AFRL-IF-RS-TR-2001-228
Final Technical Report
October 2001


# NATIONAL INSTITUTE OF JUSTICE (NIJ) CENTER REQUIREMENTS DEFINITION, PROGRAM DEVELOPMENT AND TECHNICAL ASSISTANCE

**Emergent Information Technologies, Inc.**

**Robert L. DeCarlo, Jr.**

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.*

**AIR FORCE RESEARCH LABORATORY**
**INFORMATION DIRECTORATE**
**ROME RESEARCH SITE**
**ROME, NEW YORK**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2001-228 has been reviewed and is approved for publication.

APPROVED:

ERIC C. JONES
Project Engineer

FOR THE DIRECTOR:

JOSEPH CAMERA, Chief
Information & Intelligence Exploitation Division
Information Directorate

If your address has changed or if you wish to be removed from the Air Force Research Laboratory Rome Research Site mailing list, or if the addressee is no longer employed by your organization, please notify AFRL/IFEA, 32 Brooks Rd, Rome, NY 13441-4114. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

| REPORT DOCUMENTATION PAGE | Form Approved OMB No. 0704-0188 |
|---|---|



| 1. AGENCY USE ONLY *(Leave blank)* | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | OCTOBER 2001 | Final May 2000 - May 2001 |

**4. TITLE AND SUBTITLE**
NATIONAL INSTITUTE OF JUSTICE (NIJ) CENTER REQUIREMENTS DEFINITION, PROGRAM DEVELOPMENT AND TECHNICAL ASSISTANCE

**5. FUNDING NUMBERS**
C - F30602-97-C-0070, Task 15
PE - N/A
PR - NIJR
TA - QF
WU - 04

**6. AUTHOR(S)**
Robert L. DeCarlo Jr.

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Emergent Information Technologies, Inc. (East)
1300-B Floyd Ave.
Rome, NY 13440-4615

**8. PERFORMING ORGANIZATION REPORT NUMBER**
Emergent Report # 1NY-1808

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Air Force Research Laboratory/IFEA
32 Brooks Road
Rome, NY 13441-4114

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
AFRL-IF-RS-TR-2001-228

**11. SUPPLEMENTARY NOTES**
Air Force Research Laboratory Project Engineer: Eric C. Jones/IFEA/(315) 330-4410

**12a. DISTRIBUTION AVAILABILITY STATEMENT**
Approved For Public Release; Distribution Unlimited.

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** *(Maximum 200 words)*

The mission of the National Law Enforcement and Corrections Technology Center - Northeast Region (NLECTC-NE), in conjunction with the Air Force Research Laboratory/Information Directorate (AFRL/IF), is to facilitate the identification, development, and adoption of new products and technologies specifically designed for law enforcement, corrections, and other criminal justice applications. The current technology thrust areas for the Northeast Region are Concealed Weapons Detection (CWD), Secure Communication, Computer Forensics, Passive Location Tracking and Tagging, Information Management, Advanced Generation Interoperability for Law Enforcement (AGILE), and various technical assistance projects. This report outlines the major accomplishments of the NLECTC-NE under the Emergent Information Technologies, Inc. (East) Task Ordering Contract (TOC), and identifies on-going technology efforts. These accomplishments include outreach activities, scientific and engineering assistance, and special projects including AGILE, computer crime initiatives, and an operational evaluation of a CWD device for school safety applications.

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| NLECTC-NE, CWD, Computer Forensics, Secure Communications, Information Management, Communications Interoperability | 32 |
| | 16. PRICE CODE |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | UL |

# TABLE OF CONTENTS

## TABLE OF FIGURES

**SECTION** **PAGE**

## 1. BACKGROUND

The mission of the National Law Enforcement and Corrections Technology Center–Northeast Region (NLECTC-NE), in conjunction with the Air Force Research Laboratory/Information Directorate (AFRL/IF), is to facilitate the identification, development, and adoption of new products and technologies specifically designed for law enforcement, corrections, and other criminal justice applications. The current technology thrust areas for the Northeast Region are Concealed Weapons Detection, Secure Communications, Timeline Analysis, Computer Forensics, Audio/Video Processing, Information Management, Automatic Speaker Recognition, Automatic Language Translation and Facial Recognition. This report outlines the major accomplishments of the NLECTC-NE under the Emergent Information Technologies, Inc., Task Ordering Contract (TOC).

### 1.1 NLECTC-NE CENTER

The NLECTC-NE Center is located in Central New York at the Air Force Research Laboratory/Information Directorate (AFRL/IF) in Rome, NY. Emergent Information Technologies, Inc. (Emergent) and New York State Technology Enterprise Corporation (NYSTEC) support the management of the Center under contract. The Team consists of both Emergent and NYSTEC personnel and will henceforth be referred to as the Emergent Team or the Team.

## 2. OUTREACH ACTIVITIES

Part of the mission of the Center is to publicize the activities and the services of the NLECTC system to the state and local law enforcement and corrections community. This is accomplished by presentations at key conferences and meetings, by conducting demonstrations of technologies at Tech Fairs and by working with an advisory council.

### 2.1 PRESENTATIONS, CONFERENCES, MEETINGS AND DEMONSTRATIONS

The Team conducted a number of outreach activities including presentations, and attendance at regional and national law enforcement and corrections conferences and seminars across the Northeast. The following is a list of the conferences and meetings supported:

| DATE | CONFERENCE | LOCATION |
|---|---|---|
| May 2000 | Center for Technology Commercialization (CTC) Public Safety Technology Workshop | Westborough, MA |
| May 2000 | NDAA (National District Attorneys Association) Metropolitan Prosecutors Meeting | Alexandria, VA |
| May 2000 | NIJ/OST Congressional Tech Fair | Washington, DC |
| June 2000 | NIJ's Technologies for Public Safety in Critical Incident Response Conference 2000 | Denver, CO |
| July 2000 | Weed and Seed Annual Conference | New Orleans, LA |
| July 2000 | NLECTC-NE 1033 State Coordinators Conference | Harrisburg, PA |

| DATE | CONFERENCE | LOCATION |
|---|---|---|
| August 2000 | New York Prosecutors Training Institute for NYS Prosecutors | Syracuse, NY |
| August 2000 | New York Police Department Conference on New Frontiers in Policing | New York City, NY |
| September 2000 | MN Annual Sheriff's and Jail Administration Conference | Brainer, MN |
| October 2000 | San Diego Regional Computer Forensic Laboratory (SDRCFL) Conference | San Diego, CA |
| October 2000 | Rural Law Enforcement Tech Fair | Somerset, KY |
| November 2000 | IACP Convention | San Diego, CA |
| January 2001 | CyberCrime 2001 Conference and Exhibition | Foxwoods Resorts and Casino, Connecticut |
| February 2001 | International Conference on Electronic Crime (ICE) | New York, NY |
| March 2001 | OST School Safety Grant Review Meeting | Alexandria, VA |
| March 2001 | Massachusetts Chiefs of Police Association Annual Vendor Exhibit | Boxborough, MA |
| April 2001 | Tour for MVCC Faculty Members of AFRL/IF Information Assurance Lab, LEAF, and Northeast Cyberscience Lab. | Rome, NY |

## 2.2 NLECTC-NE ADVISORY COUNCIL

The NLECTC-NE Advisory Council is composed of law enforcement and corrections practitioners from each of the sixteen states in the Northeast region. Their mission is to provide prioritization of requirements, address state and local issues, and to support interfaces with the law enforcement and corrections community within each state. The Council meets semi-annually within the various states in the Northeast region and the Emergent team fully supports each meeting, including the planning and coordinating of sites, agendas, travel arrangements and guest speakers.

NLECTC-NE Advisory Council Meetings were held in Rome, NY on September 29-30, 2000 and in Framingham, MA on May 10-11, 2001.

## 3. SCIENTIFIC AND ENGINEERING ASSISTANCE

### 3.1 SCHOOL SECURITY

Team personnel worked with Sandia National Labs on a School Safety Assessment at the Madison Park Technical-Vocational High School in Boston, MA. Congress had allocated $100,000 for a school safety grant to implement new security measures, which covered the cost of the hardware. After the initial assessment, NLECTC-NE personnel met with representatives from security camera and metal detector manufacturers and assessed their capabilities and also determined the appropriate location for these security measures inside the school. After Sandia chose the vendors, work began on the upgrades.

To date, the following new security measures have been installed at Madison Park:

- 3 *CEIA* Metal Detectors;
- 64 Surveillance Cameras;
- Digital Video Storage System;
- New ID Badge System; and
- New Visitor Passes.

A senior Madison-Park official stated that, "With the implementation of this safety system a number of incidents are not taking place and we have been able to apprehend students who have caused problems. In one particular case it led to the expulsion of a student. Due to the installation and implementation of this entire system, students and staff appear to feel safer and participate a lot more in the monitoring of the school."

NLECTC-NE will continue to monitor the installation of the upgrades and report progress, lessons learned that can be applied elsewhere, and any other meaningful developments.

### 3.2 1033 PROGRAM SUPPORT

Assistance with the 1033 Federal Surplus Property Program was given to 78 specific Law Enforcement, Corrections, and Public Safety agencies from the Northeast region. A total of $2,444,161 in excess equipment was transferred to Law Enforcement. These included 2 ½ ton trucks, M106-A2 Armored Personnel Carriers (APC's), security cages, Chevy Blazers, two 60-kilowatt generators, computers, oxygen tanks, and night vision goggles. Some of the equipment is shown in Figure 3-1 and Figure 3-2 below.

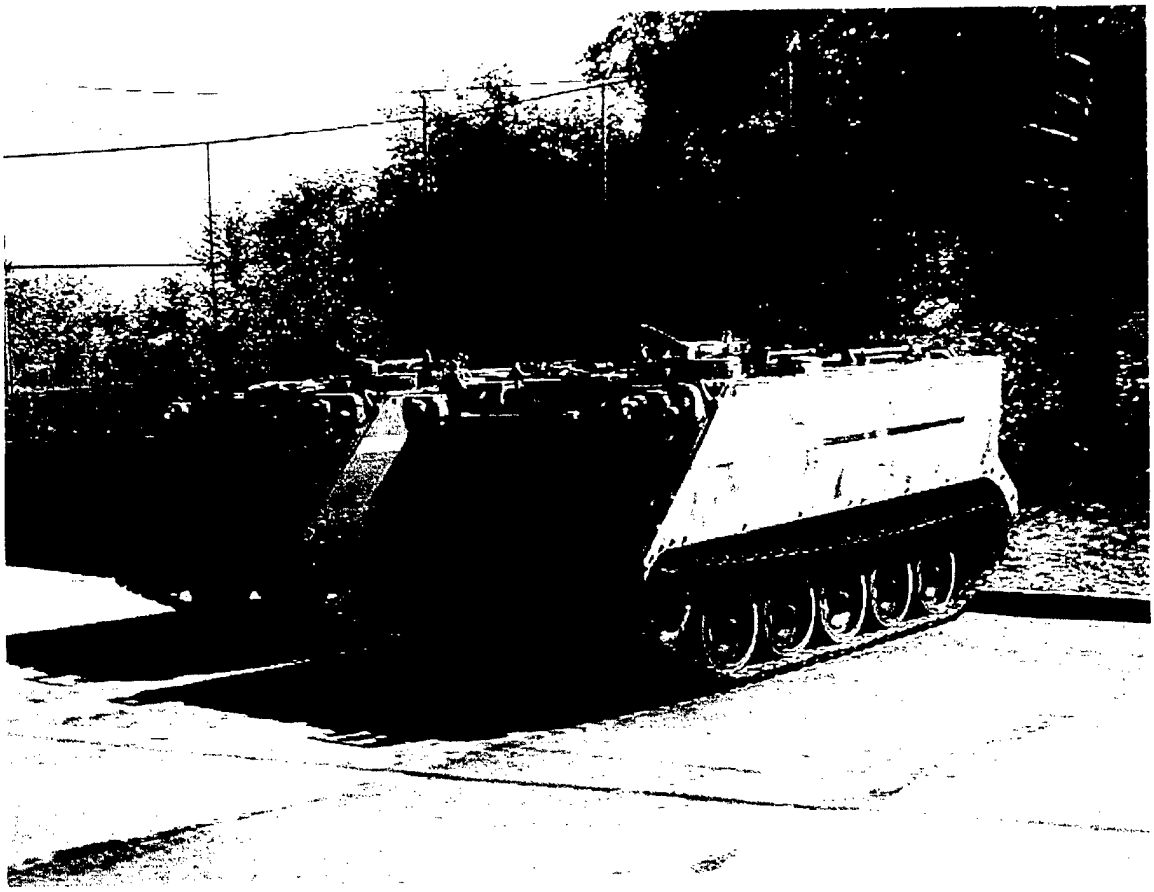

**Figure 3-1: Armored Personnel Carriers *Before* Acquisition Through 1033 Program by Massachusetts Department of Corrections Special Operations Unit**


**Figure 3-2: Armored Personnel Carrier *After* Acquisition Through 1033 Program by Massachusetts Department of Corrections Special Operations Unit**

## 3.3 SUPPORT TO THE UTICA ARSON STRIKE FORCE AND ONEIDA COUNTY DRUG ENFORCEMENT TASK FORCE

Team personnel provided technical support to the Utica Arson Strike Force (UASF) and Oneida County Drug Enforcement Task Force (OCDETF) to maintain and upgrade capabilities provided under previous NIJ contracts. Specific activities included:

- Setting up and maintaining the network servers, establishing user security levels and backup schedules, and adding and removing network nodes.
- Installing, reinstalling and adding operating systems, application software, and device drivers on network workstations and notebook computers.
- Creating databases for case tracking and information gathering.
- Installing and configuring new Notebook/Desktop Computers, upgrading and repairing existing ones.
- Reconfiguring the networks to include the addition of a new mug shot retrieve station and interfacing it with a countywide mug shot database.

- Adding and rerouting network cabling for more users, setting up new security for the server due to the addition of new officers attached to the Utica Arson Strike Force as part of the new Oneida County Major Crimes Task Force.

## 3.4 COMMUNICATIONS AND INFORMATION TECHNOLOGY ASSISTANCE EFFORTS

Scientific and Engineering assistance was provided to several public safety agencies in the general area of communication and information technology. Assistance ranged from simple responses to questions, to more detailed studies, analyses, and on-site visits. Activities that required analysis and/or site visits were conducted on behalf of the following agencies:

- *Amherst (NY) Police Department*—Provided assistance in assessing the cause of performance problems with their radio system and assessing problems caused by in-car computers interfering with their radios.
- *Erie County (NY) Central Policing Services*—Provided assistance in assessing the cause of receiver coverage problems with their mobile data terminals.
- *Essex County (MA) Sheriff's Office*—Conducted an on-site visit to assist in identifying information technology needs for the Essex County Jail.
- *Franklin (VA) Police Department*—Provided assistance in identifying potential solutions for a radio coverage problem.
- *Madison County (NY) E911 Center*—Provided assistance in identifying requirements for a CAD/RMS system and mobile data terminals.
- *Renssalaer County (NY) Sheriff's Department/Broome County (NY) Sheriff's Department/Albany County (NY) Sheriff's Department/Onondaga County Sheriff's Department (NY)/Oneida County (NY) Sheriff's Department* —Conducted site visits to jails administered by each of these agencies and compiled a "best practices" guidebook for tracking gang activity and information in the county jails.
- *Oneida County (NY) E911 Center*—Provided assistance by identifying requirements and developing a plan for a multi-jurisdictional CAD system.
- *Rome (NY) Fire Department*—Provided assistance by analyzing the radio coverage from two different candidate tower sites.
- *West Seneca (NY) Police Department*—Provided assistance in assessing the cause of performance problems with their radio system.

## 3.5 OTHER SCIENTIFIC AND ENGINEERING ASSISTANCE EFFORTS

Technical support was provided to the New York State (NYS) Department of Correctional Services (DoCS) Product Evaluation Committee (PEC). The PEC evaluates new products to be procured by the NYS DoCS system or facilities. Information coordination was provided for the PEC by tracking product evaluations in other states to facilitate information exchange and provide technical advice on products under evaluation.

General technical support to the NLECTC-NE has been provided, including compilation of reports for the National Institute of Justice (NIJ), conference and meeting coordination, maintenance of the Northeast website, and grant assistance. There were 254 requests for information received by the NLECTC-NE. These included Commercialization Assistance, Equipment Acquisition Assistance,

Requests for Information & Publications Assistance, Standards and Testing, Technology Assistance (SEAS), Technology Demonstrations/Introductions, and Training Assistance (Capacity Building).

# 4. SPECIAL PROJECTS

## 4.1 ADVANCED GENERATION INTEROPERABILITY FOR LAW ENFORCEMENT

The Advanced Generation of Interoperability for Law Enforcement (AGILE) program is a major commitment by the National Institute of Justice (NIJ) to address the issues of interoperability that hampers effective and efficient cooperation among multiple law enforcement and other public safety agencies. Interoperability issues appear in various ways: communications systems which cannot support inter-agency communications, information that is not accessible by all agencies who need it, and open case and suspect information maintained by one agency that is unknown by other agencies working on related cases. The AGILE program is a broad-based set of activities to address the varied aspects of the interoperability challenge, organized into three major thrust areas:

- Research, development, test, and evaluation (RDT&E);
- Standards identification, development, and adoption; and
- Outreach and technical assistance.

A key component of the AGILE RDT&E thrust area is an Operational Test Bed (OTB) in a public safety environment to integrate, test, and evaluate technologies that can contribute to addressing interoperability needs. For the OTB, candidate technology solutions to specific interoperability requirements are categorized and evaluated to address key issues of voice over-the-air interoperability, data transmission interoperability, data sharing, and data analysis. The evaluations include quantitative performance measurements as well as qualitative evaluations of the impact of the technology on law enforcement agency operations.

NIJ has partnered with the Alexandria Police Department to be the focal point of an Operational Test Bed (referred to as the Operational Test Bed-Alexandria, or OTB-A) to evaluate interoperability technologies. Emergent, under contract to the NLECTC-NE, is providing the technical and systems engineering support for integrating technologies into the OTB-A.

Activities in support of the OTB-A have generally involved two major initiatives: the deployment of crossband technology to facilitate voice communications among multiple agencies operating radio systems on different frequency bands; and technology to facilitate rapid image dissemination of images of missing children when officers respond to a missing child call. In addition to these two initiatives, the Team is also providing technical support to a pilot project to further investigate applications of crossband technology in a pilot project in Syracuse, NY. Finally, the Team has also provided support to other AGILE activities, including research and development, identification and development of standards, and education/outreach activities. Each of these activities is described in the sections that follow.

### 4.1.1 Crossband Technology for Voice Communications Interoperability

A fundamental interoperability challenge is over-the-air voice communications among agencies that have different radio systems operating in different radio frequency bands. The Team has installed a Gateway Device in the Alexandria (VA) Police Department. This Gateway provides direct connectivity between the radio systems of the Alexandria Police Department (APD) and departments with overlapping or adjacent jurisdiction, accommodating the fact that these systems operate at different frequency bands (VHF, UHF, and 800 MHz).

The Gateway Subsystem is the equipment shown inside the red box in Figure 4-1, and includes antennas, radios, the ACU-1000, a PC-based graphical user interface (GUI) located with the ACU-1000, a

dispatch supervisor's console (consisting of the same GUI and an audio unit), and the cabling necessary to connect these components.

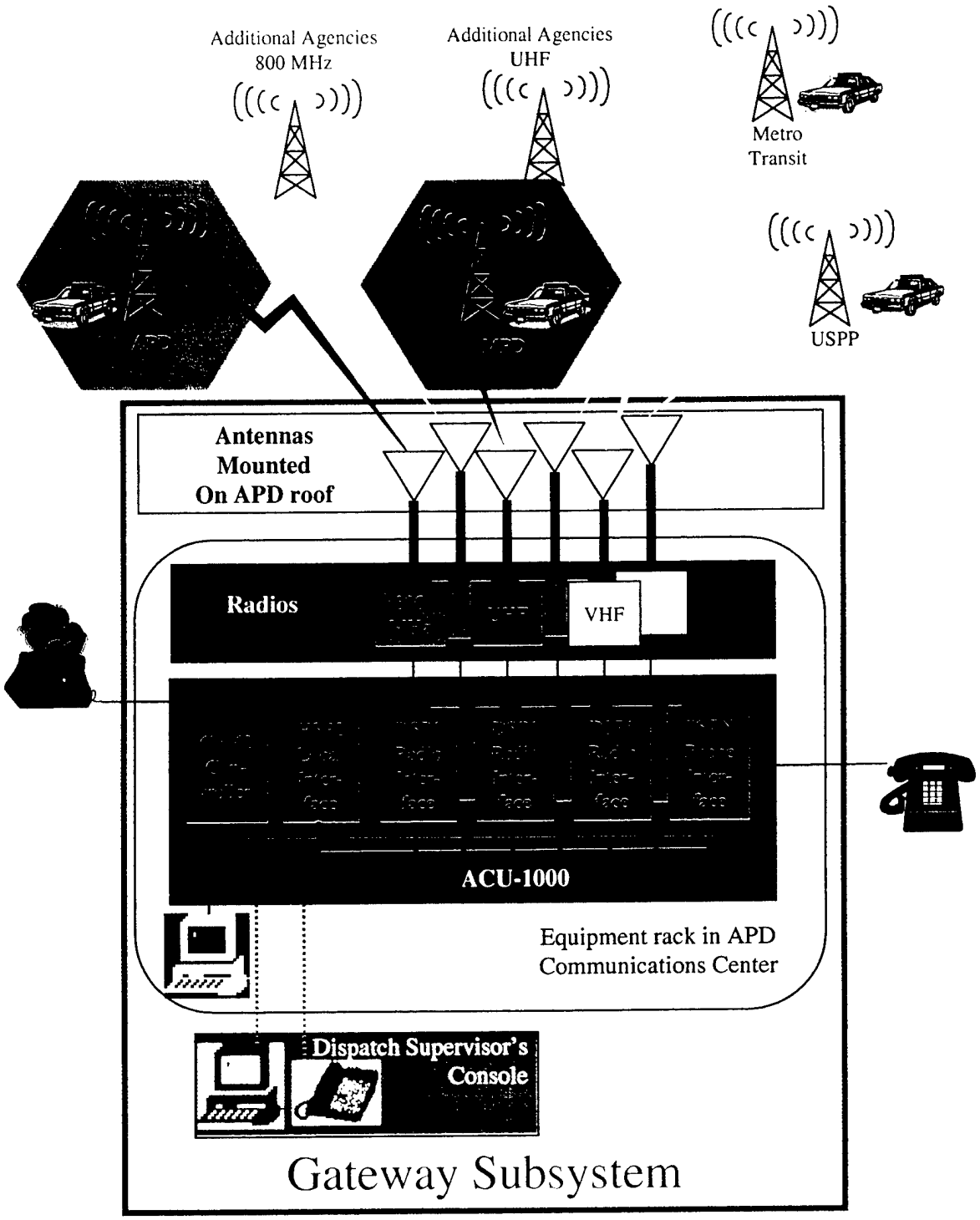


**Figure 4-1: Gateway Subsystem Architecture**

The heart of the Gateway Subsystem is the ACU-1000 Intelligent Interconnect System, a commercial product developed by JPS Communications. The ACU-1000 is a modularized approach to interconnecting various types of communications systems, including land mobile radios. Its basic components include:

- Interface modules, each designed to connect communications media such as radios or telephones;
- A control module;
- A power supply module;
- A local operator interface module;
- A chassis to accommodate the modules, and
- A backplane to route audio and control signals between modules.

For each radio system being connected by the ACU-1000, a radio is integrated into the unit through an interface module. The interface modules convert communications traffic into its essential elements: receive and transmit audio, and non-proprietary and/or industry-standard accessory port control signals (required to control the device to which the module is interfacing). Software to control the unit includes an intuitive user interface to connect and disconnect the radios integrated into the unit. Voice prompts give users audible instructions for establishing connections. Setting up connections can be done remotely using standard DTMF tones such as from a telephone or radio DTMF keypad. Local control is provided using the operator interface module, or using the software interface program running on a PC.

The antennas are mounted on the roof of APD's headquarters building, as shown in Figure 4-2. The antennas were selected and installed in order to ensure that the radios interfaced to the ACU-1000 can communicate with select repeaters of each participating agency. In this way, any radio within the coverage area of its own land mobile radio system can communicate with the radio systems of the other participating agencies via the Gateway Subsystem.

The radios and ACU-1000 are mounted in an equipment rack (see Figure 4-3) in the Equipment Room of the APD Dispatch Center located at APD headquarters. The radios are programmed with frequencies licensed to the participating agencies. Typically the radios are set to a default channel that a participating agency designates for inter-agency communications. Radio channels may be switched manually as required to transmit and receive on a different frequency channel, or to accommodate a different participating agency. For example, the second 800 MHz radio (currently programmed to interface with APD) provides immediate expansion to accommodate additional participating agencies with 800 MHz radio systems and a repeater within coverage range of the Gateway Subsystem.

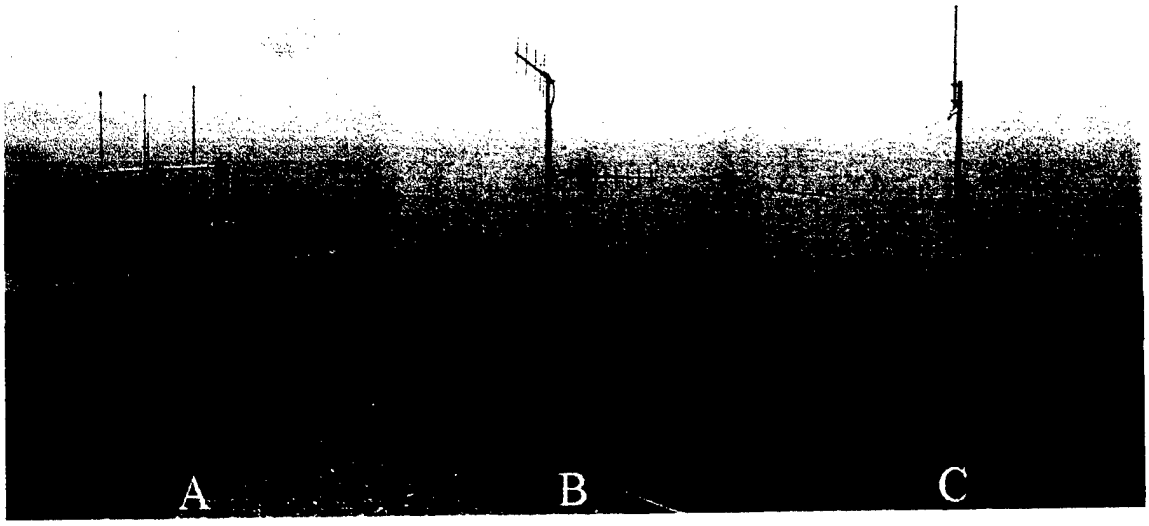


**Figure 4-2: Gateway Subsystem Antennas**

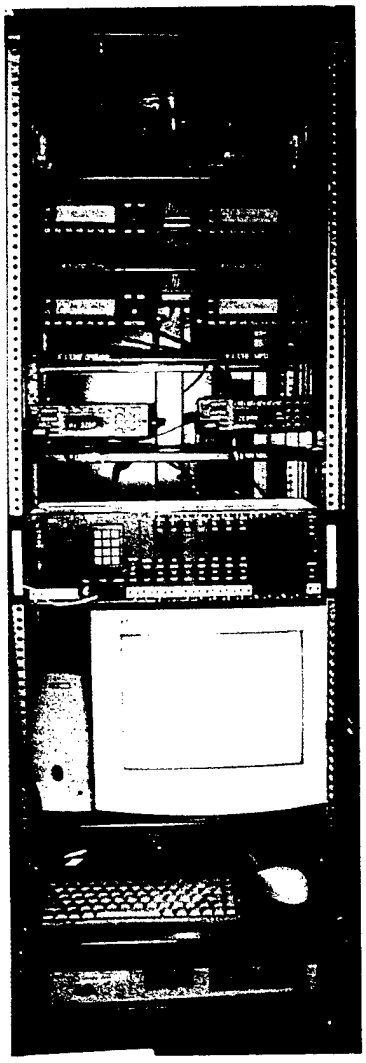

**Figure 4-3: Gateway Subsystem Equipment Rack**

After the Gateway Subsystem was installed, a series of functional and operational tests were conducted. The primary objective of these tests was to ensure that the Gateway Subsystem functioned sufficiently to begin use in multi-agency training exercises. These tests were not a comprehensive evaluation of all equipment functionality, but rather a set of progressively involved tests to ensure that radio-to-radio over-the-air communications across agency radio systems could be accomplished through the Gateway Subsystem.

Key issues addressed in these tests included:

- Communication: Ensure that the Gateway Subsystem can communicate with dispatch centers and field officers of the participating agencies.
- Control: Ensure that connections can be created and terminated through the ACU-1000 console.
- Interoperability: Ensure that the connections established through the ACU-1000 allow communications among radios operating on different radio systems.
- Voice Quality: Ensure that the communications can be understood, and without unacceptable delays.

These tests were organized into sets that progressively test the capabilities of the subsystem. The tests were as follows:

- Functional Test:
  - Receive only tests – no links;
  - Receive only, audio link to PSTN-1, no transmissions;
  - Transmission tests to a non-operational channel;
  - Transmission tests to communications centers, no links;
  - Transmission tests direct to field units, no links;
  - Test links and unit to unit transmissions;
  - Test link within same band (USPP – Metro Transit); and
  - Link multi-bands with units side by side.
- Operational Tests:
  - Follow the Leader (Operational Tests #1 and #3); and
  - Traffic Control (Operational Tests #2 and #4).

The Gateway Subsystem at the Alexandria Police Department underwent its first operational use as part of the communications infrastructure used to support security for the Inauguration of George W. Bush. The AGILE Project Team offered use of the subsystem (including the ACU-1000 switch manufactured by JPS Communications) since it met most of the interoperability requirements of the U.S. Secret Service (USSS). The AGILE Project Team worked with the USSS to extend the configuration to interface with the radio systems of the USSS, the U.S. Capitol Police, and the FBI. They installed additional antennas and radios to create the interface between the Gateway Subsystem and these agencies.

During the Inauguration activities, a link was opened to connect these three agencies with the Metropolitan Police Department (MPD) and the U.S. Park Police (USPP). Since MPD and USPP are currently participating in operational testing of the Gateway Subsystem, it had already been configured to link with the radio systems of those agencies. The link was open on a continuous basis for 36 hours and designated for use in the event of a major incident. While no major incident occurred, testing and incidental radio traffic confirmed that the link was operational during the designated time period.

According to the Secret Service After Action Report, "The equipment functioned as designed, providing good cross-band transmit and receive audio to all agencies. The ease of operation and versatility was excellent. The [ACU-1000] software provided excellent accessibility to the modules being used for the multiple sites and could be manipulated to isolate sites instantaneously."

Since the Inauguration, the Gateway Subsystem has been utilized for other operations. The U.S Park Police (USPP) and Metro Police Department (MPD) used the Gateway Subsystem to support joint details for presidential escort. USPP and APD were linked through the Gateway Subsystem when searching for the perpetrator of an attempted abduction in a park in Alexandria.

Based on the successful operations described above, additional agencies agreed to participate in testing, including the U.S. Capitol Police, U.S. Marshals Service, and the Maryland State Police (MSP). The U.S. Marshals Service provided an MCS2000 radio, and the Maryland State Police provided an antenna and a 60-watt base station radio for their 39.3 MHz frequency. The antenna was mounted on a tripod and placed on the roof; the base station was installed on the top shelf of the rack. MSP also provided an interface cable to connect the radio to the ACU-1000. The system was connected and a functional test was executed linking the MSP with the Alexandria Police Department's (APD) 800 MHz Zebra channel. Communications were successfully conducted from the Forestville Barracks to an APD handheld unit. MSP field units could be heard as well as the MSP College Park Barracks, but no field unit testing was conducted. MSP also tested the RTU-200 unit that enables a remote site to be linked into an ACU-1000 through a land line connection. This approach is being evaluated as a potential approach to linking in the Department of Transportation agencies.

Several documents were generated based on the work described above, including:

- A Technical Memorandum describing Lessons Learned.
- Operational Test Bed—Alexandria Communications Interoperability Gateway Subsystem Description Document, AGILE Report No. TE-00-01, 15 February 2001.
- Operational Test Bed—Alexandria Communications Interoperability Gateway Subsystem Operational Test Document, AGILE Report No. TE-00-04, 23 July 2001.

These reports are available at the AGILE Web site (www.agileprogram.org).

### 4.1.2 CapWIN Support

Part of the AGILE effort included support of the Capital Wireless Information Network (CapWIN) project. The goal of CapWIN is to deploy a wireless information infrastructure in the metropolitan Washington (DC) area to support transportation and public safety information exchange requirements. Support included assisting in requirements definition for, and developing the Request for Proposal for, the data switch.

### 4.1.3 Rapid Image Dissemination for Missing and Exploited Children

Technology exists to facilitate the rapid dissemination of images in scenarios involving missing and exploited children. Another initiative undertaken in the OTB-A is an integration of relatively inexpensive commercially-available equipment to provide a rapid dissemination of images of children and to interface with the existing infrastructure put in place by the National Center for Missing and Exploited Children (NCM&EC). The objective of this technology integration is to provide a means for shortening the timeline from when an officer first responds to a missing child call, until the time that photographic images arrive at the location where they can be useful (e.g., in other patrol cars and at the NCM&EC).

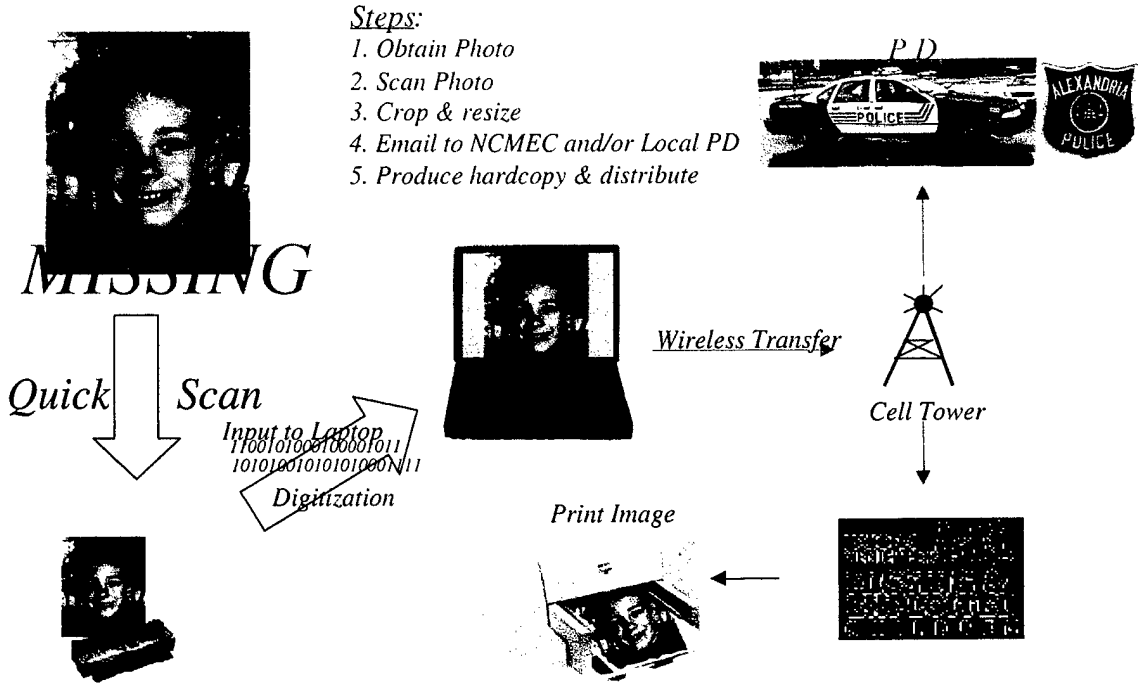


**Figure 4-4: Concept for Rapid Image Dissemination for Missing and Exploited Children**

The initial deployment utilized a Canon BJC-50 handheld scanner/printer connected to a laptop computer in a patrol car. As depicted in Figure 4-4, an officer responding to a missing child call can immediately scan a photograph to capture an image which then can be either transmitted back to a police station for further processing, or be cropped and sized by an officer directly on his/her laptop. In addition to immediate dissemination of the image to other officers, the printer capability can be used to generate hardcopies on the scene for distribution and neighborhood canvasses. In addition, the capability to format images and transmit them to the NCM&EC has also been incorporated.

Due to constraints in the Alexandria Police Department Mobile Data Browser[1], this capability could not be fully demonstrated in the OTB-A. However, APD's Youth Division began beta-testing the software on desktop systems to address a backlog of missing children and runaway cases. They scanned photographs using the software and then posted the images on the Mobile Data Browser to be downloaded to patrol cars. Based on their feedback, a number of enhancements were made to the software.

### 4.1.4 Syracuse Communications Interoperability Operational Evaluation

The objective of this operational evaluation is to (a) demonstrate and evaluate use of ACU-1000 in situations that require secure communications; and (b) identify technical and operational requirements for interoperability among local, state, and federal agencies in situations that require secure communications. Under this activity, the NLECTC-NE is assisting the Syracuse Police Department in configuring and deploying an ACU-1000, which they purchased for both general incident management as well as

[1] The current system does not allow uploading of images from a patrol car through the Mobile Data Browser; images can only be downloaded. While images can be emailed without using the Mobile data Browser, Internet access is not enabled from the patrol cars.

counternarcotic task force operations. The counternarcotics application requires that communications be encrypted.

NLECTC-NE assembled an ACU-1000 along with VHF and UHF radios. Support was provided to the Syracuse Police Department and Onondaga County Sheriff's Department with the initial testing phase of the mobile ACU-1000 communications base including linking various channels. The links were all operational although some parameters were identified that needed modification to optimize performance. The initial plan to deploy the unit in a van was changed because the unit did not fit in the van. Instead, the unit was hooked to VHF and UHF antennas at SPD's Special Investigation Division. Radio checks were conducted with radios in the building as well as in the field. Some parameters were adjusted to address repeater hang time issues and audio quality.

### 4.1.5 Support to Other AGILE Initiatives

In addition to the Test & Evaluation activities described in the preceding sections, the NLECTC-NE staff also supported other AGILE initiatives. Activities included the following:

- Monitored research and development grants awarded by NIJ under the AGILE program, including Software Radio Infrastructure, awarded to Vanu, Inc., of Cambridge, Massachusetts, and Multi-Band Antenna System, awarded to Mission Research Corporation, Dayton, Ohio.
- Provided material for the AGILE Website.
- Compiled technical documentation from the Test & Evaluation activities as well as other documents, reports, papers, and videos relating to the AGILE program, and produced an Interoperability Resource CD-ROM to be provided to public safety practitioners.
- Began writing a series of Executive Technology Briefs on key topics in communications interoperability.

## 4.2 COMPUTER CRIME INITIATIVES

### 4.2.1 National Law Enforcement CyberScience Laboratory (NLECSL-NE)

The Emergent Team established the National Law Enforcement CyberScience Laboratory - Northeast (NLECSL-NE), also known as the CyberScience Lab (CSL) in March 2000. The mission of the CSL is to provide e-crime technical assistance, build a forensic tool knowledge base, and heighten awareness of cybercrime issues among federal, state and local law enforcement agencies. It is the first such lab in the Northeast, co-located with the Air Force Research Laboratory/Information Directorate (AFRL/IF) in Rome, NY at the Griffiss Business and Technology Park. CSL is in partnership with several state and local law enforcement agencies and Utica College as shown in Figure 4-5.

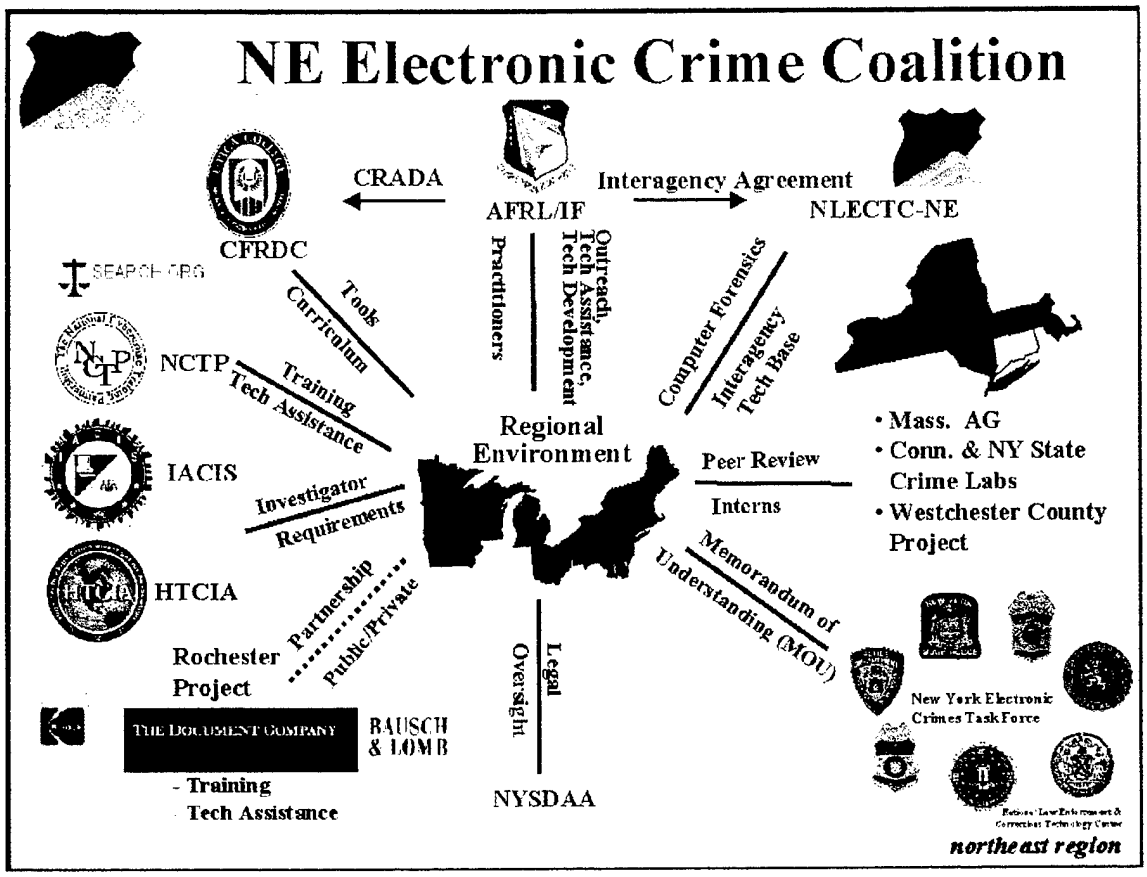


**Figure 4-5: NE Electronic Crime Coalition**

The CSL is involved in multiple projects that encourage government, industry and academic collaboration to address cybercrime technical issues.

Another venture of the CSL is distributing e-crime technology and tools, and providing training materials to state and local law enforcement agencies, high tech crime task forces and regional computer forensics crime laboratories. Software tested included the following:

- 'extractor', a utility developed by WetStone Technologies and used to recover deleted data from Linux-based systems;
- 'EnCase', a tool developed by Guidance Software specifically for the computer forensics arena; and
- Analyst Notebook, software used in performing various analyses of the Melissa Virus case, that allows investigators or analysts to generate charts that assists in reading through complex information and discovering key information throughout an investigation. The Link Notebook portion of the software is a visualization tool that is designed to link charts to uncover, interpret, and display connections and relationships within data. The Case Notebook portion of the software is a visualization tool that creates charts in which events are positioned on a timeline allowing the charts to reveal sequences of events over time during an investigation. This part of the software is also useful for establishing the cause and effect of events and corroborating witness statements.

Work began on investigating the feasibility of establishing a Center of Excellence in the fields of information assurance and electronic crime. Operational planning documents are currently under review by parties involved to ensure a strong partnership and technology transfer opportunities to benefit communities at large. Parties involved include NIJ, NLECTC-NE, the Institute for Information Assurance at Cornell and the AFRL/IF Information Institute.

To publicize the CSL, an article on the National Law Enforcement Cyberscience Lab (NLECSL-NE) was submitted to the AFRL/IF publication entitled "Technology Horizons". Also, a story on the New York Electronic Crime Task Force (NYECTF) was published in the summer 2000 issue of TechBeat.

### 4.2.2 Training and Outreach

Training was provided on the installation and use of "Extractor", a Linux file system deleted file recovery tool, for the Connecticut State Police Crime Lab. The Team also researched and tracked the events that occurred in the Tim Lloyd and Love Bug case and documented them with Analyst Notebook software.

The e-Crime Intern Program provides a unique opportunity for college students to gain knowledge and hands-on experience in the field of cyberscience in the law enforcement community. The foundation of this program is a joint venture between academia and both public and private sectors in an effort to expose students to a challenging experience in support of cyberscience developments.

The Team also held CFX 2000, a cyber forensics experiment that was a collaborative effort between the Department of Defense (DoD), NIJ, various law enforcement agencies, the commercial sector and academia. This three-day experiment provided technical analysis and evaluation of computer forensic tools and provided recommendations for the law enforcement and military defense communities in response to cyber threats. The approach involved the enactment of a pragmatic scenario that depicted a cyber attack on an information and economic infrastructure.

As a member of the New York Electronic Crimes Task Force (NYECTF), CSL has formed a partnership with the United States Secret Service (USSS) and a host of other public safety agencies and private corporations. The NYECTF, in partnership with various sponsors, presented the International Conference on e-Crime (ICE): Prevention, Detection and Enforcement. ICE featured keynote speakers, panel discussions, papers, presentations, tutorials and exhibits highlighting the prevention, detection and enforcement of electronic crime. The conference provided a collaborative environment in which law enforcement practitioners, technologists, and researchers addressed the rapidly emerging threat of electronic crime.

The Team hosted the Basic Data Recovery and Analysis Course at the National White Collar Crime Center in Fairmont, WV. The event was a hands-on training course that focused on preparing investigators for the challenges created by computer literate criminals, data recovery of digital evidence, and extraction of information for criminal investigations. The course was a big success.

The Emergent Team along with AFRL/IF hosted the first workshop in the Information Assurance and e-Crime Workshop Series: Opportunities for Public, Private and Academic Partnerships in Information Assurance and e-Crime. The workshop served as a forum to address Information Assurance and e-Crime Interdependency, sources of support and current capabilities and building collective momentum. The workshop was held at SUNY-IT Utica/Rome in Marcy, NY.

### 4.2.3 Cybercrime Conferences, Meetings, and Training

The Team has attended several Cybercrime events over the course of the contract, which contributed to their overall knowledge base and expertise, which in turn was shared with state and local police agencies across the Northeast Region. These activities are listed below.

| DATE | CONFERENCE | LOCATION |
|---|---|---|
| May 2000 | Forensic Sciences and Crime Scene Technology Conference and Exposition (FRENZY) | Washington, DC |
| May 2000 | Northeast Chapter of High Technology Crime Investigation Association (HTCIA) | US Secret Service, New York, NY |
| May 2000 | New York Electronic Crimes Task Force (NYECTF) quarterly review meeting | US Secret Service, New York, NY |
| June 2000 | Northeast Chapter of the High Tech Crime Investigation Association (HTCIA) | US Secret Service, New York, NY |
| July 2000 | NIJ OS&T Digital Evidence Planning Panel Meeting | DoD Computer Forensics Lab Linthicum, MD |
| August 2000 | New York Police Department Conference on New Frontiers in Policing | New York, NY |
| August 2000 | NIST/OLES Meeting on Electronic Crime Scene Investigation: A Guide for First Responders | Gaithersburg, MD |
| August 2000 | AFRL/IF and the New York State Office for Science, Technology and Academic Research | Rome, NY |
| September 2000 | High Technology Crime Investigation Association 2000 International Training Conference | Chicago, IL |
| September 2000 | NIJ Cybersecurity Roundtable Meeting | Washington, DC |
| September 2000 | Digital Evidence Collection, Processing and Presentation | Rome, NY |
| October 2000 | Computer Forensics Experiment (CFX) - 2000 | NY State Police FIC Albany, NY |
| October 2000 | San Diego Regional Computer Forensic Laboratory (SDRCFL) Conference | San Diego, CA |
| November 2000 | NIST/OLES Technical Working Group Meeting | Orlando, FL |
| November 2000 | Scientific Working Group on Digital Evidence Meeting | DoD Computer Forensics Lab Linthicum, MD |
| November 2000 | NIST/OLES Technical Working Group Meeting | Gaithersburg, MD |

| DATE | CONFERENCE | LOCATION |
|---|---|---|
| January 2001 | CyberCrime 2001 Conference and Exhibition | Foxwoods Resorts and Casino, Connecticut |
| February 2001 | International Conference on Electronic Crime | New York, NY |
| March 2001 | New York Electronic Crimes Task Force Meeting (NYECTF) | US Secret Service, New York, NY |
| April 2001 | Basic Data Recovery and Analysis Course at the National White Collar Crime Center | Fairmont, WV |
| April 2001 | Information Assurance and e-Crime Workshop Series: Opportunities for Public, Private and Academic Partnerships in Information Assurance and e-Crime. | SUNY-IT Utica/Rome Marcy, NY |
| May 2001 | Advanced Training session at the International Association of Computer Investigative Specialists (IACIS) Annual Training Conference | Altamonte Springs, FL |

## 4.3 OPERATIONAL EVALUATION OF CONCEALED WEAPONS DETECTION DEVICE FOR SCHOOL SAFETY

The National Institute of Justice (NIJ) funded implementation of a Concealed Weapons Detection (CWD) Testbed in one of New York City's public schools to gather data on the potential of a magnetic gradiometer based system to augment the standard detection apparatus used by School Safety detachments of the New York City Police Department (NYPD). This project was developed to address problems experienced in New York City's schools associated with incidents of violence committed by razor blade slashings. Despite the fact that metallic object detection devices have been installed in a number of schools, some students have been able to hide razor blades and Exacto blades in various ways designed to avoid detection by the current genre of equipment used by school safety personnel.

The Idaho National Engineering and Environmental Laboratory (INEEL) in Idaho Falls, Idaho, has modified Passive Magnetic Gradiometer technology originally developed for defense applications such as submarine detection to passively locate ferrous metal objects being carried in a concealed fashion. The resultant product is called the Secure Scan 2000. The objective of the CWD Testbed was to assess the utility of deploying such technology (in the form of a Secure Scan 2000) in a public school environment.

In order to ensure "non interference" with normal operations, a "Usability Test" format was selected as the means for gathering initial data on the Secure Scan 2000. The Usability Test was conducted at the CWD Testbed implemented at Washington Irving High School in Manhattan under a Joint Memorandum of Understanding (MOU) developed by the National Law Enforcement and Corrections Technology Center—Northeast and the NYPD School Safety Division.

The Secure Scan 2000 model used in the Testbed is the first mobile version of this product to be used in this capacity. The system consists of the following elements:

- Passive Magnetic Gradiometer Detection Gate;

- Miniature Video Camera;
- Customized Software to superimpose detection data on video images; and
- Specialized Operator Console to house computer, video camera, and uninterruptible power supply.

The NYPD School Safety Division selected Washington Irving High School (WIHS) as the site for the Testbed. The Secure Scan 2000 was deployed within the framework of the existing security systems, because the new CWD technology needed to be introduced on a not to interfere basis with normal security operations. In this way the Secure Scan 2000 primarily provided an additional degree of localization and identification when combined with systems in use at WIHS. The CWD Testbed (shown in Figure 4-6) consisted of the following systems:

- Student ID card Scanner;
- CEIA Metallic Item Detector;
- Baggage Scanner;
- Secure Scan 2000 Ferrous Metal Detector; and
- Garrett Hand Scanner.

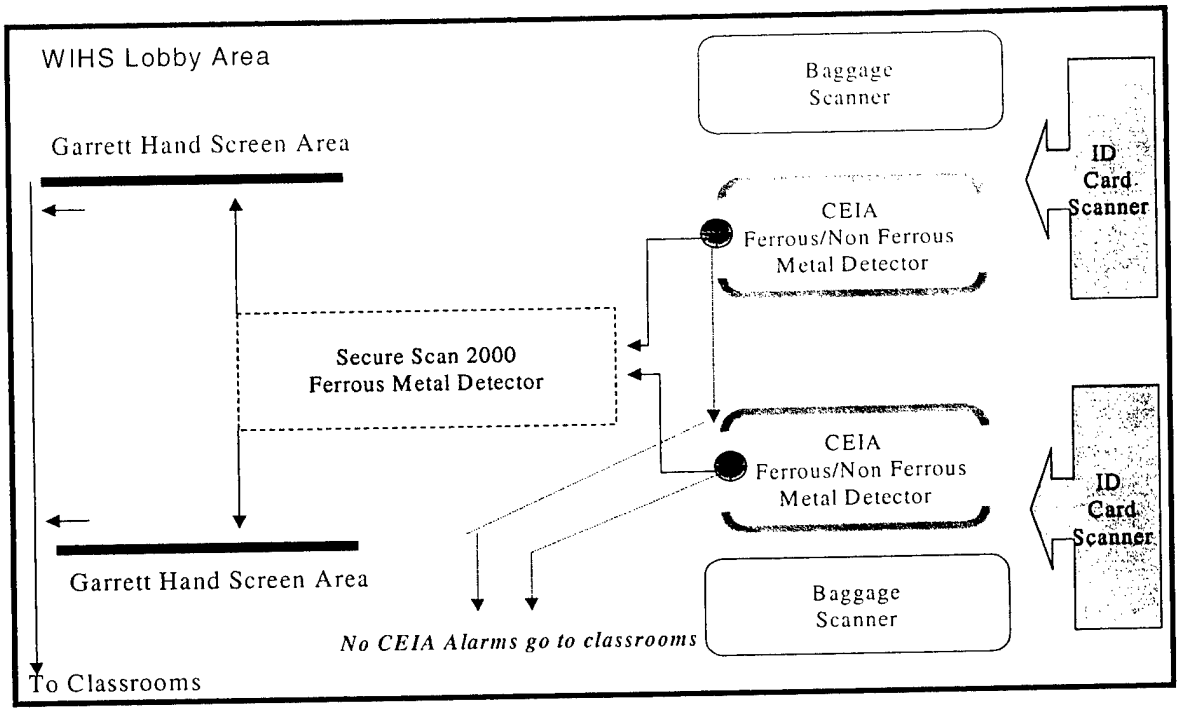


**Figure 4-6: CWD Testbed Layout**

Observations were collected from the school security officers' users in the following areas:

- User Interface,
- Detection Thresholds, and
- Distinguishing Features.

User Interface evaluations centered on the characteristics of the Secure Scan 2000 system that influenced its ease of setup, breakdown, storage, operating system software initiation, integration into the existing security environment, operational employment, and automated data collection application.

Detection Thresholds have dynamic ranges that can be set to optimize detection of certain objects. The focus of the usability test in this area was to determine the users' capability to adjust the dynamic detection thresholds. A default range is set upon system initiation that users can then modify. User observation of patterns associated with detection ranges and objects detected serves as the foundation for decisions on using other than the default settings.

Users were also asked to comment on Distinguishing Features of the Secure Scan including: the ability of the system to automatically collect time and date of a detection; recording a video image of the individual in the detection gate; the location of objects detected by the device's passive magnetic Gradiometer; and its ability to capture this data on video.

The Secure Scan 2000 was deployed at WIHS and data was collected over a 10-week period. Four methods were used to gather information on operation of the system during the active phase of Testbed data collection:

- User's Logbook,

- Interviews,
- Reports, and
- Electronic Information Capture.

In general the users were able to set up and use the Secure Scan 2000, and students quickly became acclimated to passing through the device when required. A number of recommendations were forwarded to the developers regarding the configuration and documentation associated with the Secure Scan 2000. A more detailed description of the CWD Testbed and the detailed findings and recommendations can be found in *A Final Report on the NIJ Concealed Weapons Detection School Safety Project Testbed*, NLECTC-NE, currently in draft form.

## 5. FUTURE OUTLOOK

The vast majority of NLECTC-NE's efforts are ongoing. Technical and administrative support will continue to be provided under follow-on contract funding.

***MISSION***
***OF***
***AFRL/INFORMATION DIRECTORATE (IF)***

*The advancement and application of Information Systems Science and Technology to meet Air Force unique requirements for Information Dominance and its transition to aerospace systems to meet Air Force needs.*