United States
Department of
Agriculture

Forest Service

Technology &
Development
Program

6600–CIO
November 2009
0966–2839–MTDC

MIMIT Pilot Project Report

Lessons Learned

MIMIT Pilot Project Report

Lessons Learned

Andy Trent
Project Leader
Missoula Technology and Development Center

Michael Morgen
MIMIT Project Business Lead
Bureau of Land Management

Theron Miller
Project Leader
Missoula Technology and Development Center

Doug Stefan
Quality Management Analyst
Forest Service Chief Information Office

USDA Forest Service
Technology and Development Center
Missoula, MT

OE02P98—CIO Thin Client Pilot Project

November 2009

The Forest Service, United States Department of Agriculture (USDA), has developed this information for the guidance of its employees, its contractors, and its cooperating Federal and State agencies and is not responsible for the interpretation or use of this information by anyone except its own employees. The use of trade, firm, or corporation names in this document is for the information and convenience of the reader and does not constitute an endorsement by the Department of any product or service to the exclusion of others that may be suitable.

The U.S. Department of Agriculture (USDA) prohibits discrimination in all its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex, marital status, familial status, parental status, religion, sexual orientation, genetic information, political beliefs, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD).

To file a complaint of discrimination, write to USDA, Director, Office of Civil Rights, 1400 Independence Avenue, S.W., Washington, D.C. 20250-9410, or call (800) 795-3272 (voice) or (202) 720-6382 (TDD). USDA is an equal opportunity provider and employer.

Contents

Executive Summary iii
Introduction 1
Background 3
Fiscal Year 2007 3
Fiscal Year 2008 3
Fiscal Year 2009 4
MIMIT Pilot Project Accomplishments Before 2009 Deployments 5
Trailer Design and Fabrication 5
MIMIT Standard Operating Procedures and Web Site 6
Computer Technical Specialist Training 7
Wireless Configuration 7
Active Directory and Federal Desktop Core Configuration 8
Security Assessment 8
Help Desk 8
Hardware Purchase 8
Great Basin Geographic Area MIMIT Deployment Summaries 9
Red Rock Fire 9
Big Pole Fire 11
Hoyt Fire 12
Mill Flat Fire 13
Gunsight Fire 14
Informal User Responses 15
What Did We Study? 15
What Components of the System Did Respondents Use? 16
Relative Merits of the MIMIT System 17
Evaluation of System Functionality 18
Cost-Benefit Analysis 20
Background of the Cost-Benefit Analysis 20
Results of the Cost-Benefit Analysis 20

Executive Summary

The Interagency Interoperability Oversight Group (IIOG) funded an interagency team to continue development and evaluation of the Mobile Incident Management Information Technology (MIMIT) system during fiscal year 2009. The project's goal was to assess the system's ability to meet the information technology (IT) needs of incident management teams, the system's ease of deployment and system administration, and overall user satisfaction. Additionally, the IIOG provided funding for a cost-benefit analysis comparing the cost of ownership of a national cache of completely outfitted MIMIT trailers to the cost of contracting equivalent IT services.

The 2009 MIMIT evaluation was intended to solve two important problems identified during the 2008 fire season. First, personnel needed to be tasked specifically with the responsibility of moving the project forward. A project lead and business lead were funded to support the project. Second, trailers were needed to store the IT equipment so it would be ready for deployment, to provide an environmentally protected and secure area for the server, and to provide working space for incident management team members.

The 2009 MIMIT project funding also allowed additional equipment to be purchased and was used to pay a detailer to develop a cost-benefit analysis. The funds were also used to pay developers to document MIMIT system deployment and troubleshooting. Designers were funded to prepare a Web site, and a contractor was hired to establish a help desk.

A wireless solution, based on a U.S. Department of the Interior (DOI) incident command post pilot project in 2008, was successfully integrated and tested with the MIMIT system during 2009. A technical vulnerability assessment of the MIMIT system was completed by the Bureau of Land Management's IT security program at the National Interagency Fire Center (NIFC).

The MIMIT system was tested during 2009 deployments in the Great Basin Geographic Area. Training on operation of the MIMIT system was provided to all Great Basin computer technical specialists (CTSPs) before the field season. The MIMIT system was deployed on every Type 1 and Type 2 incident (five incidents) during the relatively inactive fire season in the Great Basin. None of the incidents lasted long enough for a team transition. Major lessons learned during the deployments include:

- The MIMIT standard configuration of hardware, software, and wireless network met incident needs.
- After CTSP training, CTSPs successfully managed the MIMIT system.
- The cache concept of refurbishing the MIMIT trailers established a standard approach for cached equipment and provided consistent quality of service.
- The use of the trailer exceeded expectations, providing immediate working space for incident personnel while the rest of camp was being set up and space for holding planning meetings and building incident action plans.
- An effective communication plan between the Eastern and Western Great Basin Coordination Centers, incident commanders, CTSPs, and the interagency MIMIT team was essential for timely mobilizations and project success.
- The wireless local area network (WLAN) connectivity using a wireless LAN controller and wireless access points was successful.
- Because the MIMIT system has not been deployed on an incident that lasted long enough for one incident management team to be replaced by another, transition processes and procedures have not been evaluated.
- The router/firewall had several technical problems that were restored with a reset. The cause of these problems should be investigated.
- The trailer air conditioning units tended to freeze up. A higher capacity air conditioning unit may be needed.
- Some incident personnel using personal computers would like access to the WLAN for Internet access. A secure, monitored solution should be developed for consideration.

Users provided feedback on the MIMIT system during four incidents. Most of the 22 respondents rated the MIMIT system favorably compared to other systems they had used on incidents. They also felt they were more productive using the MIMIT equipment. Most respondents indicated that they would prefer to use a system like MIMIT during future assignments. Problems identified by the respondents included the lack of USB drives (this problem was fixed after the first incident), inability to access internal Government Web sites and resources, and the unavailability of certain applications.

A cost-benefit analysis was developed to determine whether funding the MIMIT system beyond the pilot stage provides a favorable return on investment (ROI) and reasonable payback period. Three program options were evaluated; no additional MIMIT trailers, adding 10 completely outfitted MIMIT trailers, and adding 20 completely outfitted MIMIT trailers to the inventory. The total program cost (hardware, personnel, facilities, equipment replacements, etc.) for a 10-year period was compared to the cost of contracting similar services. Option 3, the addition of 20 completely outfitted MIMIT trailers, was the most economical. The return on investment was the greatest and payback time the shortest. Based on historical information, this option will support 80 percent of all incidents during the peak months of the fire season. The ROI and payback period improve significantly if the MIMIT trailers are used to support other missions, such as Type 3 incidents, training, or natural disasters. The total cost of implementing the recommended program during fiscal year 2010 is about $2.6 million.

Introduction

A rapidly deployed, easily managed information technology system has been developed for incident management. The Mobile Incident Management Information Technology (MIMIT) system stores and deploys incident command post (ICP) computer and networking hardware and software from a trailer (figure 1). The equipment is configured before incidents so it can be deployed and set up quickly. The MIMIT system provides standardized equipment and procedures for incident management support and provides consistent support to incidents.

The MIMIT system is ordered from a national cache and assigned for the duration of the incident. This cache-standardized approach is a departure from the current system where teams provide or contract for their technology support. The Interagency Interoperability Oversight Group (IIOG) sponsored the 2009 pilot project that continued the development and evaluation of the MIMIT system in the Great Basin Geographic Area. The pilot project assessed the MIMIT system's ability to meet the information technology (IT) needs of incident management teams, its ease of deployment and system administration, and overall user satisfaction. Additionally, the IIOG provided funding for a cost-benefit analysis (CBA) comparing the cost of ownership of a national cache of completely outfitted MIMIT trailers to the cost of contracting similar services.

The MIMIT system includes a terminal server, wireless LAN (local area network) controller, wireless access

Figure 1—The MIMIT trailer provides a secure and environmentally protected space for the server and other equipment. The trailer and IT equipment are configured before incidents so they can be deployed and set up rapidly. The trailer also provides a working space for the incident's computer technical specialist and other incident personnel.

points, mobile thin clients (laptops without hard drives), laptops, printers, and associated networking equipment. The standardized components are configured to meet the needs of incident management teams.

The equipment is stored in a 20-foot air-conditioned trailer that is towed to the incident. The trailer is set up with workstations that are ready for use once the trailer arrives. The MIMIT system will support the incident from beginning to end, a change from the present system where each team brings its own computer and networking equipment to an incident (and takes the equipment when it leaves).

Most persons working at an ICP will access applications and data by connecting to the server from a mobile thin client. The mobile thin clients (figure 2) are relatively inexpensive computers with no hard drives that access the server through a wireless local area network (WLAN), although they can be connected with a network cable. All applications run on the server and all files are stored there. Benefits of the system include:

- A stable, secure IT environment. The entire incident's data (including personally identifiable information) is stored centrally on the server—not on the individual mobile thin clients. User accounts and permissions are managed centrally on the server.
- Quick deployment and setup. All the equipment is configured and ready for setup. The MIMIT trailer can be ready for use within half an hour after it arrives at an incident.

Figure 2—Mobile thin clients are used by most camp personnel to access applications and store data on the server. Thin clients are inexpensive computers that store little data, relying instead on access to a server.

- Smoother transitions between incident management teams. The server and computers will stay at the incident through team rotations.
- Consistent operational procedures.
- Standardized, reliable hardware and software will make training and troubleshooting easier.
- Flexibility. The wireless mobile thin clients and laptop computers can be moved easily because the computer network isn't strung together with wires.
- Quick, reliable refurbishing. After an incident, the MIMIT trailers can be refurbished by the National Interagency Cache System so they're ready for deployment at the next incident.

Background

Information technology and networking requirements are critical at an ICP. Most functions at ICPs require data input, management, and storage or require access to the Internet. I-Suite, the most commonly used application, consists of integrated resource, cost, time, planning, and supply modules. Other applications, such as ArcGIS and Google Earth, are used by GIS specialists. Standard Microsoft Office applications are used by ICP personnel to create reports and share information.

Now, incident management teams (IMTs) usually provide their own IT equipment at an incident. Most IMTs have at least one CTSP who sets up and manages the equipment and network. A few teams hire contractors for this function. Contracts allow teams to rent laptops and other networking equipment if needed.

The current model where teams supply and manage (or contract) their own equipment has many drawbacks. The traditional setup and deployment of IT equipment at an ICP has been almost exclusively based on laptop PCs. Generally, the laptops represent whatever the team has been able to acquire (often surplus equipment) and rental equipment. Providing incidents with inconsistent computer support is a cause for concern on many levels. Security, experience, reliability, transitions, and availability are key issues. Teams are not equally equipped. Some hit the ground running, while others limp into the incidents with less than reliable equipment and can be almost paralyzed while waiting on rental equipment. Preordering equipment does little to alleviate this problem, as orders can take days to be filled. Wait times for rental equipment can be 48 to 72 hours, with even longer delivery times for incidents in remote areas.

Fiscal Year 2007

Two CTSPs from the National Park Service successfully tested a new model for delivering IT and network services to the ICP. They implemented and tested a prototype system using a terminal server and mobile thin clients. Their goals were to provide a more stable and robust network environment for incident management.

Specifically, the terminal server was intended to:

- Increase physical and logical security with the introduction of mobile thin clients
- Provide a stable network environment for incident management
- Decrease network lag time
- Improve system availability for users
- Establish a consistent work environment for users on incidents
- Ensure a single location for incident file storage
- Simplify network printing for users
- Reduce the daily operating costs for an incident's IT infrastructure

Four terminal server/mobile thin client kits were developed with funding from the National Park Service and the other participating Federal agencies. Each kit contained a terminal server (supplied by the agency or team carrying the kit) and 10 Hewlett Packard thin clients. The kits were set up on some new incidents and replaced established networks on other incidents.

Fiscal Year 2008

An interagency team was formed to pilot the project in 2008. Team members represented the Forest Service, Bureau of Land Management, National Park Service, and Bureau of Indian Affairs. The team presented the concept and advantages of the using the terminal server/thin client model to the National Wildfire Coordinating Group (NWCG) at Boise, ID. The NWCG funded the team to purchase additional equipment, support two detailers, and test the systems at incidents across the country. In addition, the concept was presented to the Chief Information Officers (CIOs) of several agencies at a summit in Boise. The NWCG funding purchased enough components for five terminal server/thin client kits. The kit components included servers, mobile and desktop thin clients, monitors, keyboards, mice, printers, switches, and miscellaneous networking equipment. Hard plastic shipping cases were purchased to protect the equipment. In the spring of 2008, Vaughn Stokes, the

Forest Service's CIO, funded the Missoula Technology and Development Center (MTDC) to evaluate thin clients and assist with project management.

The terminal server/thin client kits were deployed on three fires in 2008, two in New Mexico and one in California. Informal responses indicated users liked the terminal server/thin client kits.

One lesson learned during 2008 was that the project had outgrown its ad hoc roots and required personnel specifically tasked with managing and administering the equipment. Additionally, trailers were needed to safely transport the equipment and protect it at an ICP. Even though the equipment was packaged in rugged plastic cases, servers and other equipment were being damaged. Additionally, a secure, environmentally protected area was needed to operate the server at the ICP. Trailers allow the IT equipment to be packaged and preconfigured. The trailer also provides office space, of particular importance during the early hours of an incident.

Fiscal Year 2009

The IIOG, made up of agency CIOs and other staff, funded the pilot project to continue testing the terminal server/thin client model. The IIOG wanted to implement the new approaches developed during 2008 and conduct more field deployment tests. Funding was approved to support two employees to manage and evaluate the equipment purchased during 2008. In addition, funding was approved to purchase trailers, develop deployment documentation, conduct training, integrate a secure wireless solution, test the system at ICPs, and develop a cost-benefit analysis.

This report describes of the MIMIT pilot project's progress during 2009.

MIMIT Pilot Project Accomplishments Before 2009 Deployments

During 2009, the MIMIT project continued implementing security measures and developing the system.

Trailer Design and Fabrication

One of the main lessons learned during 2008 was that an air conditioned deployment trailer was needed to store all the equipment and provide a cool, environmentally protected workspace for the server. ICPs can be hot, dusty, and smoky; not an ideal environment for a high-powered server. If the server gets too hot (about 100 degrees Fahrenheit), it will shut itself down. Operating the server in a cooler, dust-free environment extends its life. As the amount of IT equipment needed to support an ICP increases (for example more printers and the wireless networking system), the best way to deploy the equipment is in a trailer.

MTDC engineers conducted a MIMIT trailer design review with Great Basin CTSPs. Based on MTDC's final design, the trailer is:

- 20 feet long by 8 feet wide with enough space for the server, three work areas, storage for the mobile thin clients (figure 3), printers, wireless access points, and other networking equipment.
- Hard wired with network data ports and power outlets (external and internal) for ease of setup (figures 4 and 5).
- Equipped with two access doors. One access door opens to a ramp for loading and unloading equipment.
- Equipped with a Honda 6,500-watt generator capable of operating the trailer, including the air conditioner.
- Equipped with a 32-inch wide screen monitor (figure 6).

Five commercial cargo trailers were procured and delivered to MTDC. MTDC employees installed all the interior cabinets and countertops (figure 7), the power and network wiring, lighting, and generator. A full systems test was completed to make sure the trailers were ready for deployment to the National Interagency Fire Center (NIFC).

Figure 3—Two large storage cabinets inside the trailer hold the mobile thin clients, printers, and networking hardware.

Figure 4—The trailer has three work areas wired with data ports and electrical power.

Figure 5—A hatch door on the side of the MIMIT trailer allows access to the power circuits (4) and external networking data ports (12) that connect to network cables at the incident command post.

Figure 6—A wide-screen monitor in the back of the MIMIT trailer can be used to view maps and other detailed images.

Figure 7—MTDC employees installed custom cabinets and other components inside the MIMIT trailers. Electricians installed the power and network wiring. The trailers were delivered to NIFC in May 2009.

MIMIT Standard Operating Procedures and Web Site

The development of standard operating procedures (SOPs) for the CTSPs was one of the key tasks identified for successful implementation of the MIMIT system. A contractor (Benchmark Safety and Research) was hired to assemble the SOPs. The contractor also developed a password-protected wiki-style Web site (https://www.mimitonline.net) where the SOPs can be easily accessed and updated. SOPs were developed in the following areas:

- **Basics—**Describes the MIMIT trailer's inventory, software loaded on the server, device naming conventions, optimum network layout, default network and IP schemes for the mobile thin clients, printers, laptops, and other devices.
- **Quick Start Guides—**Explain how to power up the trailer, initialize the server, create user accounts, and connect mobile thin clients and laptops to the network.
- **Customize the Network—**Includes the SOPs describing how to provide access to team files and custom applications and to set up I-Suite.
- **Expanding the Network—**Contains procedures explaining how to add printers, plotters, user accounts, laptops, and other computers to the network.
- **System Monitoring and Troubleshooting—**Describes how to monitor the wireless network from the wireless LAN controller, check fuel and oil levels on the generator, and keep the printers operating. It also has a troubleshooting section for problems CTSPs may encounter and describes how to contact the help desk.
- **Other Guides—**Describes what CTSPs should do during team transitions and demobilization. It also includes manuals for different components of the MIMIT system.

Each of the pages of the MIMIT Web site has a discussion section where questions or comments can be added by the CTSPs.

Computer Technical Specialist Training

A 2-day training class for the Great Basin CTSPs was conducted during May 2009. The training class was intended to give the CTSPs an overview of the MIMIT system, describe the strategic plan for deploying the MIMIT system in the Great Basin, and run through examples of typical tasks such as adding computers and user accounts and monitoring the wireless LAN controller.

The five MIMIT trailers were ready in time for the training (figure 8). The CTSPs were broken into small groups and went through mock deployments using the computer and network equipment in the trailers.

The CTSPs who administered the MIMIT system during the fire season had very little difficulty setting it up, thanks in part to the training they received.

Figure 8—Great Basin Geographic Area CTSPs were provided hands-on training on the setup and operation of the MIMIT system during May 2009.

Wireless Configuration

The IIOG requested the MIMIT pilot project to develop and test a wireless network for ICPs. The MIMIT system uses a Cisco wireless LAN controller (Model 2106) and lightweight wireless access points (Model LWAP 1240 AG) to make up a secure wireless network for the ICP. The wireless access points connect to the network through the wireless LAN controller. The wireless LAN controller manages the configuration, firmware, and control transactions, such as 802.1x authentications. In addition, all wireless data traffic is tunneled through the controller.

The U.S. Department of the Interior funded a pilot project in 2008 to develop and test a secure wireless network for various situations, including a mobile solution for incident camps (figure 9). A prototype wireless network was tested successfully in the Great Basin geographic area during the fire season of 2008. That configuration was the basis for the MIMIT's wireless network.

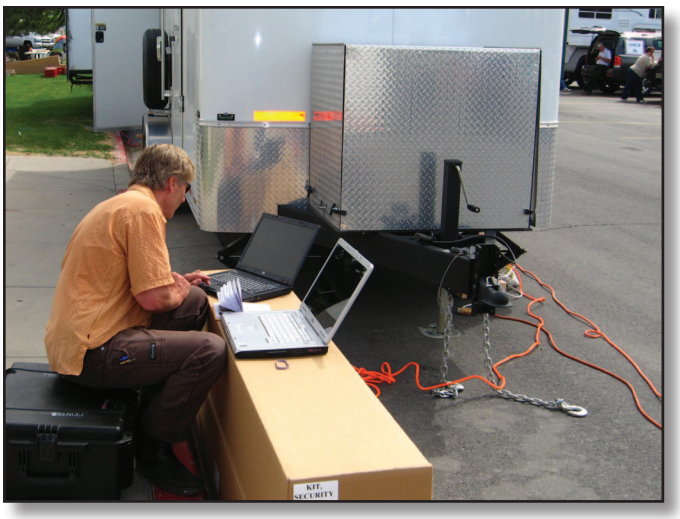

Figure 9—The MIMIT wireless network provides a secure wireless connection to the server applications and the Internet. The MIMIT system can be ready in less than 30 minutes after arriving at an incident. At the Big Pole Fire, one incident management team member used the WLAN outside the MIMIT trailer while the rest of camp was being set up.

Active Directory and Federal Desktop Core Configuration

The MIMIT uses Windows Server 2003. Clients log onto the server using Remote Desktop Protocol (RDP). In 2009, the MIMIT system switched from a workgroup (peer-to-peer) model of grouping the server and clients to a domain model using Active Directory. The domain model has several advantages. It allows administrators to manage accounts and assign policies more easily. Each user is assigned a unique user account and password. The overall security of the network is enhanced. The domain model also allows the MIMIT system to use group policy to provide centralized configuration of the user accounts that control users' working environments. The domain model applies restrictions to the users' access to different portions of the server and effectively enhances the security of the system.

The Federal Desktop Core Configuration (FDCC) is a mandate requiring all Federal agencies to apply standard security and configuration baseline settings to their desktop computing environments. The FDCC is based on National Institute of Standards and Technology (NIST) recommendations. The MIMIT system implemented and tested the FDCC settings on the server because all the clients were using RDP for applications and file management on the server. Secutor Prime, an automated security evaluation and remediation tool from ThreatGuard, Inc., was used to assess the MIMIT for FDCC compliance. The MIMIT rated 95.6-percent compliance with FDCC requirements.

Security Assessment

The BLM's IT Security Program at NIFC completed a technical vulnerability assessment (TVA) on the MIMIT system. The TVA was completed to identify any critical or high-level security vulnerabilities and to establish an IT security baseline for future reference. The TVA checked for vulnerabilities of the operating system and network configuration, checked FDCC compliance, and checked wireless network traffic for potential disclosure of sensitive information. A report was generated detailing the TVA. Recommendations will be implemented before future deployments.

Help Desk

The BLM Help Desk at NIFC supported the MIMIT project in a variety of ways during 2009. One position was funded for support of the project from April to November 2009. Help Desk personnel were trained on the MIMIT system in May so they could support the CTSPs during deployments. Help desk personnel helped configure, set up, and test the IT equipment in the trailers. Besides loading, labeling, and inventorying the equipment, help desk personnel developed procedures for imaging the servers and clients using Altiris client software.

The help desk also was responsible for refurbishing the trailers and IT equipment when it returned from deployments. Refurbishing includes reimaging the server, mobile thin clients, and laptops; cleaning the equipment; checking printer cartridges; and servicing the generator when needed. The help desk personnel also were responsible for final testing of the complete system (server, wireless LAN controller, wireless access points, mobile thin clients, laptops, and printers).

Hardware Purchase

Funding from the NWCG allowed most of the hardware for the MIMIT system to be purchased during 2008. During 2009, the project purchased all the wireless hardware (wireless LAN controller and wireless access points), more printers (black and white and color), networking cables, and some additional network switches. Several additional laptops were purchased for each trailer.

Great Basin Geographic Area MIMIT Deployment Summaries

Red Rock Fire

Incident Number:	NV-CCD-000660
Incident Location:	Carson City District
Incident Status:	New incident
Team Name:	Whalen GB IMT2
Assignment Length:	7 days
MIMIT Trailer:	No. 1
Number of thin clients:	18
Number of Dell laptops:	1
Number of team laptops:	7
Number of agency laptops:	6
Number of rental laptops:	0

Incident Commander Mike Whalen's Type 2 incident management team set up the Red Rock ICP at the Cold Springs Middle School. The MIMIT trailer was outside a main entrance near the school's utility closet. The trailer became a fully operational mobile office within 22 minutes. The server was running, the wireless LAN controller and wireless access points were operational, the Dell laptop and HP mobile thin clients were running, and the color LaserJet printer was online.

One LAN cable snaked through the school, acting as the trunk for printers and three wireless access points deployed throughout the school. One wireless access point was placed where it could serve the communications unit outside the school. Within 60 minutes of arrival, the MIMIT trailer was providing Internet connectivity (from the contractor, FireDawg). The MIMIT trailer was plugged into the school's power grid.

Major Technical Issues

I-Suite worked fine until an automated backup began looking for an external hard drive that wasn't there. I-Suite crashed and could not be reinstalled on the terminal server.

The Dell laptop in the MIMIT trailer became the I-Suite server and seven team laptops were distributed to team members to continue incident work. The client version of I-Suite was successfully installed on the terminal server using the Dell laptop as the I-Suite server.

Minor Technical Issues

On MIMIT thin clients and laptops, USB devices were not accessible. Team members used agency laptops to copy files from USB jump drives. The wireless network was used to transfer files to where they were needed. The USB problem was caused by FDCC settings that were not fully tested before deployment. After this deployment, the MIMIT system was reconfigured to resolve the USB issue.

The school's power grid did not have enough circuits available to power the MIMIT trailer, which needs at least three distinct circuits. Although circuit breakers tripped irregularly, the MIMIT trailer's uninterruptible power supply allowed the network to continue operating. Another problem was that the MIMIT trailer's air-conditioning unit (needed to keep the server cool) required repeated defrost operations.

Incident Milestones

A higher standard for ICP IT physical security was implemented during this deployment. Security cables were used to lock all network devices (mobile thin clients, access points, and digital projectors). Until this deployment, the best way to implement physical security at an ICP was to

collect network devices at the end of a shift and store them under lock and key until the beginning of the next shift. Security cables provide physical security 24 hours a day, 7 days a week, eliminating the ritual of collecting devices each evening and redistributing them the following morning. Setting up the security cables at a user's workspace takes just a couple of minutes per device.

All team members had Windows Active Directory accounts established on the server. The first time members logged in, they saw a screen explaining how the system worked and were required to change their password.

Incident Summary

The MIMIT trailer arrived at the ICP ahead of schedule. Team CTSPs had attended the MIMIT training during the spring and were familiar with the MIMIT system—it was operating within minutes of its arrival. With the exception of the I-Suite crash and the inability to use USB devices, the MIMIT system performed as expected.

"The MIMIT trailer pilot program played an important role in this incident and was very successful."

—Shawn McEvers
Planning Section Chief

Figure 10—Incident management team personnel using the mobile thin clients at an incident.

Big Pole Fire

Incident Number:	UT-SLD-000544
Incident Location:	Salt Lake Ranger District
Incident Status:	New incident
Team Name:	Ourada GB IMT2
Assignment Length:	6 days
MIMIT Trailer:	No. 1

Number of thin clients:	18
Number of Dell laptops:	1
Number of team laptops:	0
Number of agency laptops:	4+
Number of rental laptops:	0

The MIMIT trailer arrived at Chris Ourada's Type 2 incident management team's inbriefing at the Bureau of Land Management's Salt Lake Field Office. The trailer, deployed in the field office parking lot, was operational at the conclusion of the inbriefing. MIMIT personnel worked with the team CTSP and planning section chief to prepare the initial incident action plan using I-Suite's automated incident action plan module.

The following day, the Big Pole ICP was set up in the parking lot of the Grantsville, UT, high school. Because office trailers were not operational until the following day, the MIMIT trailer was used by all functional areas during the first operational period at the ICP.

Once additional office trailers arrived, the MIMIT trailer's three wireless access points were deployed throughout the parking lot. External Internet connectivity was supplied during the first hour after the trailer's arrival by contract vendor Lyman Brothers Satellite. The MIMIT trailer was plugged into the Lyman Brothers power grid.

Major Technical Issues

None.

Minor Technical Issues

One of the four black-and-white printers became unserviceable.

A member of the incident management team suggested adding a fax machine to the MIMIT trailer's inventory.

The MIMIT trailer's air-conditioning unit became unserviceable.

Incident Milestones

The team CTSP was filling in behind the team's retired CTSP. The Big Pole incident was an introduction to fire assignments for the team's new CTSP. The MIMIT technology worked well—a measure of the system's well-thought-out network configuration, as well as the new CTSP's skills.

The ability to try something new—the automated I-Suite incident action plan module—during the first hours of incident operation illustrates the flexibility of the MIMIT technology.

Cables were used to secure all thin clients, wireless access points, and digital projectors.

Incident Summary

MIMIT mobilization was executed as planned. The MIMIT trailer arrived at the ICP ahead of schedule.

"The Mobile Incident Management Information Technology Project (MIMIT)/Thin Client out of NIFC went very well and provided the necessary computer and Internet service for the camp."

—Val Norman
Logistics Section Chief

Hoyt Fire

Incident Number:	NV-CCD-000987
Incident Location:	Carson City District
Incident Status:	New incident
Team Name:	Suwyn GB IMT2
Assignment Length:	3 days
MIMIT Trailer:	No. 2

Number of thin clients:	25
Number of Dell laptops:	1
Number of team laptops:	0
Number of agency laptops:	2
Number of rental laptops:	0

The ICP was set up at the U.S. Navy Centroid Facility between Fallon and Austin, NV. Because of confusion during the mobilization process, the MIMIT trailer was not ordered when Tom Sawyn's Type 2 incident management team was ordered. The trailer arrived at the ICP a few hours behind the team.

The following day, power grid issues hampered setup of the Hoyt ICP. The MIMIT trailer, powered by its own generator, was used by all functional areas until the team's generator was brought online. The MIMIT wireless network permitted a quick and flexible network deployment throughout the ICP. External Internet connectivity was supplied by contract vendor Lyman Brothers Satellite.

Major Technical Issues

None.

Minor Technical Issues

The virtual private network/firewall had to be rebooted occasionally to maintain external connectivity.

A member of the incident management team suggested adding a fax machine to the MIMIT trailer's inventory. Another team member suggested adding a fax/scanner/copier/printer to the trailer's inventory.

Incident Milestones

The team CTSP, who had attended the MIMIT training in May, set up the system without any issues.

Incident Summary

Because Tom Suwyn's incident management team is well equipped with trailers, computers, and a generator, the team considered handling the incident without the services of the MIMIT system. In spite of the team's apprehension, the MIMIT system was well received. On a short incident (3 days) such as this one, it is critical that any IT solution be rapidly deployed and self-contained.

"We were able to utilize the new Mobile Incident Management Information Technology (MIMIT) trailer. This trailer is built to support incident management and hopefully address the increasingly complex issues involved with database management and PII (personally identifiable information) data and computer support required to meet increasing security standards.

"During the Hoyt fire, we were able to set up and be running in a short time frame. This was great for us! We were able to utilize the trailer for many different functions, including information, check-in, and training until an electric supply issue was completed. Along with the option for added space, the functionality of wireless communication and Internet access made for quick setup between office trailers and reduced clutter from runs of wiring. The printers were mapped, users were created, and the server seemed to work consistently. We appreciated the opportunity to use this trailer and feel that having access to the MIMIT trailers in the future will be a good addition to the incident management arena."

—Heidi Little
Computer Technical Specialist

Mill Flat Fire

Incident Number:	UT-DIF-090383
Incident Location:	Dixie National Forest
Incident Status:	New incident
Team Name:	Muir GB IMT1
Assignment Length:	9 days
MIMIT Trailer:	No. 3

Number of thin clients:	20
Number of Dell laptops:	7
Number of team laptops:	0
Number of agency laptops:	4+
Number of rental laptops:	0

The Mill Flat Fire ICP was set up in a pasture outside New Harmony, UT. The MIMIT trailer was in place and available after the inbriefing for Rowdy Muir's Type 1 incident management team. External Internet connectivity (supplied by contract vendor Lightning Ridge) was available within the first operational period. The wireless infrastructure provided by the MIMIT trailer allowed a quick and flexible network deployment throughout the ICP.

Additional office space and power was not available until late in the second operational period when an industrial-sized powerplant arrived. The MIMIT generator and Lightning Ridge generators powered the entire ICP throughout the second operational period as the powerplant was assembled.

Major Technical Issues

The powerplant lacked sufficient voltage regulation and allowed power surges during the third and fourth operational periods, resulting in permanent damage to surge protectors. Total damages exceeded several thousand dollars. Although damages were limited to surge protectors, the impact to ICP productivity was significant. Obtaining clean power is an ever-present issue at fire camps. A voltage meter is part of the MIMIT trailer equipment used to check endpoints of the power grid. Usually the voltage is lower than needed, resulting in tripped circuits.

Minor Technical Issues

The of VPN/firewall had to be rebooted several times to maintain external connectivity.

Incident Milestones

MIMIT office space, including the wide-screen monitor, was used exclusively for daily planning meetings and to teach a section of S-420 Command and General Staff training.

The team's CTSP, who attended the MIMIT training in May, set up the system without any problems.

Incident Summary

The Mill Flat Fire, the longest deployment of the MIMIT system during 2009, validated the system's network design and configuration. Again, the office space was fully used along with the self-contained MIMIT generator.

"…had the trailer up and running by the time we got out of our in-brief (2300). We still got a plan out for the next operational period in a short time."

—Rowdy Muir
Incident Commander

Figure 11—The MIMIT trailer was one of the first units to arrive and be used at the Mill Flat fire.

Gunsight Fire

Incident Number:	WY-BTF-000037
Incident Location:	Bridger-Teton National Forest
Incident Status:	New incident
Team Name:	Svalberg GB IMT2
Assignment Length:	5 days
MIMIT Trailer:	No. 4
Number of thin clients:	12
Number of Dell laptops:	1
Number of team laptops	0
Number of agency laptops:	2+
Number of rental laptops:	0

The incident command post was set up in the local host facilities. The MIMIT trailer's wireless infrastructure allowed a quick and flexible network deployment. A DSL service provider supplied Internet connectivity.

Major Technical Issues

Problems with external connectivity through the VPN/firewall hardware surfaced, prolonging setup of the LAN.

Minor Technical Issues

The mount for the wide-screen monitor failed, but the monitor was not seriously damaged.

A wireless keyboard and mouse were requested for the wide-screen monitor, as well as a laser pointer.

Missing handrails to the trailer entry were noted as a safety concern.

Incident Summary

The MIMIT trailer deployment to the Gunsight Fire was the only assignment not shepherded by the MIMIT business lead. Nevertheless, team CTSPs were quickly able to set up the LAN. Both CTSPs had been through the MIMIT training months earlier.

"It worked just like it was supposed to."

—Erik Torres
Computer Technical Specialist

Informal User Responses

Incident management team members were asked to fill out a user response form that recorded their feedback on the MIMIT system. The form was available online and users were asked to fill it out at any time during the incident. We received feedback during four of the five deployments.

What Did We Study?

The online response form asked users to evaluate three aspects of their experience using the MIMIT:

- Identify the components of the system you actually used.
- Rate the relative merits of the MIMIT system compared to computer systems you used in the past.
- Rate the system's overall functionality.

Twenty-two responses were collected from users at the Red Rock, Big Pole, Hoyt, and Mill Flat Fires (figure 12).

The respondents represent a convenience sample of IMT members at incidents where the MIMIT was deployed. No attempt was made to obtain a systematic random sample. This fact, combined with the small sample size, indicates that the results presented here should not be taken as representative. Rather, the responses portray the opinions of the respondents who chose to fill out the online evaluation form.

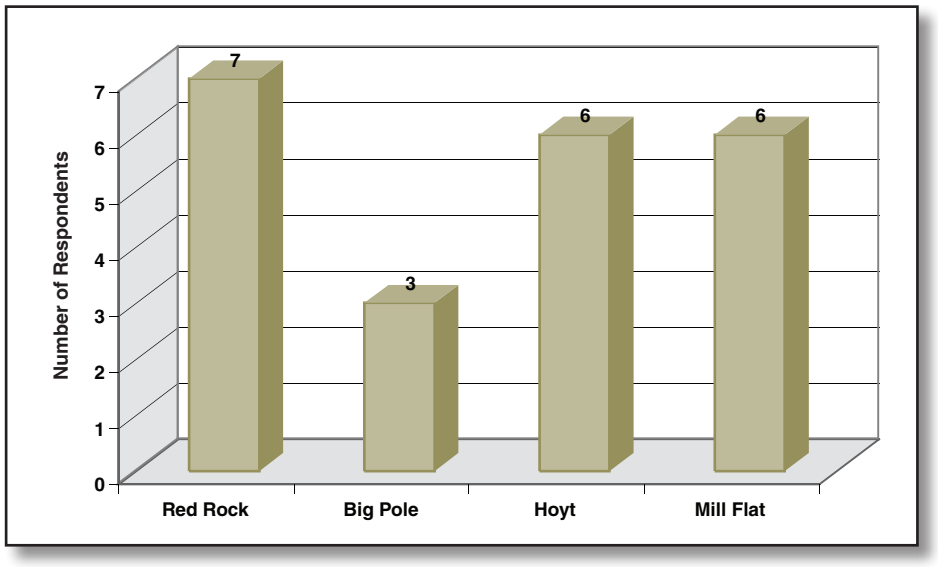

Figure 12—The number of respondents at each of the four Great Basin incidents where responses were solicited.

What Components of the System Did Respondents Use?

Wireless capabilities of the mobile thin clients, the Dell laptops, and the black-and-white printers were the most common components used by the respondents (figure 13).

Respondents were also given the opportunity to comment about aspects of the system they didn't like. The two most common responses identified additional features users wanted: access to thumb drives and access to internal Government Web sites and resources. The following quotes express these concerns.

Access to Thumb Drives

"We need access to a thumb drive. We all carry our complete finance kits on these with all the forms needed at a incident (W-4, W-5, Incident Behavior, Casual Hire, CA-1, CA-2, CA-16, FS-6100) [and the] Incident Business Management handbook— and if we can't have access to use them, we can't perform our duties as efficient as needed."*

**Note: the USB drive issue was remedied after the first deployment.*

Access to Government Web Sites

"Because we are not allowed to access internal Government (Forest Service/BLM) Web sites through fire laptops, it limits access to email information that team members have received during the year. I attempted to access information about payment packages to ASC, but was not able to access the internal web for either FS or BLM. It would be very helpful to have access to our Government email accounts and internal Web sites in order to have better business tools and instructions that are in place from these sites. Could not use Government computer to VPN to needed information contained in emails and internal Government Web sites."

"I would like to see some of the Incident Business Management forms; links and other helpful...I didn't have a reliable connection to the Forest Service sites long enough to copy the forms and instructions that I needed from the ASC incident site to complete my task and spent quite a bit more time on the phone or finding others who might have that information on a flash drive, etc."

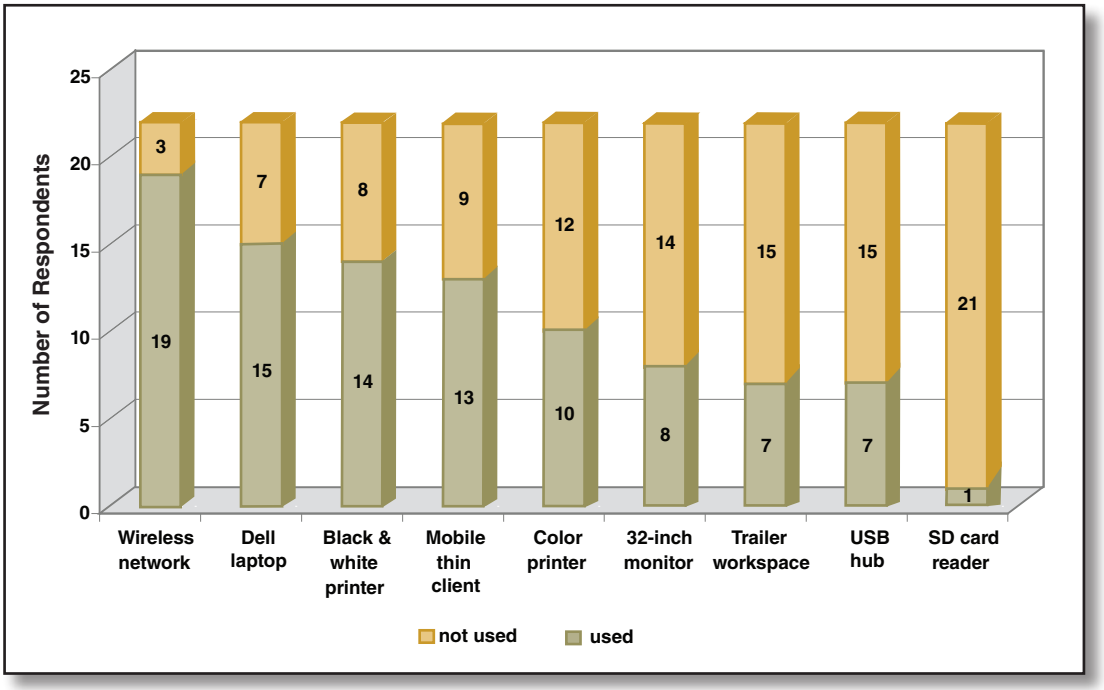

Figure 13—The number of respondents that used specific components of the MIMIT system.

Relative Merits of the MIMIT System

Most respondents rated the MIMIT system favorably, saying that the MIMIT system was up and running faster than computer systems on previous incidents (figure 14). Also, most respondents indicated that they would prefer to use a system like MIMIT in future assignments (figure 15).

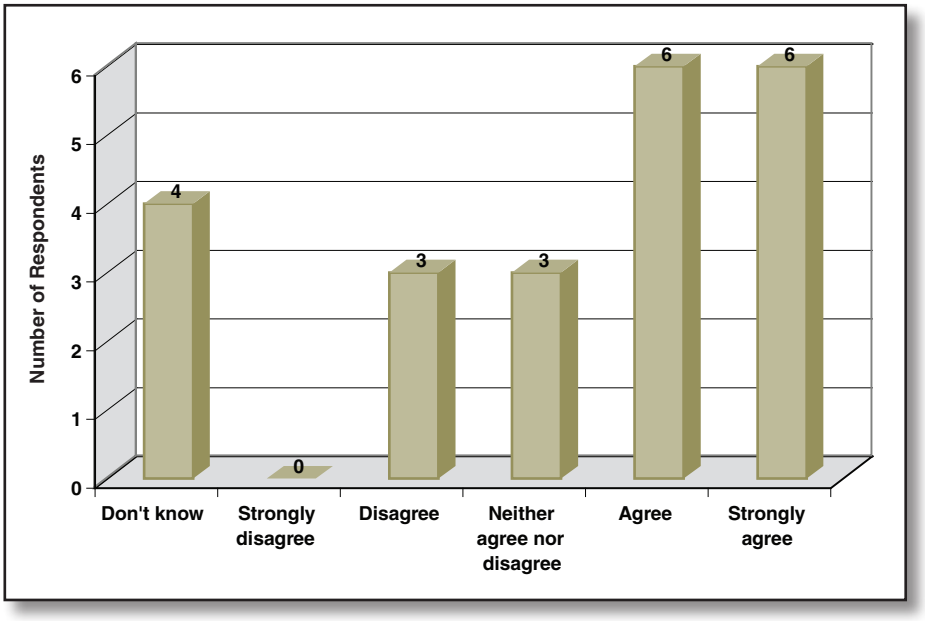

Figure 14—The number of respondents agreeing or disagreeing with the statement: "Compared to previous assignments, the system on this fire was up and running faster."

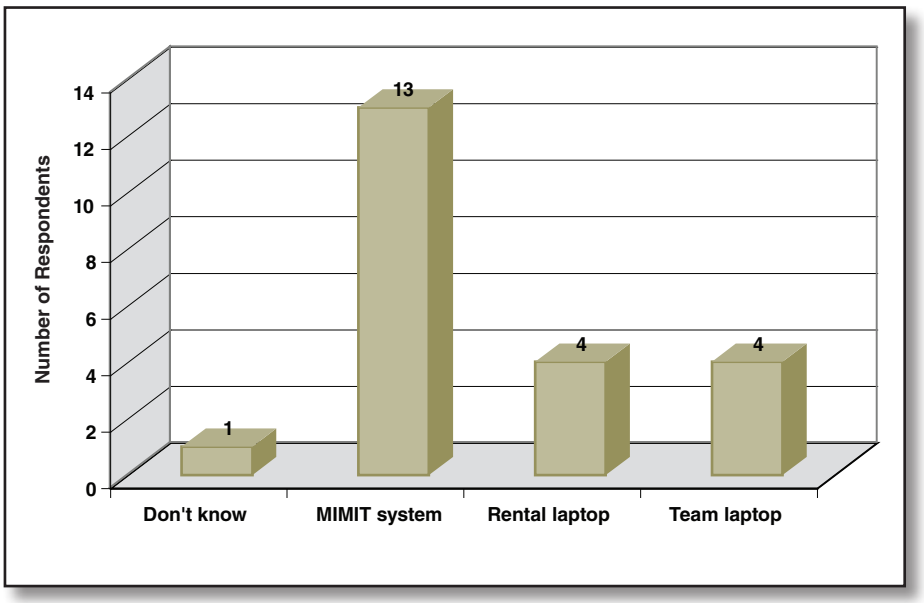

Figure 15—The number of respondents indicating their preference for computer systems while on incidents.

This overall positive evaluation is supported by user comments. When users were asked about their experience using the MIMIT system, the most frequent responses were positive general statements:

"I used the thin client 2008 version on a Type 1 fire in California last year and it was a disaster. Unreliable, no good connectivity, and unless you were a trained IT person, it was worthless. This MIMIT version is 180 degrees different. I hope this becomes SOP for incidents. In today's information environment, as PIO, I need instant access to the world and using MIMIT allowed me to concentrate on content and not be concerned with the technology. My hat is off to the project!"

"Computer layout with software is appropriate for the tasks at hand. Nice screens and computers. Bottom line is: how effective is the system to accomplish the tasks and [the system's] practicality? This system is very efficient and productive.

"The system for all intents and purposes filled the need and function at a critical time and performed well. Adequate speed and memory was available for all to use. Being linked to all [other team members] without using so many flash drives and/or trying to find a computer to use was nice."

Evaluation of System Functionality

More respondents agreed that the system made them more productive than those who disagreed (figure 16).

In general, respondents rated the following system elements favorably:

- Using incident printers
- Sufficiency of data storage
- Ease of use
- Information sharing capabilities

Respondents gave a mixed evaluation of the availability of the applications that they needed for their incident management duties. The responses were split between those that agreed and disagreed with the statement: "The system had all the applications I needed" (figure 17).

Users liked three main aspects of the MIMIT system: the speed of setup, enhanced file sharing ability, and the availability and quality of support. The following quotes are representative of these views:

Speed of Setup

"It came preconfigured, didn't need to wait several hours for good access and a work space."

"Very efficient and the system was up and running very fast."

File Sharing

"It allowed us to share the network just like at an office except that it was mobile."

Support

"A very knowledgeable computer specialist managed the system and had a working knowledge of the system. Computer specialists checked with each unit frequently to see if there were any concerns with the system."

"There was always someone to come help if you got locked out, or something wasn't working correctly. The staff was knowledgeable about the software, the hardware, and were open to suggestions."

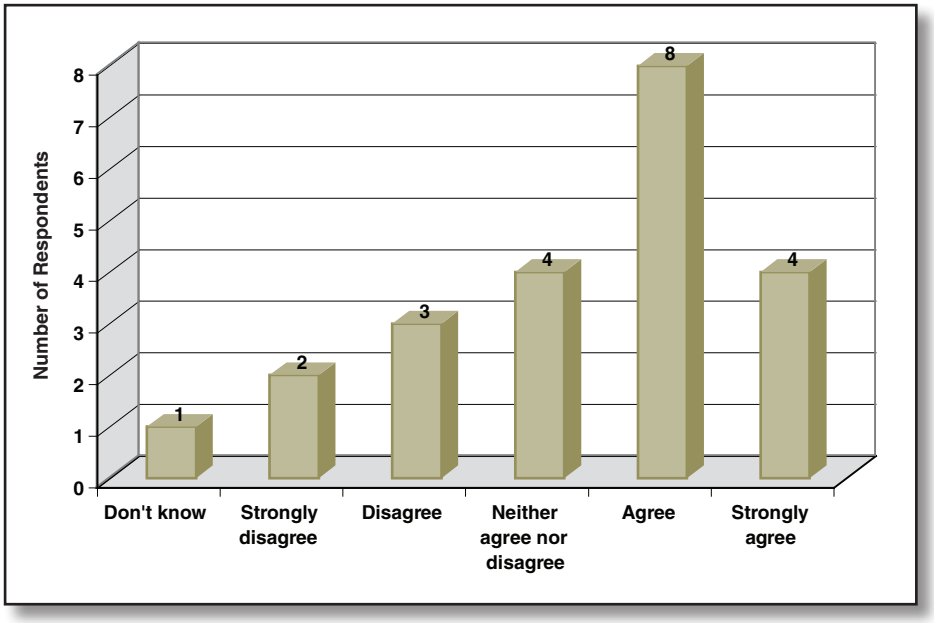

Figure 16—The number of respondents agreeing or disagreeing with the statement: "Overall, the system allowed me to be more productive."

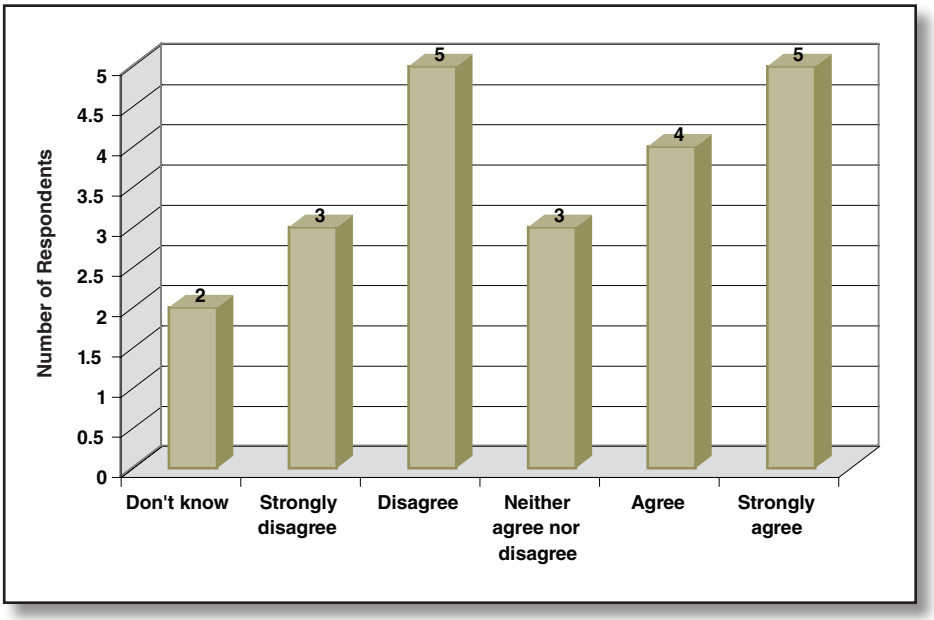

Figure 17—The number of respondents agreeing or disagreeing with the statement: "The system had all the applications I needed."

Cost-Benefit Analysis

A cost-benefit analysis (CBA) was developed for the MIMIT system to determine whether funding a national MIMIT program would provide a favorable return on investment and reasonable payback period. Other outcomes of the CBA included the probability that program benefits will exceed costs, total cost of ownership, net present value (NPV) of program benefits minus program costs, benefit-cost ratio, and fiscal year 2010 funding requirements. A summary of the CBA follows. The complete CBA can be requested from Andy Trent at MTDC.

Background of the Cost-Benefit Analysis

The MIMIT CBA followed Office of Management and Budget A-94 circular guidance that requires evaluation of three options. The options evaluated were:

Option 1: No additional MIMIT trailers added to the existing inventory of five—This option essentially funds the pilot program at current levels.

Option 2: 10 additional completely outfitted MIMIT trailers—Adding 10 trailers to the inventory was evaluated to show the ROI and NPV halfway between option 1 and option 3.

Option 3: 20 additional completely outfitted MIMIT trailers—The addition of 20 trailers is intended to achieve economies of scale, while supporting about 80 percent of Type 1 and Type 2 incidents from May through November for a peak fire season (based on data from 2004 to 2008). During a slow fire season such as 2009, this option would support 100 percent of all Type 1 and Type 2 incidents.

For each option, the cost for a Government-operated, National Interagency Support Cache program was compared to contracting the equipment used in the MIMIT system. The Government-operated program included the complete costs of the MIMIT system (server, mobile thin clients, wireless hardware, software, trailers, expendables), facilities, full-time employees, travel, and training for CTSPs. The analysis projected these costs to future years by quantifying equipment failure rates, expected inflation rates, wage increases, and other variables. The contractor costs for similar equipment delivered by the MIMIT system were estimated for a comparison. These costs were determined by reviewing historical contract expenditures using P-codes (management codes for fires) and reviewing established contracts for similar delivered services.

Another significant factor in establishing program benefits is the average number of times a year each MIMIT trailer will be used. Maximizing the deployments throughout the year has a significant impact on overall program benefits. Using the MIMIT system for other purposes (Type 3 incidents, training, natural disasters) increases the ROI significantly.

Intangible benefits of the MIMIT system include increased security for data and personally identifiable information, wireless security, rapid and reliable delivery of the MIMIT system to incidents, secure office space inside the trailer, and standardization of equipment, documentation, and training. These intangible benefits added an additional 15 percent to the overall benefits.

Results of the Cost-Benefit Analysis

The MIMIT CBA used a 10-year expected program life using Monte Carlo Analysis. Figure 18 shows the NPV of the total program costs (NPV of costs minus NPV of benefits) for the three options when supporting Type 1 and Type 2 incidents. Also shown are the ROI, NPV total cost of ownership, benefit-cost ratio, 2010 funding requirements, and the probability the program benefits will exceed costs.

Based on the CBA, the most logical choice is option 3. Option 3 (the addition of 20 completely outfitted MIMIT trailers) delivers the greatest ROI (43 percent) and has the shortest break-even point (5 years). The probability that program benefits exceed program costs is 76 percent. However, if the MIMIT trailers could be deployed two more times each per year (by supporting Type 3 incidents, training, or natural disasters), the ROI increases to 112 percent and the probability that benefits exceed costs rises to 88 percent (figure 19). Required funding for full program implementation is $2.6 million (2010 dollars) with a break-even point in about 5 years.

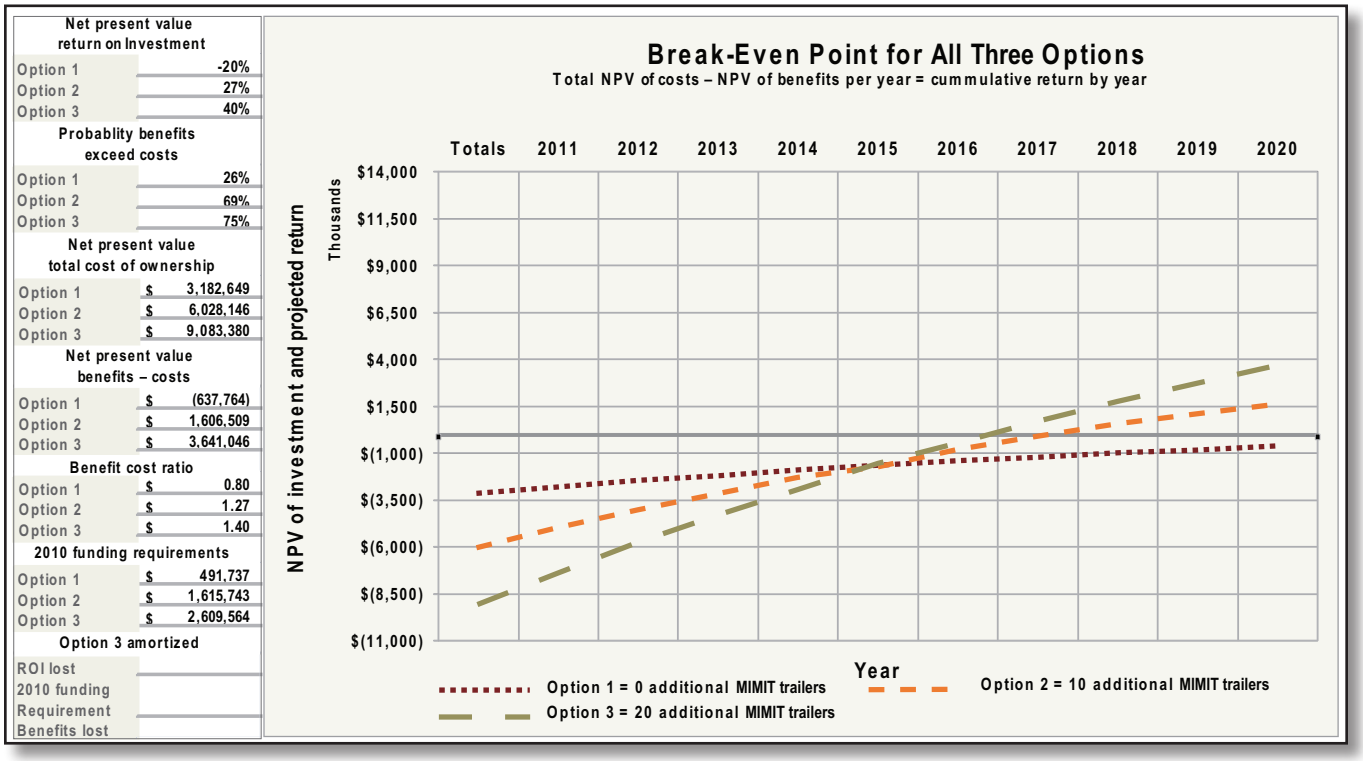

Figure 18—This chart shows the break-even point for the three MIMIT program options. Results are based on the MIMIT system being used just to support Type 1 and Type 2 incidents.

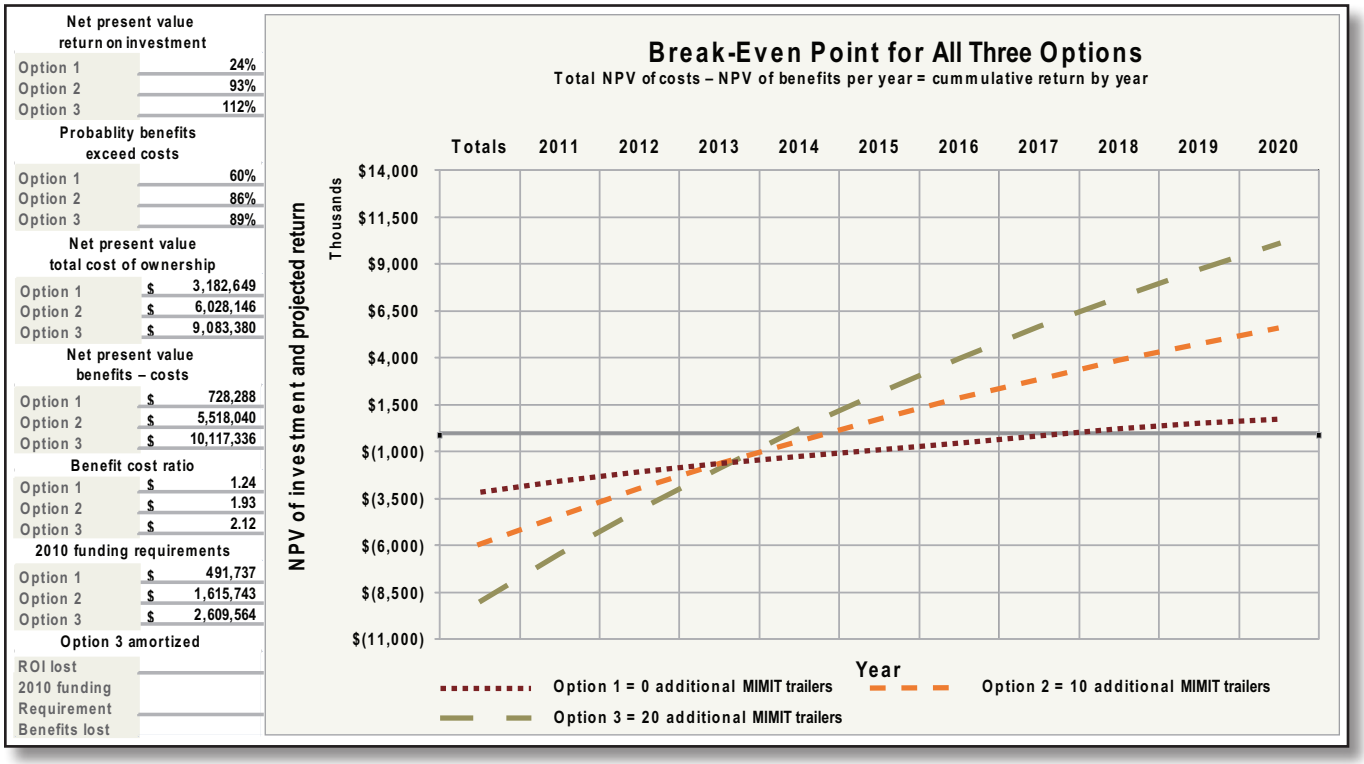

Figure 19—This chart shows the break-even point for the three MIMIT program options. Results are based on the MIMIT system supporting not only Type 1 and Type 2 incidents but also additional types of deployments (Type 3 incidents, training, natural disasters).

Acknowledgments

The authors would like to acknowledge the following:

Forest Service employees—Tyler Hackney, Steve Simon, Gina Bald, Art Clinton, Kevin Snyder, Gary Kees, Doug Lausch, Chuck Harding, Scott Gilmour, Bert Lindler, Sunni Bradshaw, Jerry Wolf, Shanon Boehlke, Kolleen Shelley, Vic Helbling, Matt Cnudde, and Jody Lane

Bureau of Land Management employees—Brian Lamb, Nichole Owen, Don Lee, John Noneman, Jason Nguyen, Mike Allison, Cory McCarthy, Rhonda Toronto, Louis Leezer, Dan Boss, Paul Lehman, and Greg Jensen

National Park Service employees—Gladys Crabtree, Erik Torres, Don Winter, and Peter Paul

Bureau of Indian Affairs employee—David Potter

About the Authors

Andy Trent is a project engineer at MTDC. He received his bachelor's degree in mechanical engineering from Montana State University in 1989. Before coming to MTDC in 1996, Andy worked as a civilian engineer for the Department of the Navy.

Michael Morgen works for the Bureau of Land Management (BLM) at the National Interagency Fire Center in Boise, ID, and is the business lead for the MIMIT project. He has served as a computer technical specialist for several incident management teams and has set up more than 50 incident networks during the last 10 seasons. Morgen was a smokejumper for 19 fire seasons for the BLM and the Forest Service.

Theron Miller is a social science analyst at MTDC. He received his Ph.D. in forestry from the University of Montana in 1997 with an emphasis in natural resources social science. After graduating, he was a research and teaching professor at the University of Montana where his area of focus was applied social sciences directly related to management of natural resources on public lands. Miller joined MTDC in 2006 and assists with projects in the safety and health, recreation, information technology, and fire and aviation management programs.

Doug Stefan is a quality management analyst for the Forest Service CIO. He has bachelor degrees in business finance management and information technology business management. Before coming to the Forest Service in 2004, he supervised a high-end engineering lab for 7 years in private industry. Stefan served in the Marine Corps for 6 years and is an assistant liaison for modular airborne firefighting systems.

Library Card

Trent, Andy; Morgan, Michael; Miller, Theron; Stefan, Doug. 2009. MIMIT pilot project. Tech. Rep. 0966–2839–MTDC. Missoula, MT: U.S. Department of Agriculture, Forest Service, Missoula Technology and Development Center. 24 p.

A mobile information technology system for use at incidents was tested at the incident command posts for five forest fires during 2009 in the Great Basin. The Mobile Incident Management Information Technology (MIMIT) system includes a terminal server, wireless local area network controller, wireless access points, laptops, printers, and associated networking equipment. All of the equipment is stored in a trailer that can be ready for use within minutes of its arrival at an incident. Some of the advantages of the system include a stable and secure information technology environment where all of the incident's data are stored on a server, not on users' computers. The MIMIT system is intended to be used for the duration of an incident. Now, when one incident management team is replaced by another, the information technology infrastructure has to be torn down so the new team can set up its own infrastructure from scratch. Users who responded to informal online evaluation forms generally liked the new system. Five MIMIT trailers were outfitted for the pilot project. A cost-benefit analysis evaluated three options: no additional MIMIT trailers, adding 10 completely outfitted MIMIT trailers, or adding 20 completely outfitted MIMIT trailers. Option 3 (having 20 additional MIMIT trailers available nationally) was determined to provide the best return on investment, even when compared to contractor costs for similar equipment and services.

Keywords: access points, cost-benefit analysis, deployments, Great Basin, incident management, information technology, interagency, IT, local area networks, security, terminal servers, thin clients, wireless LANs

Additional single copies of this document may be ordered from:

USDA Forest Service, Missoula Technology and Development Center
5785 Hwy. 10 West
Missoula, MT 59808–9361
Phone: 406–329–3978
Fax: 406–329–3719
Email: wo_mtdc_pubs@fs.fed.us

Electronic copies of MTDC's documents are available on the Internet at:

http://www.fs.fed.us/eng/t-d.php

For additional information about MIMIT Pilot Project, contact Andy Trent at MTDC:

Phone: 406–329–3912
Fax: 406–329–3719
Email: atrent@fs.fed.us

Forest Service and Bureau of Land Management employees can search a more complete collection of MTDC's documents, CDs, DVDs, and videos on their internal computer networks at:

http://fsweb.mtdc.wo.fs.fed.us/search/