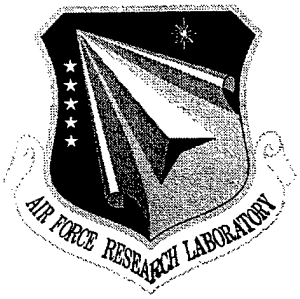
AFRL-IF-RS-TR-2000-143
Final Technical Report
October 2000



REQUIREMENTS DEFINITION FOR THE AUTOMATED REGIONAL INFORMATION EXPLOITATION/SHARING SYSTEM (ARIES)

Computer Systems & Communications Corporation

Cassandra Neal and April Roberson

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-2000-143 has been reviewed and is approved for publication.

APPROVED: 

PETER J. COSTIANES
Project Engineer

FOR THE DIRECTOR: 

JOHN V. MCNAMARA, Technical Advisor
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/IFED, 32 Brooks Road, 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 2000	Final Jan 00 - Jun 00

4. TITLE AND SUBTITLE
REQUIREMENTS DEFINITION FOR THE AUTOMATED REGIONAL INFORMATION EXPLOITATION/SHARING SYSTEM (ARIES)

5. FUNDING NUMBERS
C - F30602-00-C-0010
PE - N/A
PR - NIJR
TA - 99
WU - 01

6. AUTHOR(S)
Cassandra Neal and April Roberson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Computer Systems & Communications Corporation
1911 N. Fort Meyer Drive
Arlington VA 22209

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2000-143

11. SUPPLEMENTARY NOTES
Air Force Research Laboratory Project Engineer: Peter J. Costianes/IFED/(315) 330-4030

12a. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This document presents all of the regional data requirements for Central New York law enforcement that are relevant to being potentially shared and exploited by ARIES for purposes of expediting and enhancing criminal investigative procedures. Since ARIES is more than a loosely formed concept, but a system envisioned to leverage reusable components that were developed for an existing military automated analytical system, it seems logical to consider a context in which these data requirements can be met. Therefore, this document also presents high level proposed solutions (prioritized by practitioners), and network, hardware, and software requirements and issues.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Requirements Analysis, Law Enforcement, Data Sharing	44
	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

List of Figures

1. SUMMARY

This document is a result of a requirements assessment study that was conducted for the Central New York region's criminal law enforcement community. This community is comprised of several law enforcement agencies which are identified in the Scope section of this document. The primary purpose of the study was twofold:

1. To determine the data requirements of law enforcement personnel for identifying and locating criminal offenders by utilizing agency and inter-agency electronic records information, and
2. To assess if these requirements can be met with an automated solution in a networked environment.

This document is designed to convey the requirements that were identified during the study in the context of being supported by the Automated Regional Information Exploitation/Sharing System (ARIES).

Due to the private and sensitive nature of law enforcement information, and the impact of unauthorized access, by either internal or external penetration of the system, this regional information assurance network should protect electronic resources from unauthorized access, disclosure, eavesdropping, and tampering. Therefore, privacy and security requirements will be addressed herein in order to insure that these integral components are well understood prior to any ARIES design or implementation action.

Requirements to address ARIES usage and measures of success will be identified in this document. These requirements will help ARIES sponsors assess the value-added of ARIES for law enforcement while also providing invaluable leads to ARIES engineers for future enhancement and optimization considerations (such as indexing or caching frequently accessed data).

Each of the participating agencies has made it clear that they do not wish to replicate in house data. Therefore, ARIES should interface with existing records management systems (RMS) in a non-intrusive fashion so as not to impact existing data integrity or agency operations. The current design paradigm of ARIES includes a middle-ware solution that will gracefully provide read-only access to these data repositories without subjecting the agencies to compromise data ownership.

Finally, pursuant to the design of reusable software components and an open-ended architecture, ARIES will be scaleable enough to accommodate all the requirements presented in this document as well as meet future requirements.

2. BACKGROUND

Law enforcement officials in the Central New York region typically share information across agency boundaries. In the Central New York region, there is currently no infrastructure in place to support the sharing of inter-agency criminal data by electronically automated means; therefore, said information is generally shared via telephone. While this method does provide valuable leads, it has often fallen short because of the magnitude and time sensitive nature of criminal activity and related data. Designing and implementing a Central New York area automated network to support the dissemination and exploitation of law enforcement data could greatly enhance this region's crime analysis and investigation and overall law enforcement operations, resulting in tangible improvements in officer and public safety. Of course, to meet this goal, a thorough assessment of current law enforcement operations and data inquiry at the agency and inter-agency level must first be obtained. A study to assess these requirements was conducted during a six-month period in the Central New York region by Computer Systems & Communications Corporation (CSCC). The Northeast National Law Enforcement and Corrections Technology Center (NLECTC) assisted CSCC with the requirements assessment study by arranging meetings and interviews with appropriate law enforcement personnel.

3. OBJECTIVE

The objective of the study was to identify data requirements for law enforcement as they apply to investigative procedures for identifying and locating criminal offenders and to assess if these requirements can be met in a regional networked environment with an automated tool such as ARIES. Currently, information sharing between regional law enforcement agencies is achieved by telephone and Email. ARIES seeks to expedite this procedure by automating the sharing of information electronically.

Originally, it was suggested that ARIES interface exclusively with existing departmental records management systems (RMSs). But during the course of this study, it was found that regional access to supplementary data such as public record, photo id, and pedigree information could greatly enhance investigative procedures; especially when married with criminal record information. Of course, this supplementary data will only be exploited if it can be made available in electronic form.

This document will present all of the regional data requirements for CNY law enforcement that are relevant to being potentially shared and exploited by ARIES for purposes of expediting and enhancing criminal investigative procedures. Since ARIES is more than a loosely formed concept, but a system envisioned to leverage reusable components that were developed for an existing military automated analytical system, it seems logical to consider a context in which these data requirements can be met. Therefore, this document will also present high level proposed solutions (prioritized by practitioners), and network, hardware, and software requirements and issues.

4. CRITICAL ASSUMPTIONS AND CONSIDERATIONS

While the bulk of this document defines requirements as they pertain to regional law enforcement for purposes of information sharing, some recommended solutions will be presented as well. These solutions are not intended to define a comprehensive design and implementation approach; rather, they are presented in an exploratory context. It is often a natural progression when assessing functional requirements to consider solutions that may meet these requirements. And, as stated in the Statement of Work, assessing these requirements will "help define an automated and electronic infrastructure for information exploitation."

The Automated Regional Information Exploitation/Sharing System (ARIES) was conceived to provide regional law enforcement agencies interconnectivity for purposes of disseminating and exploiting offender data. ARIES is, however, more than just a concept born of a need to support the sharing of inter-agency law enforcement information. The ARIES concept evolved when it was seen as a good fit for law enforcement by adapting an operational, open-ended, scaleable, military-based data dissemination and exploitation tool (developed by CSCC) that supports NATO forces. It is therefore assumed that ARIES will leverage many of the software components developed for this military system.

This military tool is a browser-based system on a closed network that interfaces with Open Database Connectivity (ODBC) compliant databases using interchangeable Java components. The ODBC standard has allowed a series of military databases to be successfully and rapidly brought online and exploited. This is because ODBC drivers abstract away vendor-specific protocols by providing a common and seamless API to database clients; thus, precluding the need for vendor-specific customization.

The assumption is made that all data repositories addressed in this requirements document are ODBC compliant. This is because it is a technical consideration that ARIES initially interface only with those databases equipped with ODBC. This may sound limiting, but lack of a common database communications protocol is even more limiting. Many database servers now handle the ODBC standard of communication including (but not limited to) MS SQL, Sybase, Oracle, and MS Access. **Without** the ODBC layer, every unique vendor database would have to be reverse-engineered into the ARIES client software. This would prove costly and time consuming. **With** the ODBC layer, the ARIES client software can rapidly access many different database types with little customization.

New York State is phasing out the old Uniform Crime Reporting (UCR) system and replacing it with the more effective (in terms of data collection, analysis, and reporting) Incident Based Reporting System (IBR). While conducting this requirements assessment study, CSCC verified that each ARIES police department will comply with the IBR standard in collecting, aggregating, and reporting departmental crime information. These departments are currently using standardized NY State, IBR compliant Incident and Arrest Report forms. The records management systems (RMS)

for each of these departments will be IBR compliant as well. Therefore, it is assumed that ARIES will interface only with electronic crime report databases that are IBR compliant.

Finally, it is generally understood from our verbal exchanges with law enforcement study participants that the ARIES data-sharing infrastructure be contained as a wide area network (WAN) separated from the Internet and other departmental networks. Therefore, for the remainder of this document, it is assumed that ARIES will operate as an autonomous data sharing and exploitation network or virtual private network (VPN).

5. SCOPE

The target agencies for the requirements assessment study covered the Central New York region located in Oneida County. The agencies that participated in the study are:

1. Rome Police Department (RPD),
2. Utica Police Department (UPD),
3. New Hartford Police Department (NHPD),
4. Oneida County Drug Task Force (OCDTF),
5. Utica Arson Strike Force (UASF),
6. Oneida County Sexual Abuse Task Force (OCSATF), and
7. Oneida County District Attorney's (OCDA) Office.

The scope for the requirements assessment focused primarily on that portion of the law enforcement community that handles criminal investigations. Criminal investigators were targeted as the pilot user base in order to narrow the initial scope to the primary objective of locating and identifying criminal offenders. An ARIES prototype with this limited scope should prove successful and can subsequently be scaled to a broader scope by assessing new data requirements. Criminal investigators possess a rich working knowledge of the sources and types of criminal data (electronic or otherwise) available to them and provided excellent initial subjects for survey. Furthermore, they tend to have more computer expertise than the average practitioner. Finally, limiting the scope to criminal investigators was the logical choice for the requirements assessment study since it was determined that these individuals access and review criminal data in their day to day operations with greater frequency than the practitioner.

Interestingly enough, during the study, it was discovered that many of the data requirements of the investigators also satisfy those of the practitioner. The data would often be of the same origin, but the method in which it is used would differ between the two job categories. For the investigator, the data would aid in *solving* crimes; while for the practitioner the data would aid in *preventing* crimes. Nevertheless, the initial prototype will remain limited to the investigators, and; fortunately, will require little customization to adapt to an adjunct segment of law enforcement.

6. SHARED DATA REQUIREMENTS

The requirements presented in this section have been determined by a panel of law enforcement personnel from each of the 7 agencies participating in the ARIES Requirements Assessment study. These requirements were gathered and documented during the course of study and presented at a final Roundtable meeting. This meeting was comprised of representatives such as Police Chiefs, Captains, Lieutenants, and Investigators from various police departments and specialized Forces where shared data requirements gathered during the study were presented and subsequently agreed upon.

6.1 Departmental

Most of the study focused on shared data requirements. After all, the express purpose of ARIES is to provide a regional information sharing and exploitation tool. It was determined that the lion's share of criminal information is housed in the police departments; specifically in the form of police records. These records will be stored in record management systems (RMSs) within the next several months. This study focused on the type or content of the RMS data rather than the actual format or layout of the RMS data, since focusing on the latter would be better served when establishing a detailed system design model.

6.1.1 Utica PD (UPD)

Of all ARIES study participants, UPD will have the most advanced RMS which will cover virtually all police reports generated within the department. This RMS is a commercial off-the-shelf package that has been customized to suit some specific needs of UPD. The product was developed by Pamet Systems, Incorporated and is called PoliceServer NT and it houses crime report information in a Microsoft SQL Server database. UPD will also be purchasing and installing CADServer NT; however, there are no plans at this time to exploit CAD data with ARIES since other regional police departments' CAD data will be managed by Oneida County (who is not participating with ARIES at this time). Pamet Systems Project Manager for the effort to introduce PoliceServer NT to UPD has been contacted, and an open dialog was established. CSCC feels that this Vendor will be forthright in providing technical support for exploiting this RMS data with a regional information sharing tool such as ARIES.

Figures 6.1 through 6.8 outlines the UPD crime data that can be exploited and shared with ARIES.

6.1.2 Rome PD (RPD)

During our study, it was determined (according to NLECTC/NE) that RPD will be implementing the Government funded Spectrum Justice System (SJS) RMS to house departmental police record data. This GOTS software stores crime report information in an Oracle database which can most definitely be leveraged by ARIES. Moreover,

CSCC has already received the Entity Relationship Diagrams (ERDs) for each of the SJS databases comprised of Incident, Arrest, Person, and Warrant information.

However, very late in the stage of the ARIES requirements assessment study, NLECTC/NE claimed that due to RPD's size, an RMS other than SJS may be considered in lieu of SJS. Until a concrete and final decision is determined, we must assume that NLECTC/NE's original proclamation stands; namely, that RPD will be using SJS. Of course, if a different RMS is adopted for RPD, we are assuming that NLECTC/NE will recommend a state-of-the-art solution that is ODBC compliant.

Figures 6.1 through 6.8 outlines the RPD crime data that can be exploited and shared with ARIES.

6.1.3 New Hartford PD (NHPD)

Currently, NHPD is using an antiquated HP2000 mini/mainframe as RMS database and application servers. The system software for the RMS (and CAD) is ICAD Incorporated vendor software that was customized especially for NHPD. Currently, this system is not networked, nor is there any peripheral terminal access. In addition, the RMS database (HP's Image Database) is not ODBC compliant (although we were informed by ICAD Inc that there is a Unix shell wrapper for this software that would migrate the environment into a less proprietary and more desirable ODBC environment).

Fortunately, NHPD will be implementing a more state-of-the-art RMS into the department. It was determined (according to NLECTC/NE) that NHPD will be implementing the Government funded Spectrum Justice System (SJS) RMS to house departmental police record data. This GOTS software stores crime report information in an Oracle database which can most definitely be leveraged by ARIES. Moreover, CSCC has already received the Entity Relationship Diagrams (ERDs) for each of the SJS databases comprised of Incident, Arrest, Person, and Warrant information.

Figures 6.1 through 6.8 outlines the NHPD crime data that can be exploited and shared with ARIES.

6.1.4 Special Forces

The crime reports for the special Forces will actually be stored in regional police department RMS databases. This is a policy requirement since the task and strike forces are comprised of officers and investigators from various police departments in Oneida County. Therefore, the special Forces will participate in any ARIES follow-on in a read-only mode. Most of the crime information stored electronically at the special Forces is case information which will not be released outside the respective agencies. There may be some special Forces data that can be exploited by ARIES such as street names (for example, a drug dealer may be more readily identified on the street as "Lefty"). But there are varying views as to if and how this information should be shared.

6.1.5 Office of the Oneida County District Attorney (OCDA)

An ARIES participant with ODCA has singularly expressed an interest in sharing court appearance and disposition information. However, whether OCDA at large shares this interest remains to be seen. This information could greatly enhance the use of ARIES since law enforcement would have ready access to a person's whereabouts in order to execute warrants (ironically, criminals actually make an effort to appear in court for minor offenses in order to keep officers at bay). This appearance and disposition information can technically be leveraged by ARIES since it is stored in MS Access.

6.2 Non-Departmental

Oneida County's Shared Mug Shot System will be accessible to each department within the next few months. UPD already has access to this system. This system offers potential ARIES police departments access to all mug shots and pedigree information obtained from bookings and criminals housed in the CNY region. This system is primarily used for purposes of photo-line-ups. Since the pedigree information accompanies each photo, this database seemed like a desirable source for ARIES exploitation. The data is replicated on a daily basis between various sites.

Unfortunately, the database for the Shared Mug Shot System is a proprietary and would not be easily exploited by a tool such as ARIES. However, there has been a mention of plans to port this system to a more state-of-the-art environment, which could render it exploitable by ARIES. Barring this migration effort, CSCC could certainly replicate the data into a centralized server with relative ease thus bringing the regional-wide photo and pedigree information mainstream into ARIES. Actually, this data, once replicated, could be imported into the CSCC Shared Multimedia Archival and Retrieval Tool (SMART) where images and related information could be produced, edited, enhanced, and browsed at a regional level (Section 8 of this document presents an overview on SMART).

CSCC identified and researched several types of public record data that would enhance the investigative process. While these sources seem quite basic in terms of the information they offer, electronic access to these sources would greatly expedite investigations by eliminating the number of phone calls and inquiries an analyst would need to make. A common theme from virtually every investigator we spoke with was that regional connectivity of criminal records would indeed be valuable – but marrying this data with an online cross-referencing capability for public information would be invaluable.

1. *Residential Information*
   The local phone provider for CNY is Bell Atlantic who, for a nominal biannual fee ($124.95) offers a nationwide directory on CD-ROM that contains information on residential names, addresses, and phone numbers. This data could very easily be uploaded into a centralized database server for electronic cross referencing purposes.

2. *Property Ownership*
   The Oneida County Department of Finance houses records on real estate taxes for Oneida County. This office has offered to provide the data on CD-ROM to law enforcement agencies upon request. This could be done on a quarterly basis. This information would contain privately owned property addresses with the names of property owners. OCDTF would benefit from this online data since, for example, much drug activity reoccurs in properties where Landlords knowingly rent to criminals (specifically those involved with drugs). According to OCDTF, there are Landlords that offer these criminals a seemingly safe haven in return for cash rent. If OCDTF suspected drug activity at a certain dwelling, then they could cross reference the address with the property ownership database to determine if this property is owned by a Landlord with an inclination to rent to criminals, thus strengthening their suspicions.

3. *Businesses*
   New York's Department of State Division of Licensing Services holds records of licensed and certified professionals in New York state. This office told CSCC during our investigation into locating public record resources that they would make every effort to accommodate law enforcement with any of their needs. Currently they do not have an electronic dissemination capability for their licensing records, but are in early planning stages of providing such a capability. This information, once captured for ARIES inclusion, could provide valuable leads to law enforcement, especially since CNY has a large number of businesses that are run in private residences. Information that this department could share with law enforcement would include name, license date, number, address, city/town, and state. This department will not share private information such as DOB or SSN.

4. *Recreational Licenses*
   It was determined during our study that recreational licenses such as hunting and fishing could be captured electronically for ARIES. This information could be acquired on a biannual basis for batch upload into a centralized ARIES database server with relative ease. Since CNY contains a large number of residents who hunt and fish as well as tourists who visit for the same recreation, this information would be abundant. Moreover, it is the general consensus of our study participants that career criminals who hunt and/or fish generally apply for and maintain said licenses in order to avert unwanted attention from law enforcement.

6.3 Audit Trail Data

Checks and balances for need to know accountability with regard to ARIES will be implemented in the form of audit trail logs. This requirement is included in this section because it is a foremost data requirement that takes the form of a searchable data repository in and of itself. ARIES will provide a query interface to search a department's audit trail data for authorized persons. The audit trail data will be automatically generated by ARIES and stored in an ODBC database (such as MS SQL, Oracle, Sybase, etc.) on each ARIES server. The Privacy and Security Requirements section of this document presents recommendations on structuring audit trail data to best meet security requirements.

Figure 6.1 Summary of Shared Data Matrix

Incidents*	Incident ID/Description	*Associates ID*	*Victim ID/Description*	*Missing Person ID/Description*	*Suspect ID/Description*	*Arrested Person ID/Description*	*Property Info*	Admin Info
Arrests*	Arrest ID/Description	ID Numbers	Defendant ID/Description	Charge ID/Description	Associates ID	Admin Info		
Warrants*	Warrant ID	Suspect ID/Description	Court Info	ID Numbers	Warrant Control History			
Accidents*	Accident ID/Description	Driver ID	Vehicle ID	Admin Info				
Traffic Tickets*	Violation ID/Description	Defendant ID	Vehicle ID	Appearance Info				
Domestic Incidents*	Incident ID/Description	*Complainant ID/Description*	*Suspect ID/Description*	*Allegations*	*Reasonable Cause*	*Weapons Info*	Admin Info	
Mug Shots/Pedigree	Person ID	Person Description	Person Photo	Finger Print ID	ID Numbers			
Court	Appearances	Dispositions						
Residential	Residential Name	Residential Address	Residential Phone Number					
Property	Owner Name	Owner Address	Property Address					
Business	Licensed Name/Address	License Type/Number	Certified Name/Address	Certified Type/Number				
Recreational	Name	Address	License Type/Number					

NOTE: Those items in Italics indicate information which can be searched but not displayed in query results. If these items produce a hit, then only administrative and header information (such as DRN, Agency, Offense Date/Location, etc.) will be returned.

* Indicates that this document contains a Figure outlining detailed fielded information.

Figure 6.2 Incidents

Incident ID/Description	***Associates ID***	***Victim ID/Description***	***Missing Person ID/Description***	***Suspect ID/Description***	***Arrested Person ID/Description***	***Property Info***	**Admin Info**
Agency	*Person Type*	*DOB*	*Type/No.*	*Type/No.*	*Type/No.*	*Victim or*	Inquiries
Division/Precinct	*Name*	*Age*	*Name*	*Name*	*Name*	*Suspect No.*	NYSPIN
Case No.	*DOB*	*Sex*	*Alias/Nickname*	*Alias/Nickname*	*Alias/Nickname*	*Property Status*	Message No.
Incident No.	*Address*	*Race*	*Maiden Name*	*Maiden Name*	*Maiden Name*	*Property Type*	Officer ID No.
Incident Date	*Telephone*	*Ethnicity*	*Condition*	*Condition*	*Condition*	*Quantity*	Status
Incident Time		*Handicaps*	*Address*	*Address*	*Address*	*Make/Drug Type*	Status Date
Incident Type		*Residence Status*	*Phone*	*Phone*	*Phone*	*Model*	Notified
Business Name			*SSN*	*SSN*	*SSN*	*Serial No.*	
Weapons			*DOB*	*DOB*	*DOB*	*Description*	
Incident Address			*Age*	*Age*	*Age*	*Value*	
Offense Name			*Sex*	*Sex*	*Sex*	*Vehicle*	
			Race	*Race*	*Race*	*Status*	
			Ethnicity	*Ethnicity*	*Ethnicity*	*License No.*	
			Skin	*Skin*	*Skin*	*State*	
			Occupation	*Occupation*	*Occupation*	*Exp. Yr.*	
			Height	*Height*	*Height*	*Plate Type*	
			Weight	*Weight*	*Weight*	*Value*	
			Hair	*Hair*	*Hair*	*Vehicle Yr.*	
			Eyes	*Eyes*	*Eyes*	*Make*	
			Glasses	*Glasses*	*Glasses*	*Model*	
			Build	*Build*	*Build*	*Style*	
			Employer	*Employer*	*Employer*	*VIN.*	
			School	*School*	*School*	*Color*	
			Address	*Address*	*Address*	*Towed By:*	
			Scares/Marks	*Scares/Marks*	*Scares/Marks*	*Towed To:*	
						Vehicle Notes	

NOTE: Those items in Italics indicate information which can be searched but not displayed in query results. If these items produce a hit, then only administrative and header information (such as DRN, Agency, Offense Date/Location, etc.) will be returned.

Figure 6.3 Arrests

Arrest ID/Description	ID Numbers	Defendant ID/Description	Charge ID/Description	Associates ID
Arresting Officer	NYSID No.	Name	Incident No.	Type
Arresting Officer ID No.	FBI No.	Alias/Nickname	Arrestee Status	Name
Assisting Officer	Arrest No.	Maiden Name	Bail Amount	Address
Assisting Officer ID No.	Case No.	Phone	Bondsman	Telephone
Arrest Date	Ref. No.	Address	Photo No.	
Arrest Time	Agency	Residence Status	Arrest Type	
Arrest Location	Division/Precinct	Place of Birth	Warrant No.	
Juvenile		DOB	Arrest FOA	
Condition		Age	Other Agency	
Weapons		Sex	FP Taken	
Co-defendant Arrest No.		Race	Offense Location	
Miranda		Ethnicity	Offense Date	
Miranda By		Skin	No. Offenders	
Miranda Date		Height	No. Victims	
Miranda Time		Weight	Return Court	
Statements		Hair	Return Judge	
Status		Eyes	Return Date	
Search Warrant		Glasses	Return Time	
ID Procedure		Build	Defendant/ Case TOT Agency	
Arraignment Court		Marital Status	Officer Name	
Arraignment Judge		Citizenship	Officer ID No.	
Date		SSN	Time	
Time		Education	Date	
Property		Religion	Article & Section	
Evidence		Occupation	Offense Name	
Processed By		Employed	NCIC Code	
Disposition		Scars/Marks	Victim Age	
			Victim Sex	
			Victim Handicap	
			Assoc. No.	
			Type	

Figure 6.4 Warrants

Warrant ID	Suspect ID/Description	Court Info	ID Numbers	Warrant Control History
Complaint/ Incident No.	DOB	Date Issued	Local PD No.	Initial Contacts
Date Received	Sex	Judge	NYSID No.	Patrol History
Name	Race	Court	FBI No.	Detective History
AKA	Height	ROR	SSN	Date
Address	Weight	Bail		Time
Phone	Hair	Bail Amount		Location
Employment Phone	Skin Tone	Warrant Type		Results
Associates/ Contacts	Eyes			ID No.
Known to Frequent	Glasses			
Complainant/ Victim Address	Moustache			
Complainant/ Victim Phone	Beard			
	Scars/Marks			
	Special Warnings			
	Narrative			

Figure 6.5 Accidents

Accident ID/Description	Driver ID	Vehicle ID	Admin Info
Date Time No. of Vehicles No. Injured No. Killed Non-Highway Left Scene Photo Availability Accident Location Ticket/Arrest No. Violation Sections	Driver 1 Driver Name Address DOB Sex Unlicensed No. of Occup. License State	Vehicle 1 Plate Number State Registered Vehicle Year Vehicle Make Vehicle Type Ins. Code Vehicle Damage Info Towed By Towed To Vehicle 2 Plate Number State Registered Vehicle Year Vehicle Make Vehicle Type Ins. Code Vehicle Damage Info Towed By Towed To	Officer Rank Officer Name Badge/ID No. Department Precinct Station Reviewing Officer Date Received Time Received

Figure 6.6 Traffic Tickets

Violation ID/Description	Defendant ID	Vehicle ID	Appearance Info
Offense Date Offense Time Offense Location Violation Description MPH MPH Zone Offense Type NCIC ORI Division/Troop PCT Zone Sector Officer Name Badge/Shield	Name Address Motorist ID No. License State License Class Expiration Date Sex DOB	Plate No. Registration State Registration Type Color Vehicle Type Vehicle Year Vehicle Make	Location Address Date Time

Figure 6.7 Domestic Incidents

Incident ID/Description	***Complainant ID/Description***	***Suspect ID/Description***	***Reasonable Cause***	***Weapons Info***	**Admin Info**
Incident Report No. Date Time Location Relationship to Complainant Suspect Present Incident Involved Description Protection Order Violated Issuing Court Registry Check Exp. Date Complaint No. Weapons/Threats Injuries Hospitalized Hospital Photos Taken Arrest Made Resisting Charges Family Present Name DOB Relation Suspect Actions	*Name* *Address* *DOB* *Age* *Phone* *Race* *Ethnicity*	*Name* *Address* *DOB* *Age* *Phone* *Race* *Ethnicity*	*Child Neglect* *Referrals* *Referral Type* *Person Notified* *Date* *Time* *Notified By*	*Guns Present* *Guns Seized* *Gun Permits* *Permit No.* *Permit Seized* *Issuing County* *Name*	Agency ORI NY Officer ID No.

NOTE: Those items in Italics indicate information which can be searched but not displayed in query results. If these items produce a hit, then only administrative and header information (such as DRN, Agency, Offense Date/Location, etc.) will be returned.

Figure 6.8 Summary of Data Contribution and Sharing by Agency

	Rome PD	Utica PD	New Hartford PD	Oneida County Drug Task Force	Utica Arson Strike Force	Oneida County Sexual Abuse Task Force	Oneida County District Attorney
Incidents	■●	■●	■●	●	●	●	
Arrests	■●	■●	■●	●	●	●	●
Warrants	■●	■●	■●	●	●	●	●
Accidents	■●	■●	■●	●	●	●	
Traffic Tickets	●	■●	●	●	●	●	
Domestic Incidents	■●	■●	■●	●	●	●	
Mug Shots/Pedigree	■●	■●	■●	●	●	●	●
Court Appearances/Dispositions	●	●	●	●	●	●	■●

NOTE: Those items in Italics indicate information which can be searched but not displayed in query results. If these items produce a hit, then only administrative and header information (such as DRN, Agency, Offense Date/Location, etc.) will be returned.

* Indicates that this document contains a Figure outlining detailed fielded information.

■.....Agency produces information and is willing to contribute to ARIES for sharing.
●.....Agency will have access to shared data through ARIES.

7. PRIVACY AND SECURITY REQUIREMENTS

7.1 Juvenile Aid

The Family Court Act for New York State requires that no juvenile criminal information be released outside the immediate jurisdiction of the Family Court presiding over the case and the certified law enforcement juvenile aid specialist case worker. Each ARIES police department staffs certified juvenile aid specialists who work almost exclusively with juvenile aid offenders (individuals under the age of 16). Juvenile offender information, by law, cannot be released (to law enforcement or criminal courts) even after the person reaches adult status (except under very rare circumstances presided over by a higher court).

Often times, a 16 or 17 year old person who has been charged with a criminal offense can subsequently be deemed by a court disposition as a "youthful offender". This ruling would then require the arresting police agency to expunge the conviction from their records. Failure for the department to do so is unlawful.

Therefore, because each department has an autonomous unit to handle juvenile aid information, and due to the fact that none of this information is legally releasable) to law enforcement or court officials (other than by subpoena), the recommendation is to exclude this data entirely from a regional information sharing system.

7.2 Sealed Cases

When a case is brought to trial, a variety of dispositions may ensue. A person may be found guilty, not guilty, the case may be dismissed (due to insufficient evidence or the discovery of improper criminal proceedings), or the conviction may be reduced to a lesser offense. Some of these dispositions may cause a case to be "sealed" by the court. For example, if a case is dismissed, then the entire paper trail back to the original incident report and arrest report must be expunged from law enforcement and court document management systems. If the records are stored online, then all references to and accessibility to said documents must be removed. If the records are stored in physical file cabinets, then the documents must be placed in a sealed envelope (which will exhibit signs of tampering to protect the contents). Therefore, ARIES will effectively ignore any sealed case information. The RMSs that have been identified for ARIES inclusion sufficiently handle the electronic sealing of data by inserting flags in specified fields. ARIES will preclude these documents during all primary searches of criminal record data, thus eliminating them entirely from posterior retrieval, sort, and display functions.

7.3 Sex Offender Registry

Sex offenders who have been arrested and convicted in the CNY region will have criminal record data available for sharing with ARIES. And with the enactment of the New York State Sex Offender Registration Act (SORA), ARIES police departments must provide a mechanism to register and maintain information on qualifying sex offenders residing in their jurisdiction. These qualifications include (but are not limited to) offenders who have been convicted of certain qualifying sex related crimes, habitual

sex offenders, those individuals under parole for sex related crimes, and those who have been incarcerated for sex crimes.

Each department's sex offender registry will contain information for these offenders such as offender name, address, place of employment, and planned travel dates and destinations in and out of the jurisdiction where they are registered. The levels for these offenders are tertiary, with level 1 being low-risk offenders, to level 3 being high-risk and generally violent and/or repeat offenders. This information is maintained by each police department for purposes of updating the New York State Division of Criminal Justice Services (DCJS) Subdirectory of Sex Offenders (which SORA requires of DCJS). Actually, New York State has made a provision for public access to names of level 3 sexual predators whose offenses occurred after January 1, 1996. This fact notwithstanding, it is the general feeling of the ARIES study participants that sex offender registry databases not be made available for exploitation by ARIES. This is due primarily to the fact that there are current court proceedings underway to redefine the laws governing the dissemination of sex offender information. Still, ARIES will have access to all sex offender information where the crimes occurred within the participating CNY region. The only information that this exclusion would compromise is that of offenders who have been convicted of sex offenses outside the CNY region. And this information can be attained by CNY law enforcement through state-wide or federal data sources such as the New York Statewide Police Information Network (NYSPIN) or the National Crime Information Center (NCIC).

7.4 Warrants

Warrant information, to include issued and recalled warrants, will be stored in each of the RMSs that will be searchable at a regional level with ARIES. Sharing warrant information at a regional level will undoubtedly enhance law enforcement efforts since it can justify on the spot arrests or search and seizure. However, warrants do pose an interesting dilemma. And this dilemma is two fold. Consider the following scenarios:

1. An officer pulls over a registered car owner for speeding in jurisdiction A, and using the ARIES tool discovers that the person has an active warrant in jurisdiction B. If the officer relies on the ARIES information as the final authoritative word on the status of that warrant, then the arrest will probably be made. However, suppose that this warrant has been recalled in jurisdiction B within the previous few hours, and that this information is not immediately updated in that department's database. The impact of this scenario is that the officer just made a false arrest, and this could set the department up for future liable action. Unfortunately, even though police department B was indeed responsible for not having up to date warrant information, police department A is actually liable for the faulty arrest action.
2. Warrants (even for minor infractions and offenses) are made available at a regional level. With the introduction of the ARIES tool, if officers are made privy to active warrant information, then they are legally bound to execute these warrants by making arrests. This has both a positive and negative effect. The positive impact is that more valid arrests will be made, both for minor and major offenses. The negative impact (according to some practitioners we interviewed) is that officers may be so busy executing obligatory warrant arrests for minor

offenses that this will tie up resources that might otherwise be needed for more serious matters. However, understanding the dutiful nature of law enforcement, the positive aspects of sharing warrant information at a regional level preponderates any impact it may have on existing CONOPS.

7.4 Victim Information

Victim information is considered private and confidential to law enforcement. So it is not surprising that information will not be sharable at a regional level. This information does reside on Incident Reports and Domestic Incident Reports; however, as specified in the Shared Data Requirements section of this document, only header and administrative data from these reports will be shared. Likewise, OCSATF victim information will not be exposed to ARIES. The hesitancy to share victim information was commonly heard from practitioners during the ARIES study; therefore, no victim information will be exposed for regional sharing.

7.5 Audit Data

Several practitioners expressed concern that audit data such as user names with requested queries could compromise investigations. For example, if an OCDTF investigator requests ARIES to find all regional information pertaining to drug related crimes for a named individual, then audit log data could reveal the nature of the investigation. And many investigations are not even shared within a department, much less with another department.

Therefore, it is our recommendation that the audit log data be physically separated into two tables. The audit log data would also have dual access for accountability purposes. The first table would contain audit log header information such as name, date time stamp, and a unique key. The second table would contain audit log body information such as databases and tables accessed, query strings, and a unique key. This unique key would link the two tables; however, they will never be read in tandem. The header information would be accessible by an appointed computer administrative person while the body information would be accessible by a managerial person such as a police Chief, Captain, or Lieutenant.

It is also recommended that there be a built in capability to archive, restores, and expunge audit logs.

7.6 Information Security

ARIES will have robust system security build in every several different layers. The following security mechanisms have been presented and explained to the study participants (including technical representatives) and prioritized with their respective relevance to the ARIES Test-Bed.

1. Authentication
   Authentication security will provide assurance of identity by providing a means of confirming the correctness of an individual's identity. The server will authenticate to the client, by demonstrating possession of a particular private key. Username and password are just two examples of information that could constitute this private key.

2. Secured Socket Layer (SSL)

   SSL adds communications protection to a range of web-based applications protocols and provides for varied level encryption. It can be used to protect the communication of any applications protocol that operates over TCP, such as HTTP. Our recommendation is to use 128-bit SSL encryption.

3. Lightweight Directory Access Protocol (LDAP)

   LDAP is a protocol which is compatible with the X.500 directory server model. This will enable ARIES to keep tight and detailed control of user key attributes (such as name and email address) as well as database and table access rights. LDAP will store this data in a directory information tree which can be searched at logon as well as during application runtime (for assessing access privileges).

4. Application Level Security

   Application level security can leverage the directory server when users attempt to connect to various databases and tables. This is one example of application level security. Since higher level security mechanisms will be implemented, application level security will provide an additional data integrity precaution.

5. Certification

   A certificate is a collection of information to which a digital signature has been affixed by some authority who is recognized and trusted by some community of certificate users. A public key certificate is digitally signed by a person or entity (certification authority) that has the power to confirm or deny the identity of the holder of a corresponding private key. Public key cryptography and digital signature technology are widely used in electronic commerce today. It is our recommendation that this technology be implemented after the ARIES Test-Bed since during this initial period, there will only be a few, manageable number of ARIES users. However, should the Government deem it necessary to implement this technology up front, there is no problem, since the military system that NIJ planned to leverage for the ARIES proof of concept has a robust, operational digital certificate capability.

6. Non-repudiation

   Non-repudiation services protect against one party to a transaction or communication activity later falsely denying that the transaction or activity occurred. For the ARIES Test-Bed, non-repudiation security services probably won't be implemented since this technology is a bit overkill for a pilot system.

8. APPLICABILITY

Various solutions were proposed to the CNY practitioners during a final Roundtable meeting where they were prioritized by level of interest. These solutions are in no way to be misconstrued as a design approach; rather, they are provided for the purpose of gauging a general scenario of how the CNY practitioner community sees ARIES as a value added tool to expedite and enhance investigations and police procedures. The features that were discussed are outlined below from highest priority.

1. Ad-Hoc Criminal Data Search and Retrieval

   ARIES will provide a mechanism to search against regional RMS data repositories for purposes of finding related criminal information that could help prompt a new or expedite an existing investigation. The ad-hoc query GUI will be simple, yet powerful, by providing several different fields upon which to search such as name, alias, DOB, addresses, employment, or modus operandi. Users may select query fields with exact or wild card values and sort these fields for searching. Users may also select display fields and sort these fields for viewing. The ad-hoc query capability will initiate searches, sort the results and return records promptly while additional information is being buffered for sending to the client. These queries can be saved by name where they can be recalled at a later date. Users may also define a default ad-hoc query that appears each time the application is selected from the ARIES desktop.

   Often times, an investigator may not know about an accusatory's activity (criminal or otherwise) outside of his jurisdiction. Because of this, the investigator may not have the foreknowledge of which department to inquire and/or which inquiry to make.

   For example, suppose a suspect has committed a crime in jurisdiction A, and immediately afterwards received a parking ticket in neighboring jurisdiction B. Were the investigator to inquire about the suspect's criminal activity in jurisdiction B, he might not receive any relevant information (unless he knew to inquire specifically about parking tickets rather than criminal activity). However, with the ARIES ad-hoc query capability, the investigator would conduct a single search spanning the surrounding regional area data pool for all information pertaining to the known suspect. He would quickly receive information about the parking ticket, which could provide a valuable lead as to the suspect's whereabouts during the commission of the crime as well as perhaps providing enough evidence to justify obtaining a search warrant.

2. Canned Criminal Data Search and Retrieval

   Canned query capabilities will be provided in order to allow users "swift" access to specifically sought after information, such as person information, vehicle information, or weapons/property information. Figures 8.1, 8.2, and 8.3 illustrate simple examples of canned query screens.

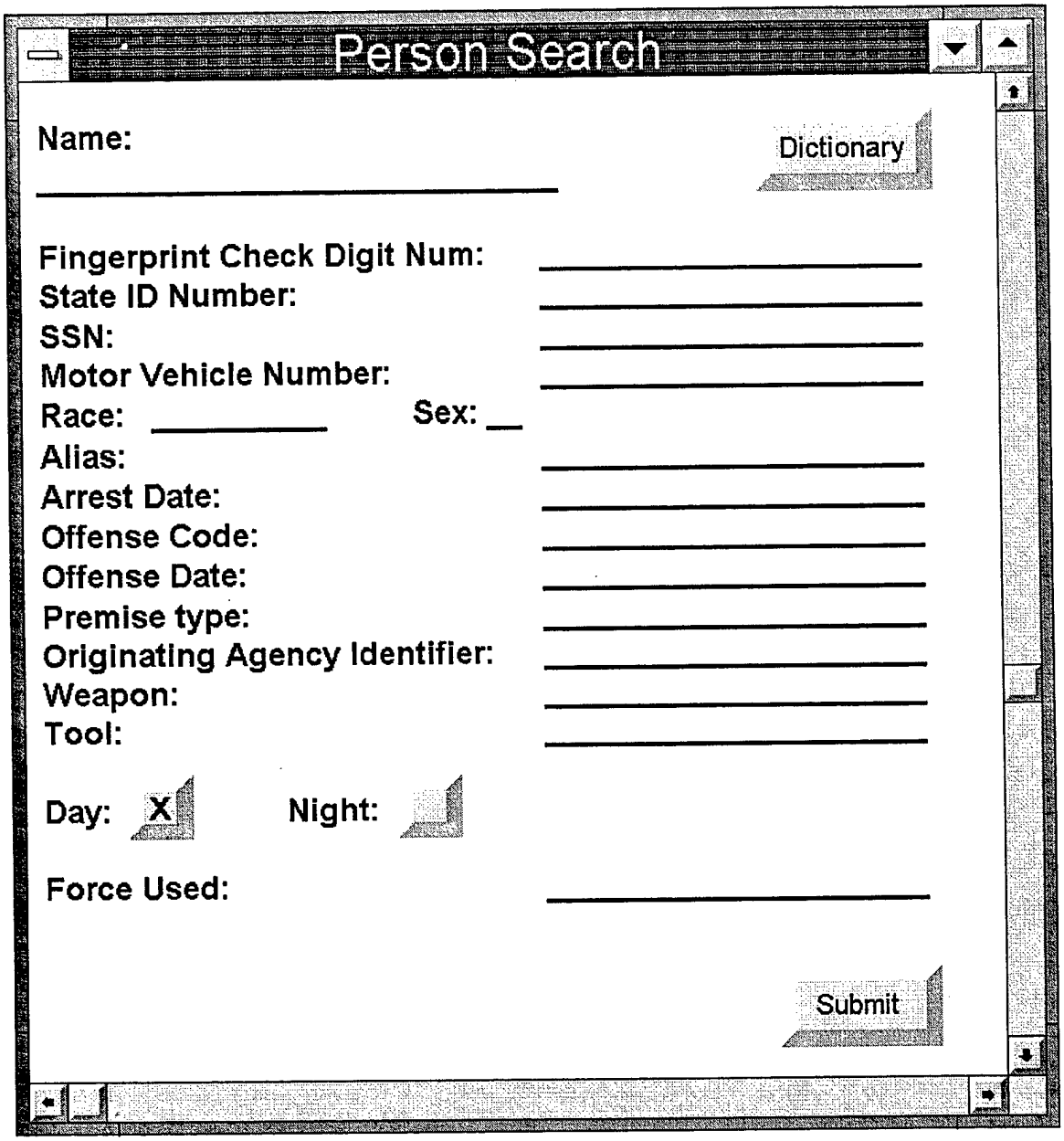

Person Search
Name:
Dictionary
Fingerprint Check Digit Num:
State ID Number:
SSN:
Motor Vehicle Number:
Race:
Sex:
Alias:
Arrest Date:
Offense Code:
Offense Date:
Premise type:
Originating Agency Identifier:
Weapon:
Tool:
Day:
X
Night:
Force Used:
Submit

Figure 8.1

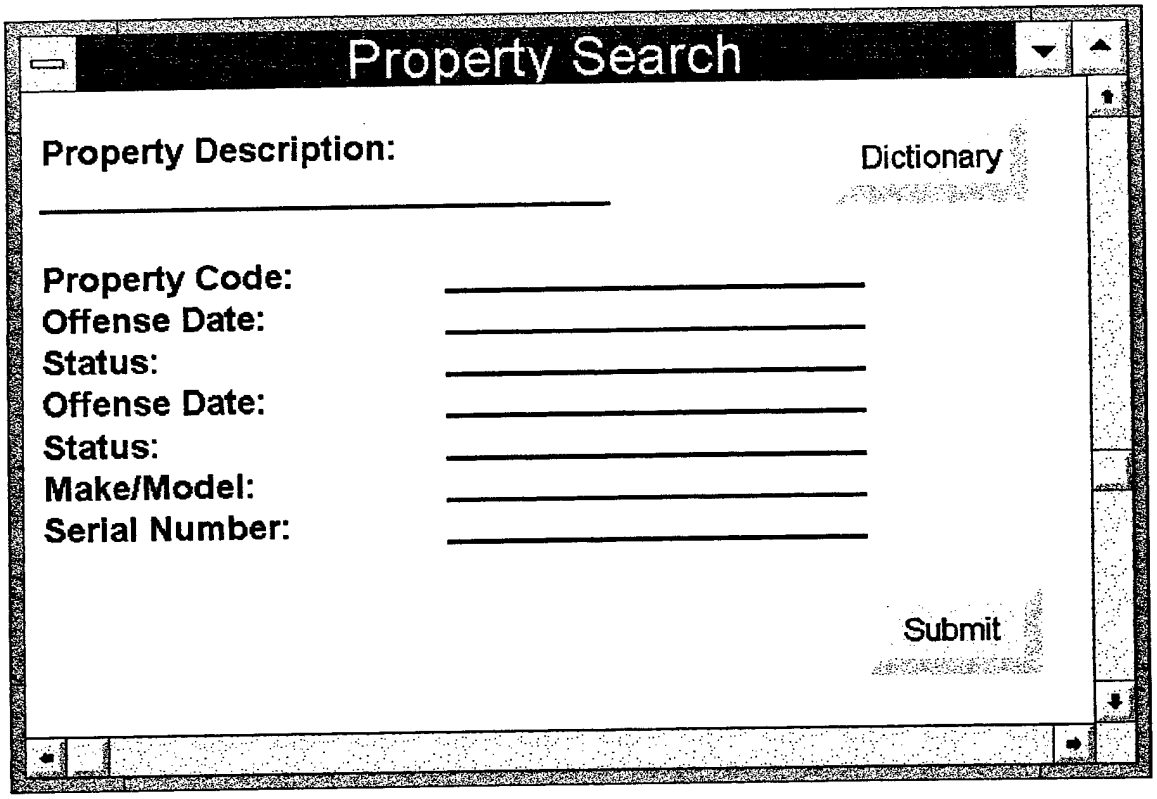


Figure 8.2

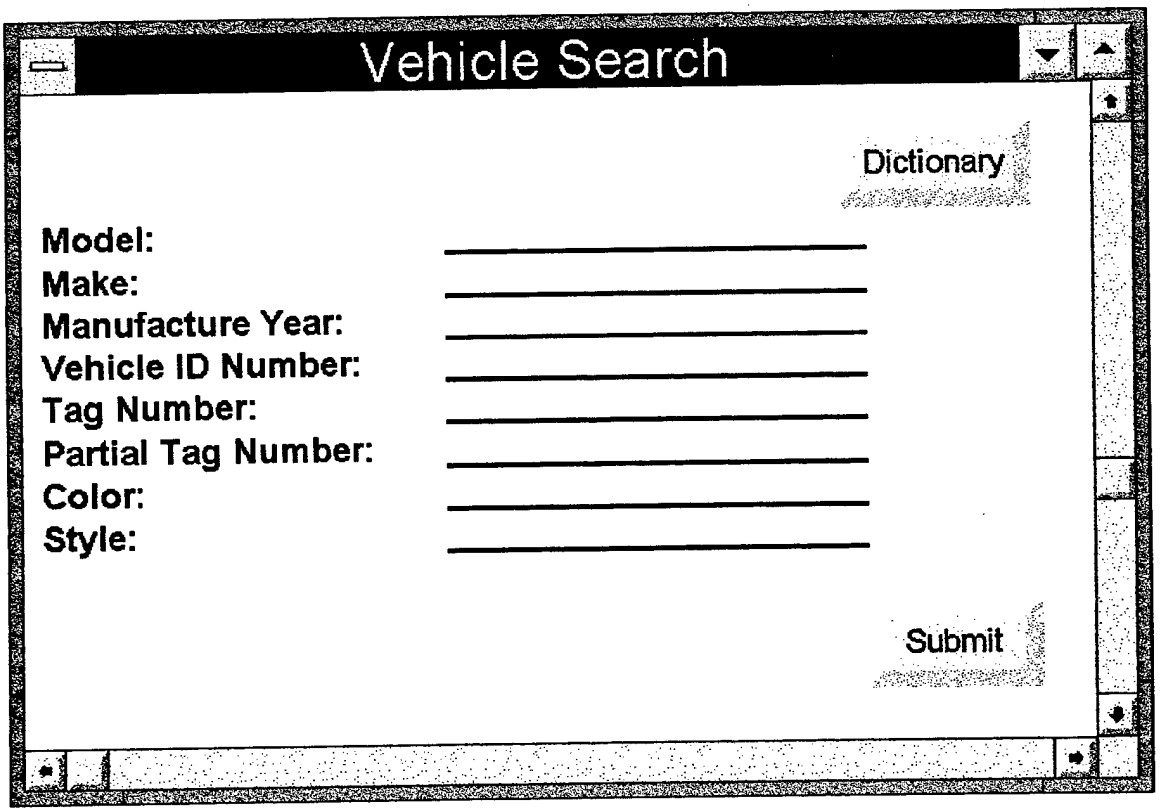


Figure 8.3

3. Filtered Criminal Data Search and Retrieval

   A filtered query capability will allow users to further refine existing queries by placing new conditions on top of already executed queries.

4. Public Record Data Search and Retrieval

   This study has identified a number of public record data sources that can be imported into a customized ARIES database. ARIES will provide utility programs to import the data on a periodic basis (obtained on external media such as compact disk). ARIES will also provide (through the ad-hoc interface) the capability to cross-reference items in these data repositories to further enhance the assimilation of investigative data.

5. Maintain, Search, Retrieve, Archive, Restore, and Expunge Audit Trail Data

   ARIES will provide background server programs which will constantly create and maintain audit trail database information so agencies can assess how their RMS data is being accessed. ARIES will provide a GUI for administrators to access and review this data. ARIES will also provide custom GUI applications to archive, restore, and expunge audit trail data.

   The audit trail data will be physically separated into two tables thus providing dual access for preserving investigative integrity. The first table would contain audit log header information such as name, date time stamp, and a unique key. The second table would contain audit log body information such as databases and tables accessed, query strings, and a unique key. This unique key would link the two tables; however, they will never be read in tandem. The header information would be accessible by an appointed computer administrative person while the body information would be accessible by a managerial person such as a police Chief, Captain, or Lieutenant.

6. Automatic Event Notification

   ARIES will provide the capability of early warning of significant events by implementing a background search capability. This feature is being referred to as an Event Trap. Qualified users may enter background searches which can then multicast notification warnings to all ARIES users who are currently logged on. An example of an Event Trap may include notifying departments of police raids just minutes prior to the actual event. This may of benefit since drug raids are often conducted by plain clothed officers, and the law enforcement community may want to be aware of such events immediately prior so that no plain clothed officers are mistaken for criminals. Another example of an event trap instance may include notifying law enforcement users of high level criminal warrants that have just been issued in the region (such as a warrant for a level 3 sex offender).

7. Regional Mail Server

   Since ARIES will be a closed, private network, a regional mail server would allow law enforcement personnel to share information that might not otherwise be safe

to send through public email. These messages may include attachments such as criminal photos, fingerprints, and other criminal information.

8. Online Chat

   For the same reasons that a regional mail server would be helpful, a private online chat capability would be of benefit to ARIES users. Here, law enforcement could converse with others within and across departments on critical and timely issues. A perfect example where this capability would have helped, according to the practitioners we interviewed, would have been the Woodstock '99 event. Officers from various CNY police departments had to communicate logistical information such as traffic patterns, incidents, reroutes, reinforcement, and other activity while managing the movement and activity of tens of thousands of people in and around the CNY cities and towns.

9. Shared Multimedia Archive and Retrieval Tool (SMART)

   ARIES could provide a region-wide capability for law enforcement to share multimedia information. This information could include photos of criminals, fingerprints, and crime scenes, fielded information such as pedigree data, and even voice and video. This capability has already been developed for the Government and could be leveraged with minimal customization to adapt to law enforcement.

10. Crime Mapping

    ARIES could leverage existing technology to provide networked crime mapping features for CNY. These features could include plotting burglaries around certain areas over time, drug related transactions and movement over time, as well as sexual assaults or criminal activity within a particular region.

11. High-End Criminal Association and Profile Clustering Tools

    ARIES could provide high-end statistical modeling tools to graphically depict criminal associations. These tools could also forecast trends based on historical and algorithmically derived data.

9. QUALITY ASSURANCE and MEASURES for SUCCESS

ARIES should include some tools for gauging usability requirements and success measures. These tools will be run as background processes on the servers to constantly monitor user activity. They will be statistical in nature by aggregating the following:

1. logon requests
2. database access
3. table access
4. field or entity level access, and
5. query execution time.

This information will help the ARIES developers further enhance and optimize ARIES. For example, this feature may show that a particular field is accessed frequently, thereby prompting ARIES engineers to perhaps add a primary index to field.

Measuring success will be difficult with standard statistical tools such as assessing if there is a greater number of arrests or a shorter time frame between incidents and arrests. Often times, these numbers may indicate that a system is responsible for increased arrest activity, when many other factors may actually contribute to said increase such as change in demographics. Perhaps the single most important factor weighing the success of ARIES (as is with most automated systems) is the propensity for usage, which these tools can provide.

10. NETWORK, HARDWARE, and SOFTWARE REQUIREMENTS

10.1 Network

As mentioned earlier in this document, the initial scope for ARIES will target the investigative community. Therefore, the first ARIES implementation need not address wireless communications (for patrol car accessibility). For a Test-Bed or Pilot ARIES network, probably the most cost effective means of connecting the network would be high speed modems. Bell Atlantic does offer high speed phone lines in CNY. Should the scope of ARIES broaden to include mobile access, then a higher end solution such as a packet-switched CDPD network may be required. Unfortunately, there is currently no CDPD availability in CNY.

There may be an existing regional information network structure in place by the time the ARIES design and implementation work begins. The Central New York Law Enforcement Network is one possible infrastructure. However, it is currently in the early implementation phase, and is now used primarily for one way dial-up capability to replicate Shared Mug Shot data between various sites.

Outsourcing ARIES networking operations to a trustworthy ISP is not recommended for the initial ARIES Test-Bed. The primary reason for this is that nearly every department we spoke with felt very uncomfortable with this approach.

10.2 Hardware

The Test-Bed will probably require one or two workstations at each of the police departments, and one workstation at each of the specialized Forces and OCDA. This comes to approximately 10 workstations with high speed modems. High quality high speed modems can be purchased for less than $150 a piece; therefore, the up front cost for modems would be under a reasonable $1500. Bell Atlantic has not yet provided quotes for the maintenance plans for the high speed lines, but since ARIES will require a persistent link, this solution won't incur huge costs, and is a simple, virtually maintenance free environment to prove the ARIES concept.

There will be a sufficient number of workstations to leverage for the ARIES Test-Bed. This is because ARIES requires no up front client software other than a browser (such as Internet Explorer or Netscape), so existing workstations may be leveraged rather than new ones procured.

Since each of the police departments will have RMSs, our recommendation is to have a server available at each of these locations. This will be a ARIES database/Java applications server which will serve up local workstation applications across the network and provide a bridge to existing RMS databases. This server will contain the audit log database. It may not be necessary to have this machine be a dedicated server. Existing departmental servers may possibly be leveraged since the ARIES server resource requirements are minimal. Actually, if there are not servers available at the time of ARIES implementation, then a simple Pentium II would suffice for an ARIES

server. These can be purchased for less than $1500, and since there will only be three server sites, the server hardware costs would come in under $4500. It is currently too early to determine what hardware server environment will be available to leverage at any of the police departments.

Should the ARIES Test-Bed include public record information, this would require the implementation of some specialized (but very simply structured) databases. If this public information is integrated into the regional information sharing network, then it is our recommendation to go ahead and procure a dedicated database server for this data. This server could also be used to maintain audit logs and serve up applications. A Pentium II architecture should suffice for this data.

10.3 Software

Each of the three ARIES servers will need to have access to SQL databases. But many of these databases will be in different forms, such as MS SQL, MS Access, and Oracle. To provide client application access to different SQL servers, a client would have to load two JDBC library interface versions. JDBC handler classes automatically register themselves, so there is no logical problem with multiple JDBC drivers, but there is a performance hit. Middleware products like dbAnywhere solve this problem. The client loads a single version of the JDBC library that either speaks several proprietary protocols, or that talks to a server which in turn talks to the databases in their native proprietary protocols. Middleware products can also help with buffering output from the server. Therefore, it is our recommendation that dbAnywhere be procured for the ARIES servers.

These servers will also need to have Java 2.X software (servlets) installed on them as well as web server (http access), directory server (database accessibility management and user information), and certificate server (digital certificates) software. Either Netscape or Microsoft products will satisfy these requirements.

Finally, if MS SQL does not already reside on an ARIES server, then it will need to be purchased. This is to satisfy the requirement for maintaining structured audit trail logs that can be searched with the ARIES interface.

11. HIGH LEVEL SOLUTIONS REQUIREMENTS MATRIX

This solution requirements matrix should not be misconstrued as comprehensive set of proposed solutions. Rather, it is here to present the level of effort required for already identified solutions (as discussed with CNY practitioners) with respect to leveraging existing technology.

The response codes used in the solution Requirements Matrix are defined as follows:

Response Codes

Y Specification exists as a standard feature or function and can be implemented by leveraging existing technology with little to no customization.

C More extensive customization of existing technology can meet this requirement.

D Specification can be met, but new applications development is required.

W Agency or department work is required to help meet this requirement.

X Alternative solution is recommended.

N Developer cannot meet the requirement.

Requirements Matrix

Feature	Requirement	Code	Comments
Data Model	The data will establish region wide access to CNY agency RMS data.	Y	
	ARIES will interface with existing RMSs in a non-intrusive fashion.	Y	
	ARIES will be scalable to accommodate future inclusion of new RMSs.	Y	
	ARIES will create and maintain public record data repositories to enhance RMS search capabilities.	Y	
	ARIES will interface only with ODBC compliant database architectures.	Y	
	Any data that may be shared with one agency, will be shared with all.	Y	
Data Input/ Output	ARIES network must include the capability to validate the data contents of each of the above record types to insure inter-agency compliance.	D	Agencies will maintain RMS data compliancy and integrity.

Feature	Requirement	Code	Comments
	ARIES will share and exploit Arrest information.	Y Y	
	ARIES will share and exploit Warrant information.	Y	
	ARIES will share and exploit Accident information.	Y	
	ARIES will share and exploit Traffic information.	Y	
	ARIES will share Incident-based information for searches, but return only administrative report information such as DRN, Agency, Incident Date, Location, and Officer.	C	
	ARIES will share and exploit residential name and location data.	C	
	ARIES will share and exploit business name and location data.	C	
	ARIES will share and exploit owned property name and location data.	C	
	ARIES will share and exploit recreational license data.	C	
	ARIES will share and exploit mug shot and pedigree information.	Y	Depending on availability of ARIES/CNYLEN network communications.
	ARIES will share and exploit court disposition information.	Y	
	ARIES will share and exploit court appearance information.	Y	
	ARIES will generate and maintain audit log information.	Y	
End-User Features	A web-enabled, browser based user friendly GUI interface will be provided for ad-hoc query capability.	Y	
	ARIES will provide the capability for users to save query (parameters) for future recall and search.	Y	
	ARIES will provide the capability for users to create a default query.	Y	
	ARIES will provide the capability for users to create a background query which can be signaled to run at a future time.	Y	
	ARIES will provide the capability to create an event trap for automatic notification to all	Y	

Feature	Requirement	Code	Comments
	logged on ARIES users. Officer Notification - provide a notification by email or some other electronic means to officers who are interested in a person, vehicle or property. For example, an officer may want to be notified when a person is entered into the system or a warrant is out for a person's arrest.		
	A web-enabled, browser based user friendly GUI interface will be provided for accessing "Person" information.	C	
	A web-enabled, browser based user friendly GUI interface will be provided for accessing "Vehicle" information.	C	
	A web-enabled, browser based user friendly GUI interface will be provided for accessing "Property and Weapon" information.	C	
	A user friendly GUI interface will be provided for accessing audit trail data for each department.	Y	
	ARIES will provide the capability to select and sort query fields.	Y	
	ARIES will provide the capability to select and sort query results fields.	Y	
	ARIES will provide the capability to print query results.	Y	
	ARIES will provide the capability to save query results to a local file.	X	Agencies do not want this capability for accountability reasons.
	The screens for describing the filters to be used for report record selection and report format and content must be easy to use. The program must provide context sensitive help functions and meaningful error messages.	Y	
	Comprehensive record filtering functionality. ARIES will include a full range of record selection features that permit a variety of record inclusion and exclusion parameters, including the capability to select records based on partial string matches of text data.	Y	
	ARIES will provide a regional mail server.	Y	
	ARIES will provide a regional online chat capability.	Y	
Security	Password protection	Y	
	Require a single sign on to access system.	Y	

Feature	Requirement	Code	Comments
	Encrypt Passwords.	Y	
	Limit number of illegal access attempts.	Y	
	The ability to monitor and report all illegal access or attempted entry into the system.	Y	
	Any GUI password fields will be masked or invisible.	Y	
	Lightweight Directory Access Protocol (LDAP) will be used for managing user information.	Y	
	System maintenance functions can be performed only be users with system administration authorization.	Y	
	Administrate security controls and access authority from a central location viewed by a user friendly GUI interface.	Y	
Security: Audit Trail	Each agency will have a centrally maintained audit trail database of RMS access requests.	Y	
	ARIES will automatically generate and maintain the audit trail database.	Y	
	The ARIES audit logs will be separated into two portions: ▪ header info (name, date, databases, and tables accessed) ▪ body info (query string) and these logs will be separately accessible with ARIES GUI and linked by unique keys.	Y	
	ARIES will provide a GUI interface to search audit logs.	Y	
	ARIES will provide a GUI interface to archive audit logs.	Y	
	ARIES will provide a GUI interface to restore audit logs.	Y	
	ARIES will provide a GUI interface to expunge audit logs.	Y	
	Access to the Dissemination Log should be restricted to the designated. ARIES network Security personnel.	Y	
Runtime	The ability to perform on-line queries in an adequate response time. The application should be optimized for this function.	Y	
	Agency databases should be designed to optimize real time on-line queries.	W	
	Any Ad Hoc or System Administration function such as Ad Hoc reporting or on-line	Y	

Feature	Requirement	Code	Comments
	backup (such as audit log archival) should minimally effect the normal operation of the system.		
	The system should be available 98% of the time. In an average month of 720 hours, this allows for a system downtime of 2%, or 14.4 hours.	Y	
	A performance model should be developed early in the design phase of the project. Data similar to those produced in the ARIES environment should be simulated over the network model. The performance should be monitored as an ongoing task.	Y	
	The solution provider should state the bandwidth requirements for adequate throughput to support the typical ARIES network for initial and future usage requirements.	Y	
General	Help screens for all online ARIES screens.	Y	
	Online user's guide.	Y	
	Application support tools and administration tasks such as maintaining user profiles and validation tables should be presented via a user friendly GUI application.	Y	
System	Year 2000 Compliance	Y	
	Flexibility: Ability to scale and support image and multimedia data types in later versions.	Y	
Future	ARIES will provide interconnectivity with the multimedia production and browsing SMART system.	C	
	ARIES will provide computer mapping features.	C	
	ARIES will provide high-end statistical models for trend analysis and crime forecasting.	D	

Figure 11.1

ACRONYMS

ADA	Assistant District Attorney
ARIES	Automated Regional Information Exploitation/Sharing System
CAD	Computer Aided Dispatch
CDPD	Cellular Digital Packet Data
CID	Criminal Investigation Division
CONOPS	Concept of Operations
DA	District Attorney
CDJS	Division of Criminal Justice Services
DOB	Date of Birth
DMS	Document Management System
DRN	Data Record Number
DSS	Department of Social Services
DSY	Division Services for Youth
ERD	Entity Relationship Diagram
GUI	Graphical User Interface
HTTP	Hyper Text Transport Protocol
IBR	Incident Based Reporting
JAD	Juvenile Aid Division
NCIC	National Crime Information Center
NHPD	New Hartford Police Department
NLECTC	National Law Enforcement and Corrections Technology Center
NYSPIN	New York Statewide Police Information Network
NYSUCS	New York State Unified Court System
OCDA	Oneida County District Attorney
OCDTF	Oneida County Drug Task Force
ODBC	Open Database Connectivity
OCSATF	Oneida County Sexual Abuse Task Force
RMS	Records Management System
RPD	Rome Police Department
S-HTTP	Secure Hyper Text Transport Protocol
SORA	Sex Offender Registration Act
SSL	Secure Socket Layer
SSN	Social Security Number
SJS	Spectrum Justice System
TLS	Transport Layer Security
UASF	Utica Arson Strike Force
UCR	Uniform Crime Reporting
UPD	Utica Police Department
VPN	Virtual Private Network
WAN	Wide Area Network

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.