details issues and resolutions, and provides an evaluation of the test results. It also serves as a resource document for current and future implementations of secure two-way paging applications.

Methodology

The Secure Two-Way Paging Pilot provided a mechanism for testing and evaluating a specific two-way secure paging technology. The pilot was intended to assess the V-One secure two-way paging solution for ease of operation, the system's ability to meet operational requests, and the interoperability of the secure paging solution between different service providers. Testing was conducted in two-phases. Phase I focused on basic system performance, while Phase II concentrated on the interoperability between service providers. Specifically, Phase II tested interoperability of the V-One paging solution between the Metrocall and SkyTel paging networks, the two networks operating in the Salt Lake City area. This two-phased testing approach provided a subjective assessment of basic system test performance and carrier interoperability. It also defined operational parameters and limitations including latency issues and undeliverable messages. Summarized below in Table ES-1 are the significant results of Phase I and Phase II testing. A maximum character limit of approximately 800 transmitted characters was encountered for all tests that involved sending messages originating from the pager, regardless of service provider. Tests were run in both encrypted and un-encrypted modes of operation.

Table ES-1
Phase I and Phase II Results Summary

PHASE	RESULTS		
	Test 1 **Pager-to-Pager**	**Test 2** **E-mail-to-Pager**	**Test 3** **Response Time**
Phase I	• Only the subtest involving test messages with fewer than 500 characters was completed • 15 of 33 technical testers responded • Approximately 44 percent of the total responders received the message within 10 minutes • Approximately 30 percent of the total responders received the message within 5 minutes	• On average, 22 out of 33 testers responded • Most messages were received within 5–10 minutes after they were sent • Text messages with a character count of 1,500 had better response times than messages with 500 or 1,000 characters	• 35 out of 45 testers responded • Most messages were received within 5 minutes of being sent • Half of the "late received" messages were late because the pager was turned off or was unable to receive a signal • There were instances where pages were received with errors. This is due to incomplete software provisioning and configuration on the pagers. This issue was solved when the pagers were provisioned and configured properly
Phase II	**Test 1** **Metrocall Pager-to-SkyTel Pager**	**Test 2** **E-mail-to-SkyTel Pager**	**Test 3** **SkyTel Pager-to-Metrocall Pager**
	• All messages received as expected	• All messages received as expected	• All messages received as expected

Key Findings

The key findings derived from the results of the Secure Paging Pilot Test are listed below. Each of the findings specifically speaks to secure paging as it relates to the V-One secure paging solution:

- **Sufficient Functionality.** It was determined that the V-One secure paging solution operates reliably and efficiently in encrypted mode and does not affect normal, unencrypted messaging over the Metrocall network (Phase I tests). Test results also indicated that the V-One secure paging solution interoperates between two different two-way paging service providers, specifically Metrocall Inc. and SkyTel (Phase II tests).

- **Limited Character Transmission.** Approximately 800 characters was the maximum number of characters that could be transmitted from the pager in the encrypted and unencrypted modes. It was determined that this character limitation is a function of

the specific two-way paging devices selected for this pilot test. Although the pager could not send more than approximately 800 characters, it was capable of receiving messages with more than 800 characters (when the message originated from a standard email service).

- **Unable to Transmit Encryption Software Via Infrared Link.** When attempting to transmit the V-Client from one pager to another via infrared link (i.e., "beaming"), not all critical system files were transmitted. This resulted in the inability to run the V-Client encryption software on the receiving pager. In order for the encryption software to work properly, it is necessary to download the V-Client software via serial connection from a personal computer (PC).

- **Non-Treasury VPN PCs Cannot Send/Receive Encrypted Pages.** Encrypted pages could not be sent or received by PCs not authenticated on the Treasury Intranet (i.e., either physically connected on a Treasury local area network [LAN] or connected to the Treasury Intranet via VPN).

- **Encrypted Messages Cannot be Sent by an Unregistered V-Client.** Pagers must be registered with a specific address to be considered fully configured and to operate properly in encrypted mode.

Considerations for Future Implementations

Secure two-way paging offers a reliable alternative to voice-only communications for the transmission of sensitive information. The public safety community may find that two-way paging can foster additional interoperability opportunities to augment voice communications. As future implementations for two-way secure paging systems are being considered, it would be beneficial to take the lessons learned as a result of this pilot test and apply them. These lessons learned, and subsequently the considerations for future implementations, have been developed directly from the key findings of this pilot as well as from overall observations during the pilot testing. The considerations for future implementations include:

- **Network Administration.** It is important that trusted personnel perform network administration and maintain the security of the network. Network administration includes the maintenance of the authentication databases, administering the secure paging VPN server, and provisioning paging devices with the secure paging software. This function is critical since pagers must be provisioned and configured correctly before they can operate in encrypted mode.

- **Group Paging Limitation/Transmit Text Length Limitation.** It is very important that all users understand that there is a limitation associated with the number of characters that can be transmitted with the paging equipment used in this pilot test (Motorola P935). Group messaging from the pager to large numbers of recipients may not be sent if the transmit character limit is reached (approximately 800 characters).

- **Internal Agency Support**. To maintain accountability for equipment, support user needs, and provide a point of contact for vendors, trained internal agency personnel will likely be required. The internal agency support personnel would be responsible for monitoring agency assets as well as maintain associated contact

information for all users. Tools such as databases can be used to track assets and user information. Further, the internal agency support personnel could act as "help-desk" support for users with hardware or software problems.

- **Training Support**. To ensure that users understand how the secure pagers work and how to send and receive messages in both encrypted and clear modes, user training should be available and mandatory for all users. This training would teach users the basics of using the pagers, how and when to use the encrypted features, and how to perform basic maintenance/troubleshooting on the devices.

- **Toll-Free vs. Local Telephone Numbers.** During the procurement process, additional fees may be incurred for the use of toll-free pager telephone numbers. Service providers assign each pager a unique telephone number. These numbers may include a local calling area prefix, or for an additional charge, a toll-free (e.g., 1-800, 1-877) prefix. For field users that routinely travel outside of the agency calling area, toll-free telephone pager numbers may be a more cost-effective option.

1. INTRODUCTION

The Public Safety Wireless Network (PSWN) Program, a federally funded initiative jointly sponsored by the Department of Justice and the Department of the Treasury, is dedicated to improving safety by facilitating the implementation of interoperable communications among public safety organizations. In support of this significant objective, the PSWN Program sponsored a secure two-way paging pilot. Lessons learned from September 11 show that paging can be used as an alternate form of dependable communications during crises. Both one-way and two-way paging are commonly used by the public safety community for routine administrative and operational information sharing; however, secure two-way paging has yet to be proven effective for large-scale field operations. By providing a secure, yet flexible mechanism, for transmitting critical, sensitive (but not classified) information, secure two-way paging can enhance the communications capabilities available to public safety users.

1.1 Background

The U.S. Department of the Treasury (Treasury) recognized a need for secure, two-way paging within Departmental Offices, as well as within the Treasury Law Enforcement/Public Safety components. To ensure that this secure two-way paging technology adheres to Treasury's strategic and business plans, a pilot test was necessary. Treasury representatives contacted the PSWN Program to request assistance in testing this technical capability for protection and security operations, including day-to-day activities, and ultimately, with the objective of deploying the technology for use during the 2002 Olympic Winter Games in Salt Lake City, Utah.

Because the 2002 Olympic Winter Games garner worldwide visibility, security and public protection are vital and essential services. Communications capabilities are a primary component of the security initiative supporting these games. Presidential Directive 62 allocates mission-critical responsibilities to several federal law enforcement agencies for major events such as the Olympics. The U.S. Secret Service (USSS) is the lead planning agency; the Federal Bureau of Investigation (FBI) is responsible for intelligence functions and the appropriate response; and the Federal Emergency Management Agency (FEMA) is in charge of consequence management. To fulfill these important missions, reliable and effective interoperable communications will be necessary in and around all of the Olympic venues. Secure two-way paging will likely provide a means to transmit sensitive information regarding a variety of topics including staffing, event disturbances, and officer locations to users equipped with a secure, two-way pager.

1.2 Purpose

The secure two-way paging pilot is intended to assess the technical merits and operational impacts of the V-One Air SmartGate/VPN Server and the V-One V-Client encryption software operating on Metrocall, Inc.'s paging service. V-One provides secure messaging and authentication for pager-to-pager, pager-to-e-mail, and e-mail-to-pager communications using Ron's Code 4 (RC4), a Variable-Key-Size Encryption Algorithm. From the pager, a Message Encryption Key (MEK) is created using the Secure Hashing Algorithm (SHA-1) to Hash a 40-bit random number with Shared Secret Key, folded with 128 bits. From there, the User message is RC4-encrypted with the MEK, and sent. Note that RC4 does not meet the National Security Agency's (NSA) standards for transmitting classified information, therefore, no classified messages were sent and received by the pagers using the V-One

encryption solution. The V-One encryption solution is only intended to privatize messages sent in encrypted mode. It is important that only sensitive messages (sensitive but un-classified) be transmitted or received. The secure pager-to-pager transmit process is detailed in Section 2.6.

This evaluation is necessary to gain an understanding of the operation of the secure paging service and to determine whether this service is sufficiently effective to deploy for operational public safety use for day-to-day activities as well as for full-scale operational environments. The pilot was conducted in two parts. The first part was proof-of-concept testing in the Washington DC/Baltimore area to ensure that the secure paging technology is operational. The second part of this pilot was robust operational testing in Salt Lake City, UT to evaluate the performance of the secure paging technology in a real-life situation/event. This report highlights the two-way paging technology, describes test plans and procedures, details issues and resolutions, and provides an evaluation of the test results. It also serves as a resource document for current and future implementations of secure two-way paging applications.

2. SECURE PAGING PILOT TECHNOLOGY

2.1 Introduction

Due to its high reliability and high probability of communications success, commercial paging technology is a relatively common form of communications within the public safety arena. Because paging systems use different technology and are independent from the commercial cellular networks, paging messages are not subject to traffic associated with the current commercial cellular services. Generally, commercial paging systems act as store-and-forward messaging. For example, if the pager is switched off or out of coverage, the message will be stored in the paging network to be delivered to the intended destination when the pager re-registers with the network (i.e., when the pager is eventually switched on or travels back in the paging coverage area). In addition, messages are sent in small bursts of data. In combination, these advantageous transmission characteristics ensure a prompt message arrival at the specified location. Historically, paging technology has been one-way in nature, i.e., receive only. Now, paging technology has advanced sufficiently to support messaging in both send and receive mode.

2.2 Background

Until recently, pagers functioned as one-way, receive-only devices. As a result of recent technology advances in the mid-90s, pagers now have the capability to send and receive message data. Generally, two-way paging networks use spectrum in the 900 megahertz (MHz) band. As with one-way paging, the pagers are assigned numeric addresses that act as a unique identifier. To send a message, or to respond to an alphanumeric message, a connection to the paging service provider's network is necessary to process the request. Two-way pagers support several practical and convenient forms of messaging including—

- **Broadcast Messaging.** Delivers a single text message to multiple pager addresses.

- **Pager-to-Pager Messaging.** Delivers a text message from a single pager to another single pager or multiple pager addresses (commonly known as peer-to-peer messaging).

- **E-mail Messaging.** Delivers a single text message from an e-mail account to single or multiple pager addresses. Also, text messages can be delivered from a single pager to an e-mail account.

The benefit of two-way paging is the convenience of the ability to send or respond to a message using the two-way paging device, as opposed to one-way paging in which a user must make a telephone call to respond to a particular message. To respond to a text message from the two-way paging device, users can compose a text message, or select a pre-programmed message, and then send that message by simply evoking the transmit capability of the pager. The send process generally mirrors that of receiving a message.

2.3 Paging Units

Approximately the size of a pocket calculator, the typical two-way pager has a built-in, miniature keyboard, and a liquid crystal display (LCD) screen that displays several lines of text and/or simple graphics. The unit functions as a transmitter by using the internal, subminiature

antenna. This secure two-way paging pilot test tested Motorola Timeport model P935 pagers. The Public Safety Wireless Network (PSWN) Program selected this particular vendor and model for a number of reasons. The first, and most important reason for choosing this particular device is that it has the physical memory space and the computational power required to store and run the V-One V-Client encryption software. Another reason that this particular device was chosen was the relative ease of use.

Both Metrocall and SkyTel provide two-way paging services in the Salt Lake City metropolitan area, and they both support the Motorola Timeport P935 two-way pager on their respective networks. Thus, pager units operating on both systems were part of the test. Specifically, the Timeport P935 messaging device weighs 6.8 ounces and resembles a 1 x 4.0 x 2.5-inch notebook personal computer (PC) when closed. The pager uses one nickel-metal hydride (NiMH) battery giving the device more than one week of use on a single charge. Its 2.4 x 1.7-inch backlit LCD screen has blue electroluminescent backlighting and displays nine, 29-character lines with a scrolling screen capability. The P935 has a full set of keys (a total of 49 keys in the basic QWERTY standard computer and typewriter keyboard layout), and a joystick-like button aids navigation. The P935 operates with the Motorola proprietary ReFLEX™ asymmetrical two-way paging protocol. The asymmetrical nature of the ReFLEX protocol allows for high-capacity, two-way paging communications. Messages are sent in batches, and responses may take 30 seconds to several minutes to be received, depending on coverage and volume of traffic on the network.

2.4 V-One Corporation

V-One Corporation provides secure messaging and authentication for pager-to-pager, pager-to-e-mail, and e-mail-to-pager communications. Together, the Air SmartGate platform and Air SmartPass (V-Client software) client securely connect users over the Internet in a wireless environment. Air SmartGate provides a framework for mutual authentication, secure messaging, access control, and audit logging. This platform comprises a proxy server, authentication server and database, and simple mail transfer protocol (SMTP) gateway that operates at the network level (allowing users to pass information easily and securely through multiple firewalls), in the same fashion that a virtual private network (VPN) operates. The Air SmartPass (V-Client Software) client is a simple software upgrade to the pager code that enables activation of the Motorola P935 two-way pagers. The client supports a secure message environment by transmitting the pager's personal identification number (PIN) with a text message. In this context, a PIN is an exclusive identification number for secure messaging that differs from a "unique identifier."

Air SmartGate server and Air SmartPass (V-Client) client provide wireless secure end-to-end two-way paging using the RSA Variable-Key-Size Encryption Algorithm commonly referred to as Ron's Code 4 (RC4), a 128-bit encryption scheme. It is important to note that RC4 does not meet the National Security Agency's (NSA) standards for transmitting classified information; therefore, in the scope of this pilot test, only sensitive-but-not-classified information could be transmitted. The pager-to-pager transmit process generally uses the following path:

1. A two-way pager transmits a coded message via a radio tower to the paging carrier's network operation center (NOC).

2. The NOC sends the message through its firewall over the Internet to the Department of the Treasury's (Treasury) Intranet, which is also protected by a firewall.

3. The Air SmartGate server verifies and authenticates the sender and receiver PINs by checking the PINs against the authentication database. (When a PIN does not belong to a registered user, the Air SmartGate server discards the message.)

4. When the PINs match, the server decodes the message; however, the message remains secure because of its location on Treasury's Intranet. A shared secret key (known only by the pager and Air SmartGate server) encodes/decodes the data. (A shared secret key is an encrypt/decrypt variable value applied using an algorithm known only to the parties exchanging messages.) This shared secret key is dynamic, changing each time an encrypted message is sent or received.

5. When transmitting a message to another pager, the Air SmartGate server codes the message, sends it over the Internet to the NOC, and finally to the receiving two-way pager via a radio tower. The encrypted message is received and can then be decrypted by the pager.

The e-mail-to-pager transmit path for a message is as follows. (The pager-to-e-mail transmit path is similar, but in the opposite direction.)

1. A VPN client (e.g., a PC accessed via dial-up or broadband) authenticates to the VPN server local on the Treasury Intranet.

2. The PC transmits a coded message via the Treasury's Intranet.

3. The Air SmartGate server verifies and authenticates the receiver's PIN by checking the PIN against the authentication database. The Air SmartGate server encrypts the message. When a PIN does not belong to a registered user, the Air SmartGate server discards the message.

4. The Treasury's Intranet sends the encrypted message through its firewall over the Internet to the NOC, which is also protected by a firewall.

5. The encrypted message is sent to the proper destination device where it is received and decrypted by the pager.

2.5 Qwest Communications

In March of 2001, Qwest Communications, in conjunction with V-One Corporation as the subcontractor, was awarded a 1-year competitive blanket purchase agreement to deliver a managed VPN to Treasury, providing users remote access to all bureau networks. A VPN is a private data network that uses the public telecommunication infrastructure, maintains privacy using protocols and security procedures, and is typically installed as part of the firewall server. Treasury personnel use Qwest's VPN for access to e-mail and other data 24 hours a day. The Qwest VPN service was extended to the two-way paging service in support of this pilot and subsequent implementations of the two-way paging service.

2.6 Secure Two-Way Paging Network

The secure two-way paging network configuration is illustrated in Figure 1. As shown in the figure, a two-way pager, assigned a PIN known to the paging carrier's NOC, and enabled with the Air SmartPass Client (V-Client software), transmits secure text via a radio tower to the paging carrier's NOC. At the NOC, the message routes through a proxy server that acts as a traffic manager. The proxy server sends messages with the appropriate PINs through the carrier's firewall over the Internet to the Treasury Communications System (TCS). TCS receives the message at the firewall and sends it to the Air SmartGate authentication server. The authentication server codes/decodes messages and manages the authentication database that contains the pagers' PINs. The server queries the database to ensure that the sender and receiver PINs are legitimate. After the authentication database verifies the validity of the PINs, the authentication server resends the secure message through the TCS firewall via the Internet through the carrier's NOC and proxy server. The message transmits to a radio tower and the second secure two-way pager. The second Air SmartPass client decodes the message for viewing by the recipient.

Also shown in the figure are the interconnections and transmission paths of a message sent from PC VPN clients (both within the TCS and outside the TCS) to secure pagers. In both of these instances, the message is encrypted at the Air SmartGate server and sent to the authenticated pager via the Internet, across the Treasury and NOC firewalls. The encrypted message is then transmitted from the towers and received by the pager. The Air SmartPass Client (V-Client software) resident on the two-way pager then decrypts the message for viewing.

For this pilot test in the Washington / Baltimore metropolitan area, the Air SmartGate server was located in a secure Treasury facility called W2. This facility was used to house all the server components (e.g., Air SmartGate, Authentication Databases) required for the proper operation of this secure two-way paging solution. Access to the W2 facility is limited to cleared personnel.

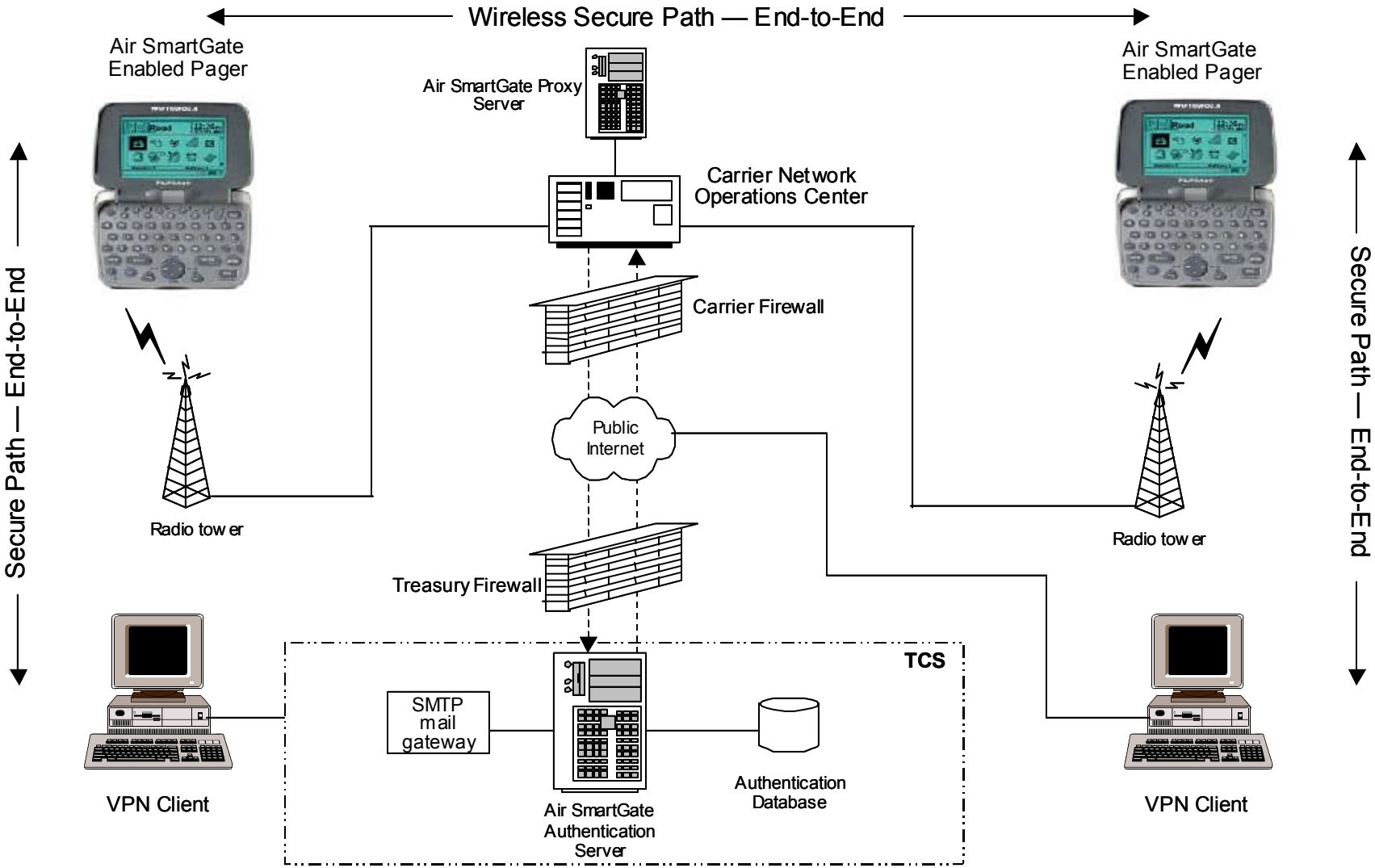

Figure 1
Secure Two-Way Paging Operational Diagram

2.7 Sequence of Steps

This section details the send and receive process for transmitting a text message from one two-way pager to another.

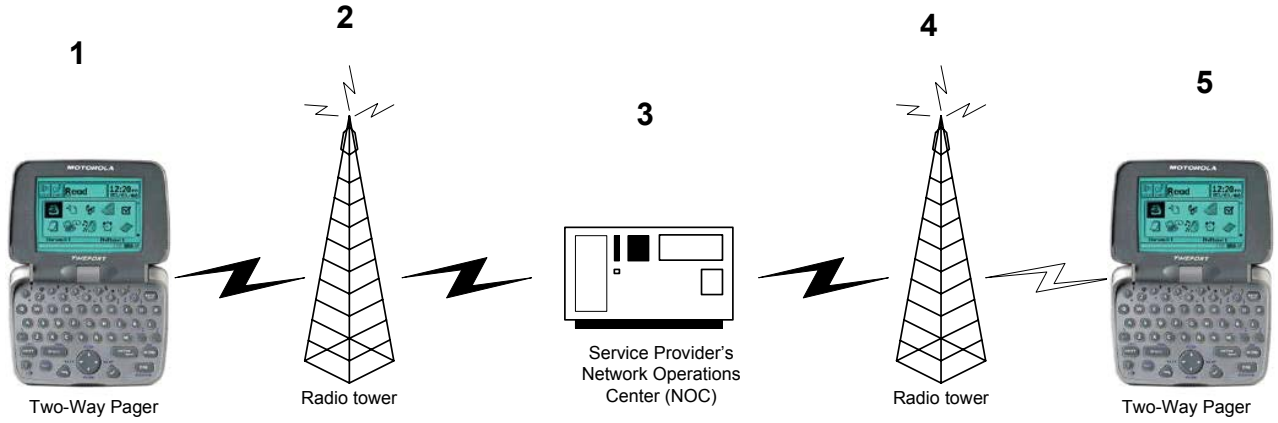

Figure 2
Two-way Paging Send/Receive Process

1. The user composes the text message, addresses the message to another pager, and selects send. The two-way pager then transmits the message over the air via radio frequency.

2. A paging base station receives this signal from the pager and then sends the message to the NOC over a data network.

3. The NOC accepts the page, verifies the validity of the pager number, and checks its database for the subscriber's correct capcode (i.e., a unique code representing a pager address). The message is converted to the appropriate signal protocol and is then sent to the appropriate paging base station(s).

4. The paging base station receives the message from the NOC via the data network and then transmits the message over the air via radio frequency.

5. The pager receives the signal from the paging base station's transmission. When the transmission is received by the pager, the user is alerted with a visual alert (an icon or LCD flashes), an audible alert (i.e., a standard beep alert, a chime, or sequence of musical notes) or a silent alert (i.e., a vibration). The message can then be opened and read.

3. PILOT APPROACH

The PSWN Program accomplished the pilot effort using a staged approach. Preplanning efforts comprised the first stage. These efforts included identifying participants and developing guidelines for participation. The next stage encompassed procurement of test equipment, hardware, and service. The final stage included hardware and software testing and analysis of resultant data. This section describes each of the pilot stages in greater detail.

3.1 Planning

Prior to testing, the PSWN Program engaged in a number of activities to establish the framework for the Secure Paging Pilot. To develop a broader understanding of the secure two-way paging solution that would be used in this pilot test, PSWN Program staff attended a V-One technology presentation that highlighted the technology, features, and overall operations.

The preparation efforts continued with the identification of organizations and users that would be willing to participate in the pilot test. Further, the roles and responsibilities for each organizations and users were detailed. The participating organizations are as follows:

- U.S. Customs Service (USCS)
- Federal Bureau of Investigation (FBI)
- Federal Law Enforcement Training Center (FLETC)
- U.S. Department of the Treasury—Department of the Assistant Secretary of Information Systems (DASIS)
- U.S. Department of the Treasury—Wireless Programs Office (WPO)
- U.S. Secret Service (USSS)
- Utah Communication Agency Network (UCAN).

Within each of these participating organizations, the PSWN Program identified users as either general participants or technical testing participants. The program asked both types of participants to become familiar with the secure two-way paging software and assess the ease of use and functionality of that software. Technical testing participants were also asked to take on additional responsibilities including following the testing procedures and sending responses to test pages sent at regular intervals, as prescribed in the test plans.

To ensure that the secure two-way paging equipment and services were used specifically for this pilot test, the PSWN Program created and sent Memoranda of Understanding (MOU) and User Agreements to each participating organization to establish the guidelines for active participation in this pilot test. The MOUs were sent to the appropriate point of contact within the organizations for signature, thus authorizing each organization to actively participate in the pilot test. Once the PSWN Program received the signed MOUs and User Agreements, staff prepared a participant list for each participating organization. Subsequently, the program provided

participants with the necessary two-way paging equipment and services. The service provider, Metrocall, assigned pager numbers (telephone numbers) and aliases (e-mail addresses) associated with each two-way pager. Appendix A contains a sample of each of the documents used in the initial planning stage for identifying and authorizing the participation of organizations and users in this pilot test. These documents include a sample MOU, a sample User Agreement, and the user list detailing the organizations, participants, pager numbers, and aliases.

3.2 Procurement

During the planning process, the PSWN Program coordinated the procurement of the two-way pagers and two-way paging service from Metrocall. For the Washington, DC, metropolitan two-way secure paging pilot test, the program procured 40 Motorola P935 pagers, along with 40 nickel-metal hydride replacement batteries for the Motorola P935 pagers. To go along with the purchase of this equipment, the program also procured two-way paging service for each pager for 1 year. The paging service allowed for 1,000 calls (pages) per month, per pager. A total of 480 months of two-way paging service was purchased.

After the initial Washington, DC/Baltimore metropolitan two-way secure paging pilot proof-of-concept testing was completed, the PSWN Program determined that the V-One secure two-way paging solution functioned as expected and would be appropriate for deployment for a wide-scale, operational pilot test implementation in support of public safety communications for the 2002 Salt Lake City Winter Olympic Games. As with the initial procurement for the Washington, DC, metropolitan two-way secure paging pilot test, the PSWN Program coordinated the larger procurement effort to purchase two-way pagers and services from Metrocall. To provide the pagers with secure two-way paging capabilities, the procurement of Qwest's virtual private network (VPN) seats was also required. For the wide-scale Olympics pilot test implementation, the PSWN Program coordinated the procurement of 500 Motorola P935 two-way pagers, along with two-way paging service for 5 months for all pagers. The paging service allows for 1,000 calls (pages) per month, per pager. A total of 2,500 months of two-way paging service was purchased.

3.3 Testing and Analysis

The Secure Two-Way Paging Pilot provides a mechanism for testing and evaluating two-way secure paging technology. The pilot was intended to assess the V-One two-way paging solution for ease of operation, the system's ability to meet operational requests, and the interoperability of different service providers. Proof-of-concept testing in the Washington DC/Baltimore metropolitan area was conducted in two-phases. Phase I focused on basic system performance, while Phase II concentrated on the interoperability between service providers. Specifically, Phase II tested interoperability of the V-One paging solution between the Metrocall and SkyTel paging networks, the two networks operating in the Salt Lake City area. This two-phased testing approach provided a subjective assessment of basic system test performance and carrier interoperability. It also defined operational parameters and limitations including latency issues and undeliverable messages.

This pilot test was not intended to test the security of the solution. Nor was this pilot intended to verify that the secure transmissions cannot be intercepted and decrypted by hackers or other potentially hostile entities. Testing of the secure paging solution's vulnerabilities was conducted prior to this pilot by the vendor, V-One.

3.3.1 Phase I Testing

Phase I tested the functionality of Metrocall and V-Client operating on Motorola's Timeport P935 two-way pagers. Phase I included three different types of tests: 1) Pager-to-Pager; 2) E-mail-to-Pager; and 3) Response Time. Testing encompassed a total of 45 pagers—33 of which were controlled by technical testing staff, 12 of which were controlled by nontechnical staff, and one of which was designated as the main testing unit. Testing for all three tests was completed during a 2-week window of time. A summary of Phase I results is included in Table 1. Note that Pager-to-Pager and E-mail-to-Pager tests were conducted in both encrypted and clear modes, Response Time tests were all conducted in encrypted mode. The actual test plans and testing log sheets are shown in Appendix B.

- **Pager-to-Pager.** This testing is composed of three separate subtests: 1) pager message not exceeding 500 characters; 2) pager message not exceeding 1,000 characters; and 3) pager message not exceeding 1,500 characters. The three separate subtests help determine the boundary for character transmission limitations. Within each subtest, encrypted and unencrypted messages are sent to determine whether latency (i.e., the time it takes to deliver a message) is introduced with the encryption process. The main testing unit sends messages, consisting of the appropriate amount of characters, only to the pagers controlled by technical testing staff. This tests the ability to broadcast a message from one pager to many pagers.

- **E-mail-to-Pager.** E-mail-to-Pager testing is composed of three separate subtests: 1) broadcast e-mail message not exceeding 500 characters; 2) broadcast e-mail message not exceeding 1,000 characters; and 3) broadcast e-mail message not exceeding 1,500 characters. Similar to pager-to-pager testing, the three separate subtests help determine the character transmission threshold. Within each subtest, encrypted and unencrypted messages are sent to determine whether latency is introduced with the encryption process. Messages consisting of the appropriate number of characters are sent via e-mail only to pagers controlled by technical testers. This tests the functionality of broadcast messaging from an e-mail account.

- **Response Time.** This testing included all pilot participants, both general and technical testing. The test schedule was set for a 7-day period, with active testing commencing every other day, for a total of 4 test days. Treasury personnel determined that 3 days of testing would be sufficient, since one of the objectives of running this same test many times was to familiarize the participants with the pagers and the secure paging solution. A broadcast page was sent from the main testing pager that included standard message text for uniformity. Each tester responds with a message indicating whether a message is received during the 5-minute time frame. If the message is not received during the transmit/receive 5-minute time frame, the responding message is required to indicate the actual time of receipt. Message latency, relative to broadcast messaging, is the major issue area tested in response time testing. To further exercise the V-One encryption solution's capabilities and to familiarize participants with the process of sending encrypted messages, all responses to response time tests are sent back to the main testing pager in the encrypted mode.

Table 1
Summary of Phase I Test Results

TEST	RESULTS		
	Fewer than 500 character text message	**Fewer than 1,000 character text message**	**Fewer than 1,500 character text message**
Test 1 Pager-to-Pager Test	• 15 of 33 technical testers responded • Approximately 44 percent of the total responders received the message within 10 minutes • Approximately 30 percent of the total responders received the message within 5 minutes	• No results found: The pager transmit limitation is approximately 800 characters (including address and subject line text)	• No results found: The pager transmit limitation is approximately 800 characters (including address and subject line text)
Test 2 E-mail-to-Pager Test	• 22 of 33 technical testers responded • Approximately 85 percent of the total responders received the message within 10 minutes • Approximately 73 percent of the total responders received the message within 5 minutes	• 20 of 33 technical testers responded • Approximately 86 percent of the total responders received the message within 10 minutes • Approximately 79 percent of the total responders received the message within 5 minutes	• 24 of 33 technical testers responded • Approximately 97 percent of the total responders received the message within 10 minutes • Approximately 70 percent of the total responders received the message within 5 minutes
Test 3 Response Time Test	• Total of 3 testing days • 35 of 45 testers responded • Approximately 84 percent of the total responders received the message within 10 minutes • Approximately 83 percent of the total responders received the message within 5 minutes • Approximately 50 percent of "late messages" received were late because the pager was turned off or was unable to receive signal (e.g., the tester was in the air during travel) • There were instances where pages were received with errors. This is due to incomplete software provisioning and configuration on the pagers. This issue was solved when the pagers were provisioned and configured properly.	N/A: This test was not conducted because of the pager transmit character limitation	N/A: This test was not conducted because the pager transmit character limitation

3.3.2 Phase II Testing

Phase II testing focused on the interoperability capabilities between the SkyTel and Metrocall service providers. Each service provider's network supports a significant number of public safety users, thus interoperability between these providers must be ensured to verify the feasibility of using secure, two-way paging for the public safety community at large and on a wide scale.

During Phase II, three different tests were conducted: 1) Metrocall Pager-to-SkyTel Pager; 2) E-mail-to-SkyTel Pager; and 3) SkyTel Pager-to-Metrocall Pager. One Metrocall pager and five SkyTel pagers served as the test units. The test units were maintained by Treasury WPO personnel. A summary of the results of Phase II testing are shown in Table 2. The actual test plan and testing log sheets are included in Appendix B.

- **Metrocall Pager-to-SkyTel Pager.** The Metrocall Pager transmits broadcast messages to SkyTel pagers. This test comprises two subtests: 1) a message of fewer than 500 characters, and 2) a message of greater than 500 characters. Within each subtest, both encrypted and unencrypted messages are sent. By routing messages between disparate service providers, this test challenges the functionality between the paging units and service providers. The inclusion of different character counts for each text message tests the character threshold of the pager and paging service.

- **E-mail-to-SkyTel Pager.** An e-mail message is routed to the SkyTel units via an e-mail account seated on the Treasury network. This test comprises two subtests: 1) a message of fewer than 500 characters, and 2) a message greater than 500 characters. The different character counts for each text message challenge the threshold of the pager and paging service. Within each subtest, both encrypted and unencrypted messages are sent. These subtests ensure that an e-mail message can be sent through a secure network and received by a specified SkyTel unit.

- **SkyTel Pager-to-Metrocall Pager.** A SkyTel unit (Motorola P935 two-way pager provisioned with the V-One Client) transmits a secure message to the main Metrocall testing pager (controlled by Treasury WPO). This test comprises two subtests: 1) a message of fewer than 500 characters, and 2) a message greater than 500 characters. Within each subtest, both encrypted and unencrypted messages are sent. The main Metrocall testing pager transmits a secure response to the SkyTel unit. This test challenges the functionality between paging units and service providers.

Table 2
Summary of Phase II Test Results

TEST	RESULTS	
	Fewer than 500 character text message	Exceeding 500 character text message
Test 1 Metrocall Pager-to-SkyTel Pager	• All messages received as expected	• All messages received as expected
Test 2 E-mail-to-SkyTel Pager	• All messages received as expected	• All messages received as expected
Test 3 SkyTel Pager-to-Metrocall Pager	• All messages received as expected	• All messages received as expected

3.3.3 User Information Survey

A user information survey, to be distributed upon completion of the robust field testing at the 2002 Winter Olympic Games, is shown in Appendix D. Results of the survey will be compiled by the Department of the Treasury's Wireless Programs Office.

3.3.4 Call Usage Information

The secure paging server collected call data during the robust field-testing in Salt Lake City (i.e., the testing accomplished while the pagers were used in support of communications requirements during the 2002 Winter Olympic Games). The call usage data presented in Appendix E shows the number of pages that were sent and received by each of the deployed secure pagers between the dates of January 10, 2002 – March 10, 2002. This call usage data will be analyzed by the Department of the Treasury's Wireless Programs Office for user trends and other operational aspects regarding the use of the secure paging units.

4. KEY FINDINGS

During the secure two-way paging pilot test, the participants assessed the V-One secure paging solution for ease of use, functionality, and message retrieval latency. Throughout the course of testing, participants exercised the V-One solution thoroughly to identify any limitations and shortcomings. The operation of the secure paging solution is critical because it will be deployed directly to support public safety operations during the 2002 Salt Lake City Winter Olympic Games. Simple and effective public safety communications is critical, especially during a high-profile, worldwide event such as the Olympics. If an emergency situation should occur during the Olympics, public safety agencies may rely heavily on secure two-way paging because regular commercial wireless solutions will not offer the security necessary and could be congested to the network saturation point.

Outlined below are the key findings derived from the results of the Secure Paging Pilot Test. Not all of the findings are a direct outcome of the pilot test, some have resulted from the effort as a whole. Each of the findings specifically speaks to secure paging as it relates to the V-One secure paging solution:

- **Sufficient Functionality.** Test results indicate that this technology is sufficient to support agency requirements for secure paging communications at the 2002 Winter Olympic Games. It was determined by Treasury personnel, with the support of program staff, that the V-One secure paging solution operates reliably and efficiently in both encrypted and unencrypted modes. Futher, it was determined that the V-One secure paging solution interoperates between two different two-way paging service providers (Metrocall Inc. and SkyTel).

- **Limited Character Transmission.** Approximately 800 characters was the maximum number of characters that could be transmitted in both the encrypted and unencrypted modes. This transmission character limitation was unique to messages originating from the two-way pagers. This transmission character limitation was not, however, unique to the paging service provider. It was determined that this character limitation is a function of the specific two-way paging devices selected for this pilot test, namely the Motorola P935 two-way pager. The approximate 800-character limitation is easily reached if the user attempts to send a message from the pager to many other users simultaneously or if the text of the message is lengthy. The character count includes characters in the address line, the subject line, and the message body.

- **Unable to Transmit Encryption Software Via Infrared Link.** When attempting to transmit the V-Client from one pager to another via infrared link (i.e., "beaming"), not all critical system files were transmitted. This resulted in the inability to run the V-Client encryption software on the receiving pager. In order for the encryption software to work properly, it is necessary to download the V-Client software via serial connection from a personal computer (PC).

- **Non-Treasury VPN PCs Cannot Send/Receive Encrypted Pages.** The test showed that encrypted pages could not be sent or received by PCs not authenticated on the Treasury Intranet (i.e., either physically connected on a Treasury local area network [LAN] or connected to the Treasury Intranet via VPN). The encryption is applied to

the message at V-One's Air SmartGate Server, and that message can only be delivered to a VPN authenticated device. All message traffic within the Treasury Intranet is unencrypted until it reaches the Air SmartGate Server. If a message is sent encrypted from a pager to a non-Treasury VPN authorized PC, the Air SmartGate Server discards the message because it cannot authenticate the receiving device and the receiving device address is not located in the look-up database that holds the authenticated destination information. Non-Treasury VPN PCs do have the ability to successfully send messages to secure pager aliases (e.g., Name.Name@VPN-2way.treas.gov); however, the message will travel across the public Internet unencrypted (in the same way that normal e-mail traffic travels) until it reaches the Air SmartGate Server, resident on the Treasury Intranet. Because it is relatively easy to intercept and decode normal e-mail traffic, this defeats the purpose of sending the encrypted message.

- **Encrypted Messages Cannot be Sent by an Unregistered V-Client.** Pagers can be provisioned with a working copy of the V-Client software, yet may remain unable to send encrypted messages. Pagers must be registered with a specific address to be considered fully configured. This configuration is necessary to register with the Air SmartGate Server before any encrypted messages can be passed. It is critical that all pagers are provisioned and configured by qualified staff to avoid the situation of not being able to send encrypted messages.

Participants encountered other, minor issues during the testing of the secure two-way paging solution. Many of these issues proved to be isolated incidents that were resolved as soon as the cause was determined, however, several are still on-going. A summary of the issues discovered during the pilot test, included the status of each issue, is detailed in Appendix C. These issues include—

- **Pager aliases are not configured correctly.** The Air SmartGate server cannot process desktop-to-pager transmissions to pagers configured with an incorrect alias (i.e., when the alias configured on the pager does not match the alias in the authentication database).
- **Pagers are not registered correctly.** Some pagers were not fully configured with V-Client.
- **Group paging (via pager) is limited (transmit character limitations).** Approximately 800 characters is the maximum amount that the pagers can transmit.
- **Unable to beam V-Client software from pager-to-pager.** Pagers must be provisioned with encryption software via PC link.
- **Updated software for W2 server is necessary.** Software update was required to test interoperability between Metrocall and SkyTel.
- **Encrypted responses cannot be routed to a PC outside of the Treasury firewall.** Encryption capability cannot be tested outside of Treasury VPN network.
- **Message receipt delays are occurring for users in close proximity to Olympic venues.** Updated software is necessary, and coverage issues may exist.

- **Unable to send messages to SkyTel pagers.** A provisioning error was identified that made interoperable messaging between Metrocall and SkyTel pagers unavailable.

5. CONSIDERATIONS FOR FUTURE IMPLEMENTATIONS

Secure two-way paging offers a reliable alternative to voice-only communications for the transmission of sensitive information. The public safety community may find that two-way paging can foster additional interoperability opportunities to augment voice communications. As future implementations for two-way secure paging systems are being considered, it would be beneficial to take the lessons learned as a result of this pilot test and apply them. These lessons learned, and subsequently the considerations for future implementations, have been developed directly from the key findings of this pilot as well as from overall observations during the pilot testing. The considerations for future implementations include:

- **Network Administration.** It is important that trusted personnel perform network administration by and maintain the security of the network. Network administration includes the maintenance of the authentication databases, administering the secure paging VPN server, and provisioning paging devices with the secure paging software. This function is critical since pagers must be provisioned and configured correctly before they can operate in encrypted mode.

- **Group Paging Limitation/Transmit Text Length Limitation.** It is very important that all users understand that there is a limitation associated with the number of characters that can be transmitted with the paging equipment used in this pilot test (Motorola P935). Group messaging from the pager to large numbers of recipients may not be sent if the transmit character limit is reached (approximately 800 characters).

- **Internal Agency Support**. To maintain accountability for equipment, support user needs, and provide a point of contact for vendors, trained internal agency personnel will likely be required. The internal agency support personnel would be responsible for monitoring agency assets as well as maintain associated contact information for all users. Tools such as databases can be used to track assets and user information. Further, the internal agency support personnel could act as "help-desk" support for users with hardware or software problems.

- **Training Support**. To ensure that users understand how the secure pagers work and how to send and receive messages in both encrypted and clear modes, user training should be available and mandatory for all users. This training would teach users the basics of using the pagers, how and when to use the encrypted features, and how to perform basic maintenance/troubleshooting on the devices.

- **Toll-Free vs. Local Telephone Numbers.** During the procurement process, additional fees may be incurred for the use of toll-free pager telephone numbers. Service providers assign each pager a unique telephone numbers. These numbers may include a local calling area prefix, or for an additional charge, a toll-free (e.g., 1-800, 1-877) prefix. For field users that routinely travel outside of the agency calling area, toll-free telephone pager numbers may be a more cost-effective option. Conversely, if the pagers will only be used locally, then the "toll free calling" feature is not needed and generates an unwarranted cost.

APPENDIX A – MEMORANDUM OF UNDERSTANDING

MEMORANDUM OF UNDERSTANDING
BETWEEN THE PUBLIC SAFETY WIRELESS NETWORK PROGRAM
AND <<AGENCY NAME>>

1. **PURPOSE:** This Memorandum of Understanding (MOU) establishes the participation of <<AGENCY NAME>> in a Secure Paging pilot being sponsored by the PSWN Program. This pilot is intended to assess the technical merits and operational impacts of the Metrocall secure paging service. The ultimate goal is to gain an understanding of the operation of the secure paging service, as well as determine whether this service is sufficiently effective to deploy for operational public safety use, to include secure interoperable communications.
2. **SCOPE:** This pilot involves the full participation of <<AGENCY NAME>> for the duration of the testing, including the full participation in user surveys.
    a. **Equipment:** The PSWN Program agrees to provide the <<AGENCY NAME>>with five (5) Motorola Timeport Two-Way Messaging Devices (model P935), with one (1) spare battery per each pager. The PSWN Program will further provide Metrocall Two-Way messaging service, for 12 months, for each messaging device included in the pilot. The service will support up to 1,000 messages per pager, per month. Virtual private network (VPN) capabilities will also be provided (directly by the Department of the Treasury, Wireless Programs Office).
    b. **Pilot Participant Responsibilities:** Although field operators will be able to use the paging service for the next few months, the duration of the actual data collection period of this pilot will be 2 to 3 weeks. During this period, field operators will be required to use their paging devices extensively, exercising all available functions in accordance with the pilot procedures. Users will be required to participate in surveys targeted at providing insight on such issues as ease of use and pager utility. Further details regarding testing procedures and survey procedures will be provided to <<AGENCY NAME>> and the selected field operators as the test period nears.
    c. **Disposition of Test Results:** The system operating data and the subsequent user surveys will be analyzed thoroughly and findings will be documented. The PSWN Program will distribute resulting documentation to each of the pilot participants (i.e., one set of documentation for each participating agency). The PSWN Program expects to complete testing, data collection, and analysis, including user surveys by the end of October 2001. Documentation will be distributed shortly thereafter. The pilot results will be used to support a decision regarding deployment of Metrocall's secure paging service for tactical, administrative, and interoperable communications during the 2002 Salt Lake City Winter Olympic Games.

d. **User Identification:** Attached to this memorandum is a form to be completed by each user participating in this pilot. These forms must be completed in their entirety, checked for accuracy, and submitted to the PSWN Program along with the signed MOU. The forms will provide the means to track each of the paging devices. Further, the paging service provider, Metrocall, will use the information provided by each user to set up individual accounts, each with a unique pager directory number (i.e., phone number and personal identification number) and e-mail address (personalized to the user). Paging "groups" and "super groups" will also be created using the information provided on the form. Paging devices, subscriber service, groups, and super groups will be activated when all forms have been completed and returned to the PSWN Program point of contact.

3. IMPACT STATEMENT: This pilot is crucial for identifying a reliable, secure means of public safety communications during the 2002 Salt Lake City Winter Olympics. Furthermore, if the outcome of this pilot yields favorable results, it may ultimately lead to the deployment of this commercial service to the federal public safety community on a broad scale. To that end, the participation of the <<AGENCY NAME>>is greatly appreciated.

4. CONCURRENCE WITH TERMS OF AGREEMENT: If you understand and agree with the pilot approach described above, please signify by affixing your signature below. By signing below, the <<AGENCY NAME>>agrees to fully participate in this pilot and will ensure that the selected field operators will follow all testing procedures and complete all surveys related to this pilot, and that the subject pagers will be returned to the PSWN Program when requested. Please return the signed MOU and signed User Agreements to the PSWN Program Management Office (addressed to: The PSWN Program, P.O. Box 3926, Fairfax, VA 22038-3926) no later than Friday, September 14, 2001.

CONCURRENCES:

_____	_____
Robert E. Lee, Jr.	Julio "Rick" Murphy
PSWN Program Manager	PSWN Program Manager
Department of Justice	Department of the Treasury

Dated:_____

_____
<<AUTHORIZED PERSONNEL>>
<<POSITION>>
<<AGENCY>>

Dated:_____

Public Safety Wireless Network (PSWN) Program
Secure Paging Pilot Test Agreement

Agency _____
_____

Name _____
Title _____
Office Address_____
City _____ **State**_____
Zip Code _____
Phone _____
Fax _____
Other Contact Number(s)_____
_____
E-mail _____

By filling in the above information and signing below, I agree to the following terms and conditions:

- I will fully participate in this pilot test
- I understand that I will be provided with the necessary equipment and paging service required to participate in this pilot test
- I understand that user training for the paging equipment and service will be available and may be mandatory
- I agree to complete the test procedures as prescribed by the test plan (to be furnished to me later)
- I agree to complete any user surveys required for the pilot test
- I agree to return all equipment upon the conclusion of this pilot test
- I understand that if I should damage or render any of the provided pilot test equipment unusable, I will not be provided new equipment
- If any equipment is rendered unusable, I agree that it will be my responsibility to coordinate with my respective agency to purchase new equipment so that I may continue to participate in this pilot test
- I understand that this pilot is being conducted to test the privatization of the provider's text paging service, and as such, I shall not transmit CLASSIFIED messages over the service and equipment that has been provided to me at any time during the pilot test

Signed _____ _____ **Date**_____
(Name) (Title)

Please print this form, complete the above information, sign and date, and send to the PSWN Program office via fax (703-279-2035, ATTN.: Rod Vinluan) as soon as possible. This form is <u>required</u> in order to obtain testing equipment (pagers) and participate in this pilot.

SECURE PAGING PILOT PARTICIPANT LIST

FLETC					
NAME	**TECHNICAL TESTER***	**OFFICE LOCATION**	**PAGER NUMBER/ E-MAIL ADDRESS**	**TELEPHONE NUMBER**	**E-MAIL ADDRESS**
Bruce Brown	Yes	FLETC – OSL Bldg 67, Glynco, GA 31524	800-609-9416 brown.bruce@my2way.com	912-267-2585	bbrown@fletc.treas.gov
Reba Fischer	Yes	FLETC – OSL Bldg 67, Glynco, GA 31524	800-799-0493 reba.fischer@my2way.com	912-267-2343	rfischer@fletc.treas.gov
Marcus L. Hill	Yes	FLETC – DO Townhouse 380, Glynco, GA 31524	800-573-1368 marcus.hill@my2way.com	912-267-2115	mhill@fletc.treas.gov
Rex Huddy	Yes	FLETC – OSL Bldg 67, Glynco, GA 31524	800-739-3401 rex.huddy@my2way.com	912-267-2181	rhuddy@fletc.treas.gov
Sandra H. Peavy	Yes	FLETC – CIO Bldg 94, Glynco, GA 31524	877-989-8584 sandy.peavy@my2way.com	912-267-3254	speavy@fletc.treas.gov

*Technical testers are required to participate in the pilot technical test plan, which will be distributed at a later date. These people will be asked to perform testing within a controlled group for the purpose of performance and use testing. You do not have to be technical to perform these functions.

SECURE PAGING PILOT PARTICIPANT LIST

TREASURY CIO ORGANIZATION/WPO					
NAME	TECHNICAL TESTER*	OFFICE LOCATION	PAGER NUMBER/ E-MAIL ADDRESS	TELEPHONE NUMBER	E-MAIL ADDRESS
Gary Allmond	Yes	Department of the Treasury/W2 7598 Coleshire Dr. McLean, VA 22102	877-510-1375 8775101375@my2way.com	703-747-9222	Gary.Allmond@cio.treas.gov
Ron Bearse	Yes	1500 Pennsylvania Ave, Rm 3183 Annex Washington, DC 20221	877-989-8589 Ron.Bearse@my2way.com	202-602-2059	Ron.Bearse@do.treas.gov
Al Bissett	Yes	1500 Pennsylvania, Rm 1150 Annex Washington, DC 20221	877-989-8593 Al.Bissett@my2way.com	202-622-3474	Alvin.Bissett@do.treas.gov
Mayi Canales	No	1425 New York Ave, Suite 300 Washington, DC 20220	877-931-2177 Mayi.Canales@my2way.com	202-927-7449	Mayi.Canales@do.treas.gov
James Downes	Yes	1425 New York Ave, Suite C105 Washington DC 20220	800-915-8167 8009158167@my2way.com	202-622-1582	James.Downes@do.treas.gov
Jim Flyzik	No	1425 New York Ave, Suite 300 Washington, DC 20220	877-989-8592 Jim.Flyzik@my2way.com	202-622-1200	Jim.Flyzik@do.treas.gov
Scott Hill	Yes	Department of the Treasury/W2 7598 Coleshire Dr. McLean, VA 22102	888-994-4768 8889944768@my2way.com	703-747-9339	Scott.Hill@cio.treas.gov
Michelle Moldenhauer	No	1500 Pennsylvania Ave, Rm 3090 Annex Washington, DC 20221	877-989-8570 Michelle.Moldenhauer@my2way.com	202-622-1110	Michelle.Moldenhauer@do.treas.gov
Bob Reed	Yes	Department of the Treasury/W2 7598 Coleshire Dr. McLean, VA 22102	888-674-7021 8886747021@my2way.com	703-747-9747	Rreed@notes.tcs.treas.gov
Dave Rossborough	Yes	1500 Pennsylvania Ave Washington DC, 20221 Rm 1150	877-989-8572 8779898572@my2way.com	202-622-1130	Dave.Rossborough@do.treas.gov
Fran School	Yes	1500 Pennsylvania Ave Washington DC, 20221 Rm 1150	877-989-8575 8779898572@my2way.com	202-622-3806	Fran.School@do.treas.gov
Jeff Shouse	Yes	1500 Pennsylvania Ave	877-989-8587	202-622-9109	Jeff.Shouse@do.treas.go

SECURE PAGING PILOT PARTICIPANT LIST

TREASURY CIO ORGANIZATION/WPO					
		Washington DC, 20221 Rm 1150	8779898587@my2way.com		v
Kyle Sinclair	Yes	1425 New York Ave, Suite C104 Washington DC 20220	877-554-5243 8775545243@my2way.com	202-622-1582	Kyle.Sinclair@do.treas.gov
Darrell Smith	Yes	1425 New York Ave, Suite C107 Washington DC 20220	800-573-0842 8005735243@my2way.com	202-622-5198	Darrell.Smith@do.treas.gov
Raymond Viets	Yes	1500 Pennsylvania Ave, Rm 3180 Annex Washington, DC 20221	877-989-8578 Raymond.Viets@my2way.com	202-622-1120	Raymond.Viets@do.treas.gov
Vicki Waizeneger	Yes	1500 Pennsylvania Ave, Rm 5171 Annex Washington, DC 20221	877-989-8576 Vicki.Waizenegger@my2way.com	202-622-2594	Vicki.Waizenegger@do.treas.gov
Tom Wiesner	No	1425 New York Ave, Rm 2150 Washington, DC 20220	888-674-7021 Tom.Wiesner@my2way.com	202-622-1592	Tom.Wiesner@do.treas.gov
Patti Wood	Yes	1310 G Street NW 3rd Floor East Washington DC 20220	800-608-3211 8006083211@my2way.com	202-622-2907	Patti.Wood@do.treas.gov

*Technical testers are required to participate in the pilot technical test plan, which will be distributed at a later date. These people will be asked to perform testing within a controlled group for the purpose of performance and use testing. You do not have to be technical to perform these functions.

SECURE PAGING PILOT PARTICIPANT LIST

UCAN					
NAME	**TECHNICAL TESTER***	**OFFICE LOCATION**	**PAGER NUMBER/ E-MAIL ADDRESS**	**TELEPHONE NUMBER**	**E-MAIL ADDRESS**
Doug Chandler	Yes	6000 State Office Building Salt Lake City, UT 84114	877-989-8563 Doug.Chandler@my2way.com	801-538-9546	Dchandler@dps.state.ut.us
Mike Christensen	Yes	2451 S 600 West, Suite 300 Salt Lake City, UT 84115	877-989-8564 Mike.Christense@my2way.com	801-840-4204	Mchriste@dps.state.ut.us
Robert Graves**	Yes	57 West, 200 South Salt Lake City, Utah 84101	877-989-8560 Robert.Graves@my2way.com	202-406-6040 801-524-4090	Rgraves@usss.treas.gov
Jake Hunt	Yes	2451 S 600 West Suite 300 Salt Lake City, UT 84115	877-989-8565 Jake.Hunt@my2way.com	801-840-4201	Jhunt@dps.state.ut.us
Jeff Pittman	Yes	150 East Social Hall Plaza, Suite 500 Salt Lake City, UT 84111	877-989-8561 Jeff.Pittman@my2way.com	801-257-2472	Jpittman@uopsc.net
Steve Proctor	Yes	2451 S. 600 West, Suite 300 Salt Lake City, UT 84115	877-989-8559 Steve.Proctor@my2way.com	801-840-4200	Sproctor@dps.state.ut.us
Floyd Ritter	Yes	6000 State Office Building Salt Lake City, UT 84114	877-989-8562 Floyd.Ritter@my2way.com	801-538-3316	Fritter@dps.state.ut.us

*Technical testers are required to participate in the pilot technical test plan, which will be distributed at a later date. These people will be asked to perform testing within a controlled group for the purpose of performance and use testing. You do not have to be technical to perform these functions.
**Secret Service radio manager resident in Salt Lake City, UT.

SECURE PAGING PILOT PARTICIPANT LIST

UNITED STATES CUSTOMS SERVICE					
NAME	**TECHNICAL TESTER**	**OFFICE LOCATION**	**PAGER NUMBER/ E-MAIL ADDRESS**	**TELEPHONE NUMBER**	**E-MAIL ADDRESS**
Chuck Bussell	Yes	Resident Agent in Charge 905 W. Riverside St, Suite 510 Spokane, WA 99210	877-989-8579 chuck.bussell@my2way.com	509-353-3132	Charles.L.Bussell@Customs.Treas.Gov
Tom Koitzsch	Yes	NLECC-Nashua Field Office 6 Columbia Dr., Suite 6C Amherst, NH 03031	877-989-8577 tom.koitzsch@my2way.com	602-886-1593	Thomas.F.Koitzsch@Customs.Treas.Gov
Chuck Lamb	Yes	Tactical Communications 1300 Pennsylvania Ave NW Rm 6.5B Washington, DC 20229	877-989-8595 chuck.lamb@my2way.com	202-927-0867	Charles.T.Lamb@Customs.Treas.Gov
Sam Russ	Yes	Tactical Communications 1300 Pennsylvania Ave NW Rm 6.5B Washington, DC 20229	877-989-8571 sam.russ@my2way.com	202-927-1028	Sam.Russ@Customs.Treas.Gov
John Santo	Yes	National Law Enforcement Communications Center 1900 Leahy Ave Orlando, FL 32803	877-989-8580 john.santo@my2way.com	407-975-1702	John.Santo@Customs.Treas.Gov

*Technical testers are required to participate in the pilot technical test plan, which will be distributed at a later date. These people will be asked to perform testing within a controlled group for the purpose of performance and use testing. You do not have to be technical to perform these functions.

SECURE PAGING PILOT PARTICIPANT LIST

UNITED STATES SECRET SERVICE					
NAME	**TECHNICAL TESTER***	**OFFICE LOCATION**	**PAGER NUMBER/E-MAIL ADDRESS**	**TELEPHONE NUMBER**	**E-MAIL ADDRESS**
Bob Buchanan	No	950 H Street, NW Washington, DC 20223	877-989-8585 Bob.buchanan@my2way.com	202-406-5366	Rbuchanan@usss.treas.gov
Steve Colo	No	950 H Street, NW Washington, DC 20223	877-989-8568 Steve.colo@my2way.com	202-406-6281	Scolo@usss.treas.gov
Joe Harris	Yes	950 H Street, NW Washington, DC 20223	877-989-8591 Joe.harris@my2way.com	202-406-5365	Jharris@usss.treas.gov
Rick Klenner	Yes	950 H Street, NW Washington, DC 20223	877-989-8566 Rick.klenner@my2way.com	202-406-6017	Rklenner@usss.treas.gov
Jim McDermond	No	950 H Street, NW Washington, DC 20223	877-989-8582 Jim.mcdermond@my2way.com	202-406-5332	Jmcdermond@usss.treas.gov

*Technical testers are required to participate in the pilot technical test plan, which will be distributed at a later date. These people will be asked to perform testing within a controlled group for the purpose of performance and use testing. You do not have to be technical to perform these functions.

SECURE PAGING PILOT PARTICIPANT LIST

FBI/NTIA/PSWN					
NAME	**TECHNICAL TESTER***	**OFFICE LOCATION**	**PAGER NUMBER/E-MAIL ADDRESS**	**TELEPHONE NUMBER**	**E-MAIL ADDRESS**
Don Ashley	No	P.O.Box 3926 Fairfax, VA 22038	877-989-8590 don.ashley@my2way.com	703-279-2009	Donashley@earthlink.net
Bob Lee	No	P.O.Box 3926 Fairfax, VA 22038	877-989-8549 robert.lee@my2way.com	703-279-2007	Springfield01@earthlink.com
Rick Murphy	No	P.O.Box 3926 Fairfax, VA 22038	877-989-8569 rick.murphy@my2way.com	703-279-2037	Rick.murphy@cio.treas.gov
McRae Smith	No	P.O.Box 3926 Fairfax, VA 22038	877-989-8574 mcrae.smith@my2way.com	703-279-2024	Mcraesmith@earthlink.net
Don Speights	No	1401 Constitution NW HCHB Room 4624 Washington, DC 20230	877-989-8583 don.speights@my2way.com	202-482-1726	Wspeights@ntia.doc.gov

*Technical testers are required to participate in the pilot technical test plan, which will be distributed at a later date. These people will be asked to perform testing within a controlled group for the purpose of performance and use testing. You do not have to be technical to perform these functions.

Secure Paging Pilot
Point of Contact List

United States Secret Service
950 H Street N.W.
Washington, DC 20223
ATTN: Joseph Harris, 202-406-5365
E-Mail: jharris@usss.treas.gov
USSS will receive 5 pagers, 1000 msg/mo service for 12 mo. - Per pager, and 5 spare NiMH batteries

Federal Law Enforcement Training Center
ISD Townhouse 389
Glynco, GA 31524
ATTN: Eric Travis, 912-267-3254
E-Mail: etravis@fletc.treas.gov
FLETC will receive 5 pagers, 1000 msg/mo service for 12 mo. - Per pager, and 5 spare NiMH batteries

United States Customs Service
Tactical Communications
1300 Pennsylvania Avenue, N.W.
Room 6.5B
Washington, DC 20229
ATTN: Charles Lamb, 202-927-0867
E-Mail: charles.t.lamb@customs.treas.gov
Customs will receive 5 pagers, 1000 msg/mo service for 12 mo. - Per pager, and 5 spare NiMH batteries

Public Safety Wireless Network Program
P.O. Box 3926
Fairfax, VA 22038
ATTN: Julio "Rick" Murphy, 703-279-2037
E-Mail: rick.murphy@cio.treas.gov
PSWN will receive 11 pagers, 1000 msg/mo service for 12 mo. - Per pager, and 11 spare NiMH batteries (this total includes pagers for both the PSWN Program and FBI)

Wireless Program Office
United States Department of the Treasury
1425 New York Avenue, N.W.
Washington, DC 20220
ATTN: Darrell Smith, 202-622-5198
E-Mail: darrell.smith@do.treas.gov
WPO will receive 5 pagers, 1000 msg/mo service for 12 mo. - Per pager, and 5 spare NiMH batteries

United States Department of the Treasury
1425 New York Avenue, N.W., Room 2155
Washington, DC 20220
ATTN: Mayi Canales, 202-927-7449
E-Mail: mayi.canales@do.treas.gov
Treasury (DASIS) will receive 5 pagers, 1000 msg/mo service for 12 mo. - Per pager, and 5 spare NiMH batteries

Utah Communications Agency Network
2451 S. 600 West, #300
Salt Lake City, Utah 84105
ATTN: Steven Proctor, 801-840-4200
E-Mail: sproctor@dps.state.ut.us
UCAN will receive 5 pagers, 100 msg/mo service for 12 mo. – Per pager, and 5 spare NiMH batteries

APPENDIX B—TEST PLANS AND RESULTS

SECURE PAGING PILOT
PHASE 1 TEST PLAN

During Phase I, three different tests will be conducted: 1. Pager-to-Pager, 2. Email-to-Pager, and 3. Response Time. Testing will involve 45 pagers total; 33 pagers will be maintained by a technical staff, 12 pagers will be maintained by non-technical staff; 1 pager will serve as the main testing unit. Phase I testing will last for seven days.

NOTE: Responding messages must be ENCRYPTED.

Test Schedule		
Day 1	10/15/01	Test 3: Response Time Testing
Day 2	10/16/01	Test 1: Pager-To-Pager Testing
Day 3	10/17/01	Test 3: Response Time Testing
Day 4	10/18/01	Test 2: Email-To-Pager Testing
Day 5	10/19/01	Test 3: Response Time Testing
Day 6	10/21/01	Test 3: Response Time Testing

1. PAGER-TO-PAGER TESTS (Technical Testers Only)		
Testing Date: 10/16/01		
• *Test #*	• *Transmit Time*	• *Test Message Notes*
Test 1a	**7:00 AM**	**Unencrypted** message not exceeding **500** characters
Test 1b	**9:00 AM**	**Unencrypted** message not exceeding **1000** characters
Test 1c	**11:00 AM**	**Unencrypted** message not exceeding **1500** characters
Test 1d	**1:00 PM**	**Encrypted** message not exceeding **500** characters
Test 1e	**3:00 PM**	**Encrypted** message not exceeding **1000** characters
Test 1f	**5:00 PM**	**Encrypted** message not exceeding **1500** characters

Sample Test Message:
Test 1a sent at 0700: Reply to test 1a with an **encrypted response** indicating time received. (Example text: This is to take up space and add more characters. This is to take up space and add more characters…)

Sample Test Response Message:
test 1a rec 0702

Additional Note:
In some cases, the test message may be sent in sections, automatically broken up by the network. If a test message is received in multiple parts, please add how many sections were received in addition to the responses (e.g., test 1c 5 of 5 rec ok 1102)

2. EMAIL-TO-PAGER TESTS (Technical Testers Only)		
Testing Date: 10/18/01		
• *Test #*	• *Transmit Time*	• *Test Message Notes*
Test 2a	**7:00 AM**	**Unencrypted** message not exceeding **500** characters
Test 2b	**9:00 AM**	**Unencrypted** message not exceeding **1000** characters
Test 2c	**11:00 AM**	**Unencrypted** message not exceeding **1500** characters
Test 2d	**1:00 PM**	**Encrypted** message not exceeding **500** characters
Test 2e	**3:00 PM**	**Encrypted** message not exceeding **1000** characters
Test 2f	**5:00 PM**	**Encrypted** message not exceeding **1500** characters

Sample Test Message:

Test 2e sent at 1500: Reply to test 2e with an **encrypted response** indicating time received. (Example text: This is to take up space and add more characters. This is to take up space and add more characters…)

Sample Response Message:

test 2e rec 1503

Additional Note:

In some cases, the test message may be sent in sections, automatically broken up by the network. If a test message is received in multiple parts, please add how many sections were received in addition to the responses (e.g., test 2f 5 of 5 rec ok 1701).

3. RESPONSE TIME TESTS (All Participants)		
Testing Dates: 10/15/01, 10/17/01, 10/19/01, 10/21/01		
• *Test #*	• *Transmit Time*	• *Test Message Notes*
Test 3a	**8:00 AM**	**Encrypted** message
Test 3b	**10:00 AM**	**Encrypted** message
Test 3c	**12:00 PM**	**Encrypted** message
Test 3d	**3:00 PM**	**Encrypted** message
Test 3e	**5:00 PM**	**Encrypted** message

Sample Test Message:

Test 3a sent at 0800: Reply to test 3a with an **encrypted response** indicating time received. Please indicate if this message was received at or after 0805. (Example text: This is to take up space and add more characters. This is to take up space and add more characters…)

Sample Response Message (if message WAS received within the 5 min test window):

test 3a rec 0802

Sample Response Message (if message WAS NOT received within the 5 min test window):

test 3a no rec 0807

Additional Note:

If the message was received *within the 5 minute test window, but the participant was unable to respond immediately*, the participant is still expected to send a confirmation message back to the main testing unit stating the time of receipt as soon as possible (i.e., **rec 3a 0802 delayed response**).

SECURE PAGING PILOT
PHASE II TEST PLAN

During Phase II, three different tests will be conducted: 1) Metrocall Pager-to-SkyTel Pager; 2) Email-to-SkyTel Pager; and 3) SkyTel Pager-to-Metrocall Pager. Testing will involve one Metrocall Pager and 10 SkyTel pagers for Tests 1 and 2. For Test 3, a SkyTel pager will transmit a page to all previously designated Treasury technical testers. The 10 SkyTel pagers will be maintained by USSS technical staff; and the Metrocall pager will serve as the main testing unit. Phase II testing will last for three days.

CAUTION: The secure text feature offered by the V-Client software is not intended for the transmission of any classified information.

TEST SCHEDULE			
Day 1	11/27/01	Test 1: Metrocall Pager-to-SkyTel Pager	USSS participants
Day 2	11/28/01	Test 2: Email-to-SkyTel Pager	USSS participants
Day 3	11/29/01	Test 3: SkyTel Pager to Metrocall Pager	All technical testers

NOTE: Secure response messages from users must be sent through the V-Client.

1. METROCALL PAGER-TO-SKYTEL PAGER TEST		
Testing Date: 11/27/01		
• *Test #*	• *Transmit Time*	• *Test Message Notes*
Test 1a	**9:00 AM**	Text message not exceeding 500 characters
Test 1b	**11:00 AM**	Text message **exceeding** 500 **c**haracters
Test 1c	**1:00 PM**	**Secure** text message not exceeding 500 characters
Test 1d	**3:00 PM**	**Secure** text message **exceeding** 500 characters
Sample Test Message: Test 1a sent at 0900: Reply to test 1a with a **secure response** indicating time received. **Sample Response Message:** **test 1a rec 0904**		
Additional Note: In some cases, the test message may be sent in sections, automatically segmented by the network. The user may have to send a request back to the network to obtain the segments that have not yet been sent.		

2. EMAIL-TO-SKYTEL PAGER TEST		
Testing Date: 11/28/01		
• *Test #*	• *Transmit Time*	• *Test Message Notes*
Test 2a	**9:00 AM**	Text message not exceeding 500 characters
Test 2b	**11:00 AM**	Text message **exceeding** 500 characters
Test 2c	**1:00 PM**	**Secure** message not exceeding 500 characters
Test 2d	**3:00 PM**	**Secure** message **exceeding** 500 characters
Sample Test Message: Test 2a sent at 0900: Reply to test 2a with a **secure response** indicating time received. **Sample Test Response Message:** **test 2a rec 0902**		
Additional Note: In some cases, the test message may be sent in sections, automatically segmented by the network. The user may have to send a request back to the network to obtain the segments that have not yet been sent.		

3. SKYTEL PAGER-TO-METROCALL PAGER TEST		
Testing Date: 11/29/01		
• *Test #*	• *Transmit Time*	• *Test Message Notes*
Test 3a	**9:00 AM**	Text message not exceeding 500 characters
Test 3b	**11:00 AM**	Text message **exceeding** 500 characters
Test 3c	**1:00 PM**	**Secure** message not exceeding 500 characters
Test 3d	**3:00 PM**	**Secure** message **exceeding** 500 characters
Sample Test Message: Test 3b sent at 0900: Reply to test 3b with a **secure response** indicating time received. (Example text: This text takes up space, this text takes up space, this test takes up space…) **Sample Test Response Message:** **test 3b rec 0902**		
Additional Note: In some cases, the test message may be sent in sections, automatically segmented by the network. The user may have to send a request back to the network to obtain the segments that have not yet been sent.		

APPENDIX C—TEST ISSUES AND RESOLUTIONS

APPENDIX C—TEST ISSUES AND RESOLUTIONS

ISSUE STATUS LIST FOR SECURE 2-WAY PAGING PILOT AS OF 10/30/2001

	ISSUE	NOTES	SOLUTION	RESOLVED
1	W2 Server Issue - Pager aliases not configured correctly, cannot send/receive encrypted pages		❖ Qwest worked with W2 and V-One to correct the desktop to pager encrypted network. Pager to desktop communications is still being addressed.	YES
2	Some pagers are not fully configured with V-Client (not registered and not able to send encrypted pages)	❖ Pagers sent to FLETC were not provisioned will all the necessary files to run the V-Client properly	❖ Chris Brook (V-One) contacted users to walk them through V-Client registration procedures ❖ FLETC has been contacted. Darrell will help FLETC users reinstall V-Client and register pager with V-One server	YES
3	Number of users that an encrypted page can be sent to (via Pager) is only 10, any more causes pager to hang	❖ Appears to be a Motorola equipment issue ❖ Pager-to-pager tests on 10/25 that required a 1000 or 1500 character message to be sent were unsuccessful and could not be tested. ➢ Booz Allen was able to send test messages with roughly 300 characters in the body of the message to groups of 10 users at once. ❖ If a message is sent with more characters than the pager can handle, the pager will get stuck in an infinite loop of attempting to send the message unsuccessfully.	❖ There is a 500 character limitation when sending messages pager-to-pager. This character count includes user aliases, subject line, and body. ❖ Chris Brook successfully sent a group message to 15 users. A limited message (only 20 characters) with a short subject line was sent.	ONGOING
4	Cannot beam V-Client from pager to pager	❖ All necessary files will not be installed on the pager if V-Client is beamed from pager to pager.	❖ Pagers ***must*** be provisioned via PC link, otherwise. ❖ Any future implementation of V-Client must be provisioned by V-One or authorized Treasury personnel ***prior*** to being sent to users	ONGOING
5	Software on W2 server needs to be updated for Metrocall/SkyTel Interoperability	❖ Relevant for Phase 2 testing ❖ Phase 2 testing scheduled for 11/12/01-11/15/01	❖ V-One is currently implementing code to resolve this issue. This will be completed in approximately 3 days.	YES

	ISSUE	NOTES	SOLUTION	RESOLVED
6	Encrypted pages cannot be routed to a PC outside of the Treasury firewall	❖ Booz Allen cannot receive encrypted responses from test participants. ❖ Booz Allen can send encrypted pages from PC, but message will be sent unencrypted to Treasury network via public internet before encryption is applied.	❖ Darrell Smith conducted email-to-pager testing ➢ Responses were forwarded to Booz Allen for recording and analysis.	ONGOING
7	Some delays were experienced receiving messages during distance testing conducted 10/25 from Olympic venues in SLC to Washington Metro area	❖ Not all routes to Olympic venues have *two-way* paging coverage. ❖ Messages were stored and forwarded to pagers when coverage improved. ❖ Patti Wood has requested coverage maps of the SLC area from Metrocall	❖ Resolved in conjunction with issue #5	YES
8	Unable to send messages to SkyTel pagers from both PC and Metrocall pagers.	❖ Messages sent would be returned with an error stating that the message delivery was unsuccessful to SkyTel address.	❖ Darrell Smith resolved this issue by calling SkyTel and having them fix the provisioning error that caused it.	YES

APPENDIX D—USER INFORMATION SURVEY

SECURE PAGING PILOT
User Information Survey

I. Contact Information

1. Please provide the following information:

Name	Agency/Position/Division
Telephone Number/Email Address	Business Address
(T) (E)	

II. Training

1. Did you participate in the pager training session?

   Yes ✖ No ✖

2. Did you find the training to be adequate?

   Yes ✖ No ✖

   What other information would have been helpful (e.g., training aids, follow-up training)?

   _____
   _____
   _____
   _____

III. Security

1. How would you rate the process for encrypting text messages?

Easy	✖	Very Difficult	✖
Moderately Easy	✖	Unable to successfully encrypt text	✖
Difficult	✖	Did not attempt	✖

2. How often did you use the encryption feature?

All of the time (100%)	✖	Some of the time (25%)	✖
Most of the time (75%)	✖	Seldom (less than 25%)	✖
Half of the time (50%)	✖	Did not use	✖

3. Do you think there is value in using the encryption feature?

   Yes ✖ No ✖

4. Do you have a need to send classified information?

   Yes ✖ No ✖

5. Would you recommend this (secure paging) service offering to your field office or division?

   Yes ✖ No ✖

   If no, please indicate reason.

Secure paging service currently in use	✖	No funding available	✖
Not useful	✖	Other: _____ _____ _____	✖

IV. Service

1. Did you travel outside your local area during the paging pilot?

   Yes ✖ No ✖

   If yes, please list all locations outside of your home area, in which you used this service (e.g., Salt Lake City, UT, Gettysburg, PA).

   _____
   _____
   _____
   _____

2. Were you able to send and receive pages from all locations?

   Yes ✖ No ✖

   If no, please provide the locations from which paging service was inadequate.

   _____
   _____
   _____
   _____

3. Did you receive any error messages?

   Yes ✖ No ✖

   If yes, please indicate they type of error message and describe how the issue was resolved.

   _____
   _____
   _____
   _____

4. Does your field office or division currently have a two-way paging service?

   Yes ✖ No ✖

IV. Latency

1. Did you experience any significant latency when sending messages (i.e., delays when attempting to send or receive messages)?

   Yes ✖ No ✖

   If yes, approximately how long was the delay?

Less than 5minutes	✖	Less than 1 day	✖
Less than 1 hour	✖	More than 1 day	✖
More than 1 hour	✖	Other: _____ _____	✖

V. Functionality

1. Did you use a two-way pager to send messages to another pager?
   Yes ✖ No ✖

   If yes, were pages successfully received by the intended recipient?

   Yes ✖ No ✖

2. Did you use e-mail to send messages to a pager?

   Yes ✖ No ✖

   If yes, were pages successfully received by the intended recipient?

   Yes ✖ No ✖

3. Did you use a two-way pager to send messages to an email account?
   Yes ✖ No ✖

   If yes, were pages successfully received by the intended recipient?

   Yes ✖ No ✖

4. Please provide additional comments concerning the pager test.

   _____
   _____
   _____
   _____

Administrator Survey

I. Installation, Configuration, and Administration

1. Did you experience any installation issues?

   Yes ✖ No ✖

   If yes, please explain.

   _____
   _____
   _____
   _____

2. Did you experience any configuration issues?

   Yes ✖ No ✖

   If yes, please explain.

   _____
   _____
   _____
   _____

3. Did you experience any difficulties while using the administration software?

   Yes ✖ No ✖

   If yes, please explain.

   _____
   _____
   _____
   _____

4. Do you have concerns or issues related to the Air Smart Gate Server?

   Yes ✖ No ✖

   If yes, please explain.

   _____
   _____
   _____
   _____

II. Messaging and Software Capabilities

1. Were you able to form groups to test the broadcast page capability?
   Yes ✖ No ✖

   If no, please explain.

   _____
   _____
   _____
   _____

2. Were you able to successfully send group pages?
   Yes ✖ No ✖

   If no, please explain.

   _____
   _____
   _____
   _____

3. Did you receive appropriate confirmation responses?

   Yes ✖ No ✖

4. Did you create system reports?

   Yes ✖ No ✖

   If yes, please explain.

   _____
   _____
   _____
   _____

5. Please provide additional comments concerning the pager test.

   _____
   _____
   _____
   _____

APPENDIX E—CALL USAGE DATA

APPENDIX E

The following pages show the call usage data collected by the V-One secure paging server. Pages E-2 through E-10 present the call usage data collected between January 10, 2002 – February 10, 2002. Pages E-11 through E-20 present the call usage data collected between February 10, 2002 – March 10, 2002. To maintain the integrity of the data, no data shown was hand-keyed. Rather, the data was photocopied onto pages formatted to be consistent with the remainder of this report. The call usage data will be analyzed by the Department of the Treasury's Wireless Programs Office for user trends and other operational aspects regarding the use of the secure paging units.

APPENDIX F—LIST OF ACRONYMS

ACRONYMS

DASIS	Department of the Assistant Secretary of Information Systems
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
LAN	Local Area Network
LCD	Liquid Crystal Display
MEK	Message Encryption Key
MHz	Megahertz
MOU	Memoranda of Understanding
NiMH	Nickel-Metal Hydride
NOC	Network Operation Center
NSA	National Security Agency
PC	Personal Computer
PIN	Personal Identification Number
PSWN	Public Safety Wireless Network
RC4	Ron's Code 4
RSA	Rivest-Shamir-Adleman
SHA	Secure Hashing Algorithm
SLC	Salt Lake City
SMTP	Simple Mail Transfer Protocol
TCS	Treasury Communications System
UCAN	Utah Communication Agency Network
USCS	United States Customs Service
USSS	United States Secret Service
WPO	Wireless Program Office
VPN	Virtual Private Network