INFORMATION SHARING AND INTEROPERABILITY IN LAW ENFORCEMENT: AN INVESTIGATION OF FEDERAL CRIMINAL JUSTICE INFORMATION SYSTEMS USE BY STATE/LOCAL LAW ENFORCEMENT ORGANIZATIONS.

THESIS

David R. Dethlefs, Captain, USAF

AFIT/GIR/ENV/03-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/ENV/03-02

INFORMATION SHARING AND INTEROPERABILITY IN LAW ENFORCEMENT: AN INVESTIGATION OF FEDERAL CRIMINAL JUSTICE INFORMATION SYSTEMS USE BY STATE/LOCAL LAW ENFORCEMENT ORGANIZATIONS.

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

David R. Dethlefs
Captain, USAF

March 2003

AFIT/GIR/ENV/03-02

INFORMATION SHARING AND INTEROPERABILITY IN LAW ENFORCEMENT: AN INVESTIGATION OF FEDERAL CRIMINAL JUSTICE INFORMATION SYSTEMS USE BY STATE/LOCAL LAW ENFORCEMENT ORGANIZATIONS.

David R. Dethlefs
Captain, USAF

Approved:

\\SIGNED\\ — 9 Apr 03
Summer E. Bartczak, Lt Col, USAF (Advisor) — Date
Associate Professor, Information Resource Management
Department of Systems and Engineering Management

\\SIGNED\\ — 9 Apr 03
Alan R. Heminger, PhD (Reader) — Date
Associate Professor, Information Resource Management
Department of Systems and Engineering Management

\\SIGNED\\ — 9 Apr 03
Henry B. Potoczny, PhD (Reader) — Date
Professor, Computer Science and Engineering
Department of Electrical and Computer Engineering

Acknowledgements

I'd like to thank Ms. Portia Gonzalez-McDade and Mr. Randy Scheiffer of the Ohio Peace Officer Training Academy for all their assistance with my survey pretest and pilot test. I was overwhelmed with the level of support I received from them, and the success of this research rests in great part to the assistance they provided.

Special thanks also go out to Mr. Bill Stamper of the SC shop for all his patience and hard work implementing the survey's website. This was a burden I was ill-equipped to handle, and I greatly appreciate all Bill did to make this a reality.

Additionally, there are those folks who really help you to maintain your bearing and sanity during certain portions of your research; and along those lines, I'd like to thank Captain Dan Ray, Major Danny Holt, and Major Edward White III for the advice and assistance they provided during the statistical analysis of the survey's results.

In conjunction with Captain Tony Kimbrough, Captain Jason May, and First Lieutenant John Wagnon, I'd like to thank the many audiences we've had over the past year in lab 243. We really enjoyed entertaining you all.

And finally, I'd like to thank my thesis committee for all their guidance and support during this research effort.

Table of Contents

List of Figures

List of Tables

Page

Abstract

This thesis investigates the frequency of use and perceptions of usefulness of federal criminal justice information systems among state and local law enforcement personnel and certain IS environmental factors that affect usage. The study is predicated by a demonstrated need for increased information sharing, interoperability, and collaboration among the three tiers of law enforcement as public safety threats within U.S. borders increase in complexity; e.g., the Murrah Federal Building bombing, Columbine High School shooting, 9/11 terrorist attacks, and D.C. sniper case. The results of this research indicate high usage and perceived usefulness of the National Crime Information Center Network (NCIC Net), National Law Enforcement Telecommunications System (NLETS), Uniform Crime Reporting/National Incident Based Reporting System (UCR/NIBRS), National Instant Criminal Background Check System (NICS), and federal LE websites. The results also indicated that the IS environmental factors information quality and trust influenced the usage and perceived usefulness of federal criminal justice information systems.

INFORMATION SHARING AND INTEROPERABILITY IN LAW ENFORCEMENT: AN INVESTIGATION OF FEDERAL CRIMINAL JUSTICE INFORMATION SYSTEMS USE BY STATE/LOCAL LAW ENFORCEMENT ORGANIZATIONS.

I. Introduction

General Issue

The federal government has spent over $370B on software, computers, and infrastructure since the network boom began in 1993 (Puzzanghera, 2002). Despite the quantity of monetary resources allocated to enhance information networks and information-sharing capabilities among governmental agencies over the past ten years, problems persist in creating a collaborative information-sharing environment in which essential information can be shared and accessed by organizations with a need to know that information. This problem most recently received a great deal of scrutiny by the public and Congress after the al Qaeda terrorist attacks on September 11, 2001; however, information-sharing across electronic networks between federal, state, and local law enforcement (LE) agencies has been a notable problem for quite some time (Cohen, 1994; Souder, 2001; Mueller, June 2002). In a report on information-sharing capabilities within the public safety community, the Public Safety Wireless Advisory Council, established by Congress in 1995, stated that "unless immediate measures are taken to alleviate shortfalls and promote interoperability, public safety agencies will not be able to adequately discharge their obligation to protect life and property in a safe, efficient, and cost-effective manner" (NLECTC, 2002).

Several information systems currently provide essential criminal justice information across the three tiers of government (federal, state, and local). Figure 1 depicts how state and local LEs access and receive information from federal criminal justice information systems. These criminal justice information systems can be characterized in a variety of ways. Some examples include fingerprint, ballistic, and

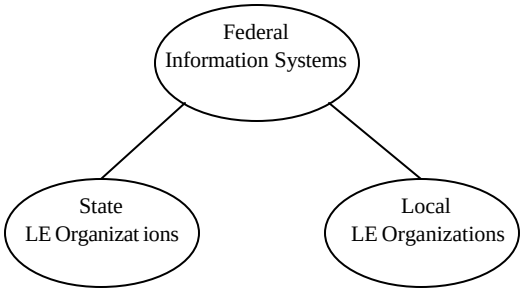

Figure 1: Federal LE agencies communicate with state and local LE organizations through federal criminal justice information systems.

criminal record databases. Traditionally, most of the high-cost systems have been fielded at the federal level with the expectation that state and local LEs will/can access them in order to tap information/data that could be helpful in execution of their daily duties. In most cases, this "information-sharing" relationship has simply not materialized (Canterbury, 2001; Johnson, 2002). Previous research indicates information quality, trust, and access as possible reasons for this lack of information sharing (Kling, 2000). Although some actions such as the Public Safety Wireless Networks program and the FBI's $400M Trilogy project are attempting to address the technology issues impeding collaborative information-sharing and networking capabilities within the LE community, Congressional testimony suggests there is more to the problem (Jordan, 2002; Mueller, 2002; Ziglar, 2001; Souder, 2001). As a precursor to developing new information systems to improve information sharing and collaboration between all levels of LEs, an

assessment of existing information systems and perceptions regarding their use and usefulness is necessary.

Problem Statement

Though several information-sharing systems currently provide essential criminal justice information across the three tiers of government (federal, state, and local), the frequency of use and perceived usefulness of these existing information systems toward enhancing LE missions has never been assessed. Additionally, perceptions about additional environmental factors that influence use of these systems (and ultimately information-sharing) have not been captured.

Research Questions

In order to address the problem stated above, this thesis will concentrate on the following research questions.

Research question #1. To what extent are existing federal criminal justice information systems used by state and local departments?

Research question #2. What are state and local LE "user" perceptions regarding the usefulness of federal criminal justice information systems in accomplishing LE missions at the state and local levels?

Research question #3. What are state and local LE "user" perceptions regarding the environmental factors that may affect criminal justice information system usage and information sharing between federal and state/local LE levels? Environmental factors include access, system quality, information quality, and trust.

Summary

The following chapters present the spectrum of information gathered and analyzed during this research effort. The purpose of each chapter is outlined below:

Chapter 2, Literature Review, provides in-depth background material on LE organizations, current interoperability/information sharing problems, existing federal information systems, and current efforts to enhance information-sharing capabilities/processes.

Chapter 3, Methodology, discusses the design, testing, and implementation of the survey used to discover the extent of use and perceived usefulness of existing federal criminal justice information systems, as well as state/local LE users' perceptions of additional environmental factors that influence the use of these information systems.

Chapter 4, Findings and Analysis, presents the survey results and analyzes the implications of those results toward the research questions proposed above.

Chapter 5, Conclusions, interprets research findings in a practical perspective and presents recommendations based on what was discovered during research. The limitations of this research effort and topics for future research are also presented.

II. Literature Review

Introduction

This chapter reviews background information pertinent to how federal law enforcement agencies share information with state and local law enforcement agencies. The discussion of literature begins by defining the boundaries between federal law enforcement and state/local law enforcement levels. The discussion then transitions into law enforcement information-sharing and interoperability. Then follows a brief review of federal law enforcement coordination efforts as they relate to electronic information-sharing capabilities. Finally, the chapter ends with a discussion of the IS environmental factors that have been cited as influencing use and perceptions of the usefulness of federal criminal justice information systems.

Definitions

Before discussing the literature, it is important to define a variety of terms in the context of this research. Terms defined in this section include law enforcement officer, information system, information sharing, and interoperability.

Law Enforcement Officer.

The first definition describes what is meant by the term "law enforcement officer." The basic definition of a law enforcement officer comes from Title 5 of the United States Code (Legal Information Institute, 2002): "an employee, the duties of whose position are primarily the investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws of the United States, or the protection of officials of the United States against threats to personal safety; and are

sufficiently rigorous that employment opportunities should be limited to young and physically vigorous individuals…." In its rulings, the Merit Systems Protection Board, an Executive Branch agency that reviews federal employment policy issues as authorized by the Civil Service Reform Act of 1978, has reinforced this definition, directing that "a federal employee meets the definition of law enforcement officer if he or she: has frequent direct contact with criminal suspects; is authorized to carry a firearm; interrogates witnesses and suspects, giving Miranda warnings when appropriate; works for long periods without a break; is on call 24 hours a day; is required to maintain a level of physical fitness" (Friel et al, 2002).

In addition to defining "law enforcement officer," it is important to distinguish between the various levels of law enforcement in the government. Federal law enforcement officers are employed by agencies operated or controlled by any one of the federal departments. For example, the Department of Justice operates several law enforcement agencies (LEAs) including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), the Immigration and Naturalization Service (INS), and the United States Marshal's Service (USMS). The Department of the Treasury also operates a number of LEAs including the Secret Service, Bureau of Alcohol, Tobacco, and Firearms (ATF), United States Customs Service, and the Internal Revenue Service Criminal Investigative Division. The Departments of State, Defense, Transportation, and the Interior also operate LEAs. In all, there are 32 federal LEAs. For descriptions of major federal LEAs, see Appendix A. An LE officer at the federal level has the broadest level of authority covering wide jurisdictions, sometimes nationwide.

Each state within the U.S. also operates a number of LEAs. State LEAs usually operate solely within the borders of the particular state and include highway patrol, state troopers, and state bureaus of investigation (e.g., Florida Highway Patrol or the Kansas Bureau of Investigation). State-run agencies may be nominally similar or share common tasks with federal agencies; however, state and federal LEAs are quite separate. For example, officers employed at the state level do not carry commensurate authority or jurisdiction as federal LE officers.

Likewise, each county, province, municipality, city, and town within a state may operate a number of LEAs. These agencies including county sheriff's offices and city police departments represent the local LE level. Local LEAs are limited in authority and jurisdiction even more so than state LEAs. Local jurisdictions might include only the area within certain county lines or within city corporate limits.

Information System.

Another important definition is that of an "information system." An information system can be defined as "a system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information" (Newton et al, 2002). Information systems can include the Internet, private or public computer networks, radio networks, etc. This thesis concentrates primarily on computer-based information systems which contain criminal justice information such as criminal histories, mugshots, fingerprints, etc. In the LE community, these systems are commonly called criminal justice information systems.

Information systems can also be conceptualized as socio-technical systems: complex, interdependent systems comprised of people, hardware, software, techniques,

support services, and information structures (such as content, rules/norms/regulations, access controls, etc) within a matrix of social and technical dependencies (Kling, 1999). In addition to the basic definition of an information system, the socio-technical view recognizes that cultural and environmental factors influence the use and perceptions of usefulness of a particular system. Because this research addresses cultural factors influencing the use and perceptions of usefulness of criminal justice information systems, the socio-technical view of information systems has been adopted. Accordingly, this thesis integrates Kling's socio-technical view of information systems, which is discussed in more depth later in the chapter.

Information sharing and interoperability have recently become extremely important topics in law enforcement (Jordan, 2002; Canterbury, 2002; Quijas, 2002). Network interoperability provides the basis for information sharing across information systems, which in turn affects the ability of distinctly separate units to work jointly toward completing tasks. As public safety threats become more complex, especially with the increased threat of terrorism (i.e., the Murrah Federal Building bombing and 9/11 terrorist attacks), the need for LE agencies to work jointly increases. Congressional testimony indicates that greater information sharing and network interoperability capabilities within the LE community are necessary to achieve effective joint operations (Jordan, 2002; Mueller, June 2002; Souder, 2001). The following paragraphs will briefly define what these terms mean in the context of this thesis effort.

Information Sharing.

Information sharing is a basic concept. It is the sharing of information and information resources among two or more parties. Despite its conceptual simplicity,

information sharing can be difficult to achieve. In government functions, there are several laws that apply to what information can be shared, how it can be shared, and with whom it can be shared (Whiting et al, 2001). Security concerns further complicate information-sharing initiatives. In testimony before the Senate's Judiciary Committee, FBI Information Sharing Task Force Director Robert Jordan iterated this concern: "One equity we must balance with our desire to share information as freely as possible is the need for the security of [highly classified and controlled] information" (Jordan, 2002). To address security concerns, the FBI has set up 47 Joint Terrorism Task Forces (JTTF) which help to streamline interaction and information sharing between federal, state, and local law enforcement organizations. Jordan stated that "JTTFs have proven to be one of the most effective methods of unifying federal, state, and local law enforcement efforts to prevent and investigate terrorist activity by ensuring that all levels of law enforcement are fully benefiting from the information possessed by each" (Jordan, 2002).

As stated in Chapter 1, several recent incidents have underscored the importance of sharing criminal justice information and have revealed numerous faults in information-sharing practices. Recent information-sharing policy changes have evolved in light of tragedies such as the Columbine High School shooting, Murrah Federal Building bombing, and the terrorist attacks of September 11, 2001. As Jordan (2002) stated before Congress, "a substantial component of this [counterterrorism] approach is information sharing, not only at the federal level but also within the entire law enforcement and intelligence communities."

Interoperability.

Interoperability incorporates two distinct, yet related, ideas: the ability of communication networks to pass information across system boundaries and the ability of separate organizations or separate sections within an organization to cooperate toward completing an action or goal. These concepts are interrelated because separate units that can't communicate with one another experience difficulty in efficiently completing joint tasks, as illustrated in the reactions of public safety agencies to the Columbine High School shooting incident (Columbine Review Commission, 2001).

Current communications interoperability problems arose from the way networks were originally designed. The data systems and radio networks used by law enforcement today were implemented largely in a "simpler, less connected age" (CIO Magazine, 2001). Inspector General Glenn Fine, in his testimony before the Senate Subcommittee on Technology, Terrorism, and Government Information, described the basic problem: "We see separate automated systems planned for almost every function in the INS, but many of these systems do not talk to each other and therefore cannot be used to meet other important agency goals" (Fine, 2001). FBI Director Mueller noted the same problem among FBI IT systems (Puzzanghera, 2002). Each system was designed to accomplish a narrowly defined purpose for a very specific group of individuals using different, often incompatible, operating systems. Because network technology was so new when these systems were implemented, little thought was given to how these systems would communicate with each other as the systems matured. Now that interoperability has become a prevalent issue, the full impact of each system's incompatibility with other related systems is being realized. It is a difficult and

expensive problem to solve. For example, the INS operates a fingerprint identification system called IDENT, and the FBI utilizes their own fingerprint identification system called IAFIS. Though the two systems perform a similar function, they were implemented using very different network architectures and operating systems. A current project to improve criminal identification capabilities will connect the two systems. That project is expected to take five years and $200M to complete (Whiting et al, 2001). Aldona Valicenti, CIO for the Commonwealth of Kentucky, noted that an integrated system can't simply be purchased; federal and state agencies are faced with constructing interoperable networks comprised of new technology and divergent legacy systems already in use (CIO Magazine, 2001).

Resolving interoperability issues is a universal challenge, not confined to certain departments or governmental functions. Given the magnitude of the problem, several interoperability research and grant programs have been implemented by the federal government to aid federal agencies in integrating their IT systems. Some of these programs, like the Advanced Generation of Interoperability for Law Enforcement (AGILE) and Public Services Wireless Networks (PSWN), both described in Appendix B, are specifically concerned with enhancing interoperability within law enforcement agencies. Many federal agencies, including the FBI, recognize that interoperability success includes a change in the way they do business. As FBI Director Mueller (June 2002) outlined the FBI's reorganization plan to the Senate in early 2002, he delineated plans involving knowledge management principles, a collaborative information-sharing environment, and a strategic view of information sharing which would be cornerstones to the reorganization's success.

Actions are also being taken to encourage interoperability between organizations in daily operations. For example, a more unified link between intelligence-gathering agencies and law enforcement agencies has been encouraged by Congress, with little outward resistance from such primary representatives of those two groups as the CIA and FBI (Mueller, June 2002). Duplication of effort has come under heavy fire as well. As law enforcement agencies feel the crunch of diminishing resources, officials are reviewing overlapping functions such as border patrol, drug interdiction, and violent crime investigation for ways to improve efficiency (Mueller, June 2002).

Such efforts are not without their problems. One of the goals of the AGILE program is to increase interoperability "without requiring substantial changes to internal systems or procedures" (AGILE, 2002). This will be a difficult goal to realize as many legacy systems will require a great deal of change in order to make them compatible with other systems, such as in the IDENT/IAFIS merger mentioned above. Cost is another issue. Modifying IT systems can be expensive, and there are a great number of systems requiring upgrades and modifications.

Despite these challenges, interoperability successes have been realized within the LE sector. For example, more than 500 police departments nationwide now utilize a wireless system linking patrol cars to an electronic database for at-the-scene information including license plate numbers, driver's license information, and criminal histories. The system returns requested information in as little as five seconds, and officers belonging to organizations using this network are able to reference up to 80 license plate checks per shift—up from 10 checks per shift using traditional methods (Motorola, 2002).

Law Enforcement Coordination Efforts

Despite the number of information-sharing systems available to LEAs, problems persist with getting critical information to the agency or individual who needs it (Council on Foreign Relations, 2002; Leahy, 1998; CIO Magazine, 2001). Federal agencies have realized that cultural factors, such as negative attitudes toward sharing information, have greatly influenced abilities to complete LE missions. Traditionally, federal agents were afforded the luxury of secrecy, often denying case details to state and local LE officials when working inside their jurisdictions. However, the proliferation of terrorist activities within the U.S. has produced a threat to public safety so great that the luxury of secrecy can no longer be afforded to federal agents. Consequently, in the weeks following the 9/11 tragedies, many federal LEAs created offices dealing specifically with LE coordination issues across the three tiers of government. This section will briefly cover FBI and INS realignment strategies intended to bolster LE coordination efforts as related to information sharing.

FBI Initiatives to Increase Information Sharing.

Both the FBI and INS have executed plans to coordinate with state and local LEAs with greater openness, frequency, and diligence after both agencies fell under scrutiny by Congress in the wake of the 9/11 terrorist attacks. The FBI began a major restructuring operation in early 2002, realigning several strategic objectives from the previous strategic plan in 1998. In his testimony to Congress in June 2002, FBI Director Robert Mueller outlined how the FBI was refocusing its mission and priorities. One of the three primary missions under the agency's new alignment is to provide support to federal, state, local, and international LE partners. Mueller also stressed that, while law

enforcement, investigations, and protecting US interests remained the focus of FBI efforts, LE coordination is "equally critical to enabling the FBI to successfully achieve its goals and objectives" (Mueller, June 2002). LE coordination efforts outlined in the FBI's new strategic plan include the creation of the Office of Law Enforcement Coordination (OLEC), Chief Technology Officer (CTO), and Office of Records Management (ORM).

The Office of Law Enforcement Coordination (OLEC) is the FBI's primary authority "responsible for improving FBI coordination and information sharing with state and local law enforcement and public safety agencies" (Federal Bureau of Investigations, 2002). OLEC will act as the formal point-of-contact in the FBI for LE professional organizations as well as state and local LE agencies. Formerly, no functional authority existed within the FBI to facilitate interaction with state and local LE officers. FBI leadership realized that ad hoc relationships with other LEAs would not suffice against emerging threats against the U.S. and the that the bureau needed to create a cohesive relationship that combined LE capabilities of federal agencies and 675,000 state and local LE personnel into a synergistic effort (Mueller, May 2002).

The FBI also expects to develop collaborative efforts in information sharing. To encourage this objective, the FBI created two new offices: the Chief Technology Officer (CTO), whose responsibility includes overseeing and modernizing IT programs including the Trilogy project, and the Office of Records Management who is "responsible for modernizing FBI records and knowledge management processes and policies" (Federal Bureau of Investigations, 2002). The CTO's responsibilities stem partly from the FBI's Chief Information Officer (CIO) mission, and the two offices are interrelated entities. The CIO's role involves IT strategy development supporting all the FBI's departments

(Mueller, July 2002), and the CTO will help to meet those strategic objectives through IT initiatives including information-sharing tools such as Law Enforcement On-line, an interactive web-based LE education application. The role of the Office of Records Management stems from an FBI goal to enhance the agency's flexibility and agility. Its mission is to combine the bits and pieces of information residing in FBI field offices into a centralized body of knowledge including subject matter experts and historical case knowledge (Mueller, June 2002) and, in the support of the FBI's shift toward counterterrorism, it is charged with "building a national level of expertise and body of knowledge that can be accessed by and deployed to all field offices and that can be readily shared with our Intelligence Community and law enforcement partners" (Mueller, June 2002). Additionally, Mueller expects the Office of Records Management to eradicate file management and documentation deficiencies noted in the House Judicial Committee's investigation report. Like the CTO/CIO relationship, the Office of Records Management will interact closely with the pre-existing Information Resources Division, which holds the responsibility of managing/planning the FBI's information resources and developing architectures for information collection and use.

INS Initiatives to Increase Information Sharing.

The INS also began restructuring after the 9/11 terrorist attacks. In his testimony before the House Judiciary Committee, INS Director James Ziglar cited serious resource shortfalls (including personnel) as a factor relating to the agency's inability to effectively meet today's immigration law enforcement challenges (Ziglar, 2001). The root causes of resource shortfalls include a "significant growth in illegal immigration activity, unprecedented increases in application for immigration services, and new immigration

laws that heightened the complexity of the agency's responsibilities" (Immigration and Naturalization Service, 2001).

The INS Restructuring Proposal outlined three important realignment features designed to improve the agency's interoperability with other federal, state, and local LEAs: splitting immigration services and immigration enforcement into two separate bureaus, creation of a CIO position, and the creation of the Interagency Liaison Officer position (Immigration and Naturalization Service, 2001).

The INS Restructuring Proposal calls for a separation of its two basic missions—immigrations services and law enforcement—into completely distinct chains of command operating within the same agency. According to the proposal, the Bureau of Immigration Services will handle all activities related to provisions outlined in guidelines of the Immigration and Naturalization Act including immigration benefits, naturalization application processes, and asylum/refugee determinations. The Bureau of Immigration Enforcement will take on all law enforcement responsibilities currently relegated to INS including border patrol, detention and removal, and international enforcement (Immigration and Naturalization Service, 2001). The proposal asserts that this change will improve INS mission effectiveness by "better defining roles and responsibilities, simplifying the chain of command, and strengthening accountability" (Immigration and Naturalization Service, 2001). The intention here is to simplify processes to improve performance and remedy major problems identified through procedural audits. Easy-to-understand organizational structure and roles are expected to facilitate communication with state and local LEAs, in effect, streamlining immigration LE processes.

The newly created CIO will manage implementation, access control, maintenance, and provision of all INS information systems. The CIO will also coordinate information-sharing activities with other federal, state, and local agencies. Finally, the Interagency Liaison Officer (ILO) holds the overall responsibility of fostering law enforcement coordination across the three tiers of government. The ILO will "facilitate an improved flow of information and cooperation with federal, state and local law enforcement organizations" (Immigration and Naturalization Service, 2001). This office is analogous to the FBI's Office of Law Enforcement Coordination.

From a LE coordination perspective, the restructuring plan seeks to improve INS mission accomplishment through clearer accountability standards, enhanced information-sharing capabilities, better defined strategic intergovernmental relationships, and elimination of competing priorities. If these objectives are met, INS expects to obtain a more synergistic relationship with state and local LEAs.

Summary of Federal LEA Initiatives to Increase Information Sharing.

Federal LEAs have begun to realize the value of open communications and robust interagency coordination efforts across jurisdictional and level-of-government boundaries. As resources get tighter on all levels, the need for synergistic operations between local, state, and federal LEAs will become critical. There are only 56 FBI field offices across the U.S.; however, these field offices are able to increase their reach, flexibility, and resource pools through collaborative efforts with the 19,000 state and local LE offices nationwide. Information-sharing tools like NLETS and IAFIS provide a foundation for distributing criminal justice information; however, effective and well-

planned coordination efforts are necessary in combination with information-sharing capabilities to make collaborative law enforcement a successful national program.

Environmental Factors that Influence Information Sharing via Information Systems

The following sections discuss the IS environmental factors discovered in the literature that influence information sharing via information systems. Social informatics is the "interdisciplinary study of the design, uses, and consequences of information technologies that takes into account their interaction with institutional and cultural contexts" (Kling, 1999). Social informatics looks at information systems in the workplace as more than just tools because an information system's use is "unavoidably linked with social and organizational factors" (Kling, 2001). Instead, information systems are viewed primarily as socio-technical systems: complex, interdependent systems comprised of people, hardware, software, techniques, support services, and information structures (such as content, rules/norms/regulations, access controls, etc.) within a matrix of social and technical dependencies (Kling, 1999). Social informatics recognizes that achieving a more complete understanding of information and communication technologies requires that business models be supplemented with an ecological viewpoint (Kling, 2000) where IS environmental factors such as institutional and cultural contexts (Kling, 1999) influence the usage and perceptions of usefulness of information systems and must be taken into consideration over the system's lifetime. While there are many IS environmental factors that influence the usage and perceptions of usefulness of information systems in general, this literature review identified four IS environmental factors specifically influential to the usage and perceptions of usefulness of federal criminal justice information systems: access, system quality, information

quality, and trust. The following paragraphs describe each of the factors and their meaning in the context of this research.

Access.

Kling (2000) talks about three aspects of access: technological access, social access, and access control. In Kling's terms, "technological access refers to the physical availability of suitable equipment, including computers that are of adequate speed and equipped with appropriate software for a given activity" (2000). Social access refers to the "mix of professional knowledge, economic resources, and technical skills for using technologies…" (Kling, 2000). Access control refers to applying constraints on certain users limiting the availability of certain resources (Newton et al, 2002). Though one of Kling's three aspects of access, social access was not identified as a potential problem for federal criminal justice information systems in the literature, technological access and access control were often cited as issues affecting frequency of use and perceptions of usefulness of criminal justice information systems (Canterbury, 2001; Jordan, 2002; Mueller, April 2002; Souder, 2001). In his testimony regarding federal information sharing with local law enforcement to the Senate Judiciary Committee, Fraternal Order of Police National Vice President Chuck Canterbury underscored the importance of access:

> It is critical that state and local agencies be kept in the loop by their federal counterparts. Ninety-six percent of law enforcement officers in the United States are employed by state and local governments….Yet, in critical situations, federal agencies citing federal statutes restrict access to this important information. All too often, interagency cooperation is hampered by the lack of a free flow of information from federal agencies to state and local departments. In the past, it has often been a one-way street, with state and local law enforcement providing information to their federal colleagues and getting very little if any information in return (Canterbury, 2001).

Chuck Wexler, executive director of the law enforcement think tank Police Executive Research Forum, describes state and local LE frustrations with federal criminal justice information systems: "…police officials are infuriated about having to undergo background checks of up to six months to gain access to FBI reports….We should be sharing information right away" (Johnson, 2002). These frustrations seem contradictory to FBI Director Mueller's promise: "Let me assure you of one thing: if a state and municipal law enforcement agency does not possess a needed expertise, the FBI will provide the assistance and expertise needed" (Mueller, June 2002). In an earlier statement, Mueller (May 2002) stated that collaboration with state and local LE organizations was an FBI priority intended to strengthen professional relationships and information sharing.

Technological Access.

As previously stated, technological access is one of the two access-related issues related to criminal justice information systems. It is a growing concern within major federal criminal justice information system programs, notably in the AGILE, IAFIS, and NIBIN programs (AGILE, 2002; CJIS Division, 2002; NIBIN Branch, 2002). Acquisition, installation, and maintenance costs for the equipment necessary to access these systems are prohibitively expensive for most police departments (CJIS Division, 2002; NIBIN Branch, 2002). This limitation almost automatically excludes many state and local LE departments from access to the information contained within those criminal justice information systems. To remedy the problem, the Department of Justice has enacted a program to provide funding to state and local LE organizations for the acquisition and installation of certain systems (NIBIN Branch, 2002). The Department of

Justice realizes that the information contained on specific federal criminal justice information systems such as NIBIN is critical to aiding state and local LE departments in effectively completing public safety missions. Specifically, this information aids investigators in the identification, apprehension, and conviction of criminal suspects. Without access to this information, the ability of state and local LE organizations to carry out public safety missions can be seriously impaired or degraded. In testimony to the House Appropriations Committee, FBI Director Mueller (June 2002) stated that "…each [Special Agent in Charge] should also take into account the ability of state, municipal, and other federal law enforcement to handle the full range of criminal violations…." This statement demonstrates an emerging attitude within the federal LE agencies to realistically consider the capabilities of state and local LE organizations and to assess how the actions of federal agencies can impact the capabilities of state/local LE organizations. More specifically, federal LE agencies are beginning to consider enhancing capabilities of state and local LE organizations through increased information sharing in order to positively impact the LE community as a whole.

Access Control.

Access control is the second access-related issue concerning federal criminal justice information systems. Access controls limit users' access to types of information or features contained on an information system. For example, a certain user may have an NLETS account which allows him access to the IAFIS database; however, due to access controls placed on his account, this user may not have access to other NLETS databases such as CODIS or III. Certain access controls were identified in the literature as possible problem areas. As in the example, the literature indicated that state/local LE units were

excluded from certain areas on federal criminal justice information systems (Whiting et al, 2001; Dempsey, 2000).

Additionally, denial of access to case-related and classified information was identified as a problem (Jordan, 2002; Mueller, June 2002). Case-related information can exist in many forms: criminal histories, fingerprints, DNA samples, psychological profiles, etc. Different pieces of information about the same person or case can exist at different locations or in different departments. While it may seem easy to simply share this information, there are obstacles that impede sharing case-related information. Legal constraints are an example of obstacles limiting access to information. Several laws prohibit the sharing of several types of information among LE organizations in order to protect the rights and privacy of citizens. The biggest obstacle, however, is finding this information. Take the D.C. sniper case for example. John Lee Malvo, the 17-year-old suspect in the sniper case, was arrested in Montgomery, AL for a shooting committed on the night of 21 September, 2002—only weeks before the D.C. shootings began. Malvo's fingerprints were obtained during the criminal investigation and stored on a criminal database run by the State of Alabama. Weeks later, during the sniper investigation, federal agents obtained shell casings from several crime scenes which contained fingerprints—possibly belonging to the shooter. The fingerprints did not match any sample in the FBI's database. As the investigation progressed, federal agents received information that linked the D.C. sniper to the Alabama case. With this lead, federal agents contacted Alabama state LE officers to investigate the match. Within two hours, a match was confirmed and federal agents now had an identified suspect in the sniper case. Since the 9/11 terrorist attacks, access controls to criminal justice information have been

reviewed. The USA Patriot Act, passed in the wake of the 9/11 terrorist attacks, relaxed and even repealed several laws impeding information sharing; however, as evidenced by the statements of Canterbury and Wexler above, more progress may be necessary to realize effective sharing of case-related information.

A greater problem may exist with classified information due to its sensitivity. Classified information possessed by federal LE agencies is shared in few circumstances. The D.C. sniper shooting case was unprecedented in the amount of classified information that passed between federal agents and state/local LE officers. As a rule, classified information possessed by federal LE agencies is only shared when the situation is so dire as to necessitate it. However, given the evolving nature of major criminal activity in the U.S., as previously discussed, this attitude may be changing.

System Quality.

System quality is another IS environmental factor that influences information system usage and perceptions of usefulness. U.S. Inspector General Glenn A. Fine testified before the Senate Judiciary Committee about system quality problems within the Justice Department: "We see separate automated systems planned for almost every function in the INS, but many of these systems do not 'talk' to each other and therefore cannot be used to meet other important agency missions" (Fine, 2001). System quality encompasses a wide range of information system characteristics ranging from how long it takes to connect to the network to how capable the system is at recovering from an attack. Four system quality characteristics were identified in the literature as possible problems: flexibility, currency, security, and interpersonal vs. electronic contact.

Flexibility.

Flexibility refers to the capability of an information system to support various platforms—often termed robustness in the IS community (Newton et al, 2002). Concern about whether a new system would be able to integrate with the various existing state/local networks was expressed during the development of the FBI's Interstate Identification Index (SAIC, 2002) (see Appendix B for program description). Developers of the III system realized that it had to be flexible enough to accommodate the various network implementations that might exist among III's future users. While the III system took this feature into consideration during the design phase, many other federal criminal justice information systems which were developed before the proliferation of networks in the workplace require upgrades or other reengineering before they are compatible with the various existing network implementations. The seriousness of this problem for the LE community has not yet been determined.

Currency.

Currency refers to how state-of-the-art federal criminal justice information system technology is. The currency of technology in the federal sector seems to be a major concern, and much of the literature referred to how obsolete criminal justice information technology is perceived to be within the federal sector. Existing federal criminal justice information systems are often described as obsolete or behind current capabilities (CIO Magazine, 2001; Dean, 2001; Dizard, 2002; Higgins K., 2002; Mueller, May 2002; Puzzanghera, 2002). Given the frequency with which federal criminal justice systems are described as obsolete, it would appear that this system quality feature may be a problem. Given that some criminal justice information systems still work in a green-screen

environment (Higgins K., 2002; Mueller, May 2002), there's little doubt that federal criminal justice information system technology is behind current capabilities. Many state and local IS networks are in just as bad shape. The funding to upgrade these systems simply has not been allocated; however, because federal systems have not been modernized, state and local systems on the same level can still access the information resident on these systems regardless of the obsolete nature of the technology.

Security.

The security of information on federal criminal information systems is another greatly discussed topic in the literature. In reaction to the growing number of cyber attacks in the late 1990s, the Critical Infrastructure Protection Board was formed to monitor emerging cyber threats and to warn government, business, and educational communities of cyber threats such as the "Melissa" virus. The intent of this organization is to limit the damage inflicted by major attacks on U.S. IT infrastructure, including criminal justice information networks. If criminal justice information networks are damaged or otherwise off-line for extended periods of time, the ability of the LE community to carry out public safety missions is negatively influenced. Likewise, the information contained on criminal justice information networks must be adequately protected from malicious manipulation, where data is illicitly deleted or changed by unauthorized system users.

In addition to protecting criminal justice information from hackers or loss (Vaida, 2001), the sensitivity of this information requires that sharing be restricted to a "need to know" basis. Jordan (2002) states "the need for information security must be balanced by the driving need of the criminal investigator to be able to follow any and all avenues

in an investigation. Creating a methodology for properly identifying individuals with a need to know and granting them access further complicates security measures. If these security measures are not addressed appropriately, perceived system quality may be negatively affected.

Interpersonal vs. electronic contact.

A preference for interpersonal contact is another cultural characteristic identified in the literature that may have significant influence on the usage and perceived usefulness of federal criminal information systems. "To get the data they need, many enforcers still favor using faxes or milking personal relationships" over information systems (CIO Magazine, 2001). Computer and network technologies are still so new that many officials in the LE community may still be significantly uncomfortable with utilizing information systems in the workplace. This cultural characteristic may take years to disappear as older LE officers are replaced by recruits who are more comfortable with utilizing IS technology in the workplace. Though this IS environmental factor is mentioned in the literature, the overall significance of this factor toward influencing the use of criminal justice information systems has not been fully analyzed.

Information Quality.

Information quality is another IS environmental factor that influences usage and perceptions of usefulness. Poor information quality can negatively affect perceptions of the usefulness of a particular system. Kling's (2001) example from the Department of Motor Vehicles (DMV) provides an illustration of how poor information quality can deteriorate the usefulness, which ultimately affects the usage, of information systems. In this example, the DMV linked the DMV database with the Social Security

Administration (SSA) database in an effort to make the license issuing process more efficient. The plan was to enter the social security number the license applicant and use the name, date of birth, and other information contained on the SSA database. However, the SSA database did not record nicknames (i.e., "Pete" instead of "Peter" or "Matt" instead of "Matthew") or name changes (i.e., for marriage or other legal name changes). These discrepancies halted the process completely, and individuals were refused a license due to these minor differences. Consequently, the new system was deemed inappropriate for accomplishing DMV objectives and was abhorred by users and customers alike.

Information quality can also be affected by the accuracy of information contained on the system (Dempsey, 2000). An example of how accuracy affects the quality of criminal justice information systems can be seen in statements found in Congressional testimony. U.S. Inspector General Fine testified that, during an inspection of INS information systems, the information on INS information systems was found to be "incomplete and unreliable due to missing departure records and errors in processing of the records" (Fine, 2001). Accuracy is a critical information quality factor in the LE community. It can lead to wrongfully convicting an innocent suspect or mistakenly acquitting a guilty suspect. Either situation can lead to tragic consequences and is deemed unacceptable by public safety standards.

Additionally, information quality can be affected by how frequently resident information on the system is updated or new information is introduced (Dempsey, 2000). Congressional testimony reinforced questions about information quality on criminal justice information systems regarding the frequency of updates. In the wake of the 9/11 terrorist attacks, INS Commissioner James Ziglar testified before the House Committee

on Government Reform that "our ability to do our job is really limited only by our resources and the time it takes to put resources online" (Souder, 2001). This problem was highlighted in recounts of the Rafael Resendez-Ramirez case, where the failure to update information on the IDENT-INS system contributed to the release of a known felon illegal alien (Resendez-Ramirez) in June 1999. Resendez-Ramirez was mistakenly released from a U.S. prison into the custody of the border patrol, who deported him to Mexico. Resendez-Ramirez "returned to the United States within days of his release and murdered several more people before surrendering…" (Fine, 2001).

Finally, information quality can be affected by how long resident information on the system is kept in the database (Dempsey, 2000). This is an important issue for maintaining any database. One simple solution is to discard information when an offender has passed away; however, this may further complicate closing some cases. For example, murder and other violent crime cases are open indefinitely. The Jack the Ripper files are open cases despite the fact that the murderer is long dead. Likewise, more modern violent crime cases remain unclosed because they have not been solved. Discarding criminal history, DNA, and fingerprint information of known felons who have died may destroy the possibility of solving open violent crime cases if one of those dead felons was involved. The literature did not yield whether the LE community perceives information on federal criminal justice information systems is kept for an adequate period of time or whether that information is discarded too quickly.

Consequently, when users perceive that information quality has dropped below a threshold of usefulness, they may turn to other information sources. If federal criminal justice information systems fail to provide the quality of information needed by the user,

state and local LE officers may turn to other available options. One such option is the local community. The following example highlights the fact that locally-obtained information sometimes holds greater value for the user. Months before the 9/11 terrorist attacks, FBI Agent Coleen Rowley discovered evidence that could have prevented the hijackings (Rowley, 2002; Council on Foreign Relations, 2002). When she channeled this information to FBI Headquarters in Washington DC, her request to investigate was denied despite her beliefs that the information was vital to national security.

Additionally, state and local LE officials also have the option of turning to state-run criminal justice information systems. Since its inception in 1999, the Kansas Criminal Justice Information System (see Appendix C for program description) has been regarded as a very successful criminal justice information system (Wartell, 2000) and has prompted other states to develop their own versions. Additionally, most states provide a state-run electronic fingerprinting service similar to the FBI's IAFIS. As discussed above, during the D.C.-area sniper case, information from Alabama's fingerprinting service helped to confirm the identities of the prime suspects in the case.

In light of these options, federal agencies are concerned with whether state/local LE users utilize federal criminal justice information systems and the information contained within those systems. One concern is the growing complexity of criminal threats against the U.S. As criminal activity becomes more sophisticated, cooperation from LE professionals across geographically separated areas will be necessary to successfully combat these threats. Clues may be widespread across the nation, as in the 9/11 terrorist case. Alone, local or regional information systems may not be effective because their grasp (across state/territorial borders) may not be sufficient to reach the

entire LE community. Federal systems, though they have not officially taken on this role, may be able to provide that kind of oversight—connecting geographically separated LE organizations to the information they need. Another reason is that federal criminal information systems are the sole source for certain pieces of information, such as ballistics information from NIBIN. Without these systems, critical information simply may not reach the organization that needs it.

Trust.

Trust is the final IS environmental factor influencing federal criminal justice information systems usage and perceptions of usefulness. In 1997, Iacono and Weisband conducted a study on virtual teams—"groups of people who must work closely together for a short period of time, learn from each other and accomplish specific goals, but for whom face-to-face contact is too costly or simply not possible most of the time" (Iacono et al, 1997). The virtual team concept closely resembles the relationship studied in this research. Iacono and Weisband's research examined how trust was developed in temporary, electronic teams (Iacono et al, 1997). Virtual teams develop a form of trust called "swift trust" (Iacono et al, 1997; Meyerson et al, 1996) where "members must act swiftly as if trust were in place rather than waiting to see who can be trusted and who cannot" (Iacono et al, 1997). Swift trust evolves over time as temporary groups reinforce their initial trust or damage it (Meyerson et al, 1996).

Iacono et al (1997) argue that virtual teams "must work continuously and consistently to maintain expectations of trust." One trust maintenance activity is how responsive federal LE agencies are to requests for information from state/local LE organizations. This behavior is alluded to several times in the literature. "[Federal, state,

and local LE agencies] should be sharing information right away," asserts Police Executive Research Forum executive director Chuck Wexler (Johnson, 2002). However, as stated earlier, inspections on federal criminal justice systems within the Justice Department found that this was not the case: "…the FBI must be able to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. Failure to capitalize on leads in its possession can delay or seriously impede an investigation" (Fine, 2001).

State/local LE officials' perceptions about federal agencies' abilities to carry out duties or effectively complete missions can impact trust. The literature suggests that certain recent federal LE actions may have damaged this trust; e.g., the Rowley incident discussed above (Council on Foreign Relations, 2002). After testimony by several federal LE commissioners during a hearing with the House Committee on Government Reform concerning post-9/11 homeland security, U.S. Representative Ben Gilman stated, "…it's important that we recognize the potential for law enforcement resources to be stretched beyond their means. In fact, we're hearing reports that resources for other law enforcement missions, such as our drug interdiction, may be diverted to fill the new demand for homeland security" (Souder, 2001). FBI Director Mueller testified that the agency's intelligence-gathering strategy was "fractured and not well coordinated" (Mueller, May 2002). In testimony later that year, Mueller stated the FBI was attempting to "create a centralized body of subject matter experts and historical case knowledge that, in the past, has been largely resident in a few FBI field offices" (Mueller, June 2002). In further testimony, Vice President of the Federal Law Enforcement Officers Association Michael Prout expressed the challenges faced by INS officers: "The INS deports 112,000

illegal immigrants a year, fewer than half the 275,000 who enter illegally each year or stay after their visas expire….As I travel to the numerous FLEOA chapters throughout the country, the topic most on the minds of the more than 1,000 beleaguered INS special agents who currently belong to FLEOA is the urgent need for a substantive and dynamic reorganization of the immigration law enforcement mission….The latest Census figures list 1,875,000 illegals in California or 4,630 per agent" (Prout, 2001). Based on these statements, it may appear that federal agencies are overwhelmed or otherwise incapable of completing public safety missions. If this impression has permeated the state and local tiers of the LE community, their trust in federal agencies may be negatively impacted.

The quality of interaction between virtual group members can impact trust as well. In the past, the quality of interaction between federal agencies and the rest of the LE community has been poor (Canterbury, 2001; Johnson, 2002). In April, 2002, FBI Director Mueller announced the creation of the FBI's Office of Law Enforcement Coordination (OLEC) as part of the FBI's reorganization—the purpose of which is "to foster cooperation and strengthen law enforcement relationships at every level" (Mueller, April 2002). Shortly after its creation, OLEC's new director, Louis Quijas, stated, "One of the goals of the OLEC is to help bring together federal, state, and local resources to make our communities safer….[Mueller] has said many times that the FBI is only as good as its relationships with state and locals. We are of the belief that quality communications will be the basis of those relationships" (Quijas, 2002). Whether reorganization efforts help to improve the quality of interaction between federal LE agencies and the rest of the LE community is yet to be seen.

Iacono et al (1997) also argue that a necessary part of interaction between virtual teams is "the forming of good communications habits (e.g., checking and responding to email as demanded by the task)…." As implied, these good communications habits include feedback. Wexler's statement about communication between state/local LE agencies and the federal government being a one-way street (Johnson, 2002) indicates that feedback from federal LE agencies has been lacking. This is another problem that the FBI and INS hope their reorganizations will help to correct.

Summary

To recap, this chapter began by defining several key concepts used throughout this thesis including law enforcement, information systems, information sharing, and interoperability. The difference between the three tiers of government (federal, state, and local) as relates to LE was also discussed. The discussion then transitioned to ongoing efforts within federal LE agencies (specifically, the FBI and INS) to better collaborate with state and local LE organizations. Finally, the IS environmental factors introduced in Chapter 1 (access, system quality, information quality, and trust) were explained in further detail.

The next chapter presents the research methodology used for this thesis effort to discover how effective federal law enforcement electronic information sharing coordination efforts are perceived among state and local law enforcement organizations. A survey-based data collection methodology was used in this research, and Chapter 3 will discuss information about survey implementation procedures, validation processes, and procedures for designing and testing the survey instrument.

III. Methodology

Introduction

This chapter describes the research methodology used during the data collection phase of this research effort. The following sections include information about survey implementation procedures, validation processes, and a description of the survey's sample population. Procedures for designing and testing the survey instrument are presented, including survey question construction, pretest and pilot test procedures, and results of the human subjects review. The research questions are also explained in more detail. Finally, data analysis strategies are discussed.

Driver for Research Design

The overall objective of this research was to collect state and local LE perceptions, or attitudinal information, about federal criminal justice information systems. It was determined that system evaluations or document reviews would only yield superficial information about the characteristics of each system (e.g., how much data is contained on the system, how many users are authorized on the system, how fast the average transfer rate on the system is, etc). Though this kind of information helps to describe a system, the methodology would not have been sufficient to achieve the research objectives. In contrast, a survey-based research design allows for the collection and analysis of quantifiable information pertaining to the research questions. Therefore, a survey was designed specifically to gain data on usage and perceptions of usefulness of federal criminal justice information systems in the context of the LE user at the state and

local levels. This research design appeared to be the most useful methodology toward achieving the stated research objectives.

Additionally, individual survey questions were constructed in a format suitable for collecting perceptual information by using a Likert scale. "The Likert scale works particularly well in the context of a series of questions that seek to elicit attitudinal information about one specific subject matter" (Rea et al., 1997).

In order to collect enough data for statistically valid results, responses were needed from a certain number of individuals from the target population. Therefore, characteristics of the target population had to be factored into the considerations for research design. The primary driver for using a survey, from the perspective of the target population, was convenience for the audience. Dr. John Firman, International Association of Chiefs of Police Research Department, advised that response rates among law enforcement personnel tend to be low. With respect to this, simplicity and ease of use became primary survey design objectives. Survey completion time had to be minimized in order to encourage a higher response rate. The total survey completion time goal was less than 15 minutes.

Components of Research Design

This section includes information on various components of the research design. Here, each of the research questions introduced in Chapter 1 is explained in more depth. The survey development process is also discussed, including brief descriptions of each survey question. The survey's sample population is also described, stating the reasons for including each portion of the sample population. Finally, research design quality considerations such as validity and reliability are presented.

Research Questions.

Research question #1: How frequently are existing federal criminal justice information systems used by state and local departments?

This question concentrated on the *frequency of use* of certain federal criminal justice information systems that connect federal LE agencies with the state and local levels. The goal of this research question was to answer, *from the perspective of state and local LE organizations*, the extent to which existing federal criminal justice information systems are used. The range of information systems examined in this survey was constrained by several factors. The first limitation was that information systems studied in this research had to be *criminal justice* information systems. Second, only *federal* criminal justice information systems were addressed. Several multi-state or regional criminal justice information systems exist—such as the Northern Lights project, a state-administered IS initiative which connects law enforcement organizations across the borders of Maine, Vermont, New Hampshire, and New York (Leahy, 1998). However, this study was concerned with information sharing between the federal level and state/local levels. Therefore, to answer this question, analysis was constrained to criminal justice information systems executed at the federal level which grant access to state/local LE users. Research question #1 implied that federal criminal justice information systems allow state/local LE users access to the information. Indeed, there are federal criminal justice information systems that do not grant access below the federal level—DRUGX, for example (Drug Enforcement Administration, 2002). However, for the purposes of this study, those systems were excluded from the survey. Only federal criminal justice information systems that allow state/local LE users access were

considered for inclusion on the survey. Additionally, only *existing* criminal justice information systems were considered—barring phased-out or future-planned information systems. Additionally, comparisons of subsets of the sample population, based on collected demographics, were conducted to determine if responses to survey items pertaining to this research question differed significantly.

Research question #2: What are state and local LE "user" perceptions regarding the usefulness of federal criminal justice information systems in accomplishing LE missions at the state and local levels? This question concentrated on the *extent of usefulness* of certain federal criminal justice information systems that connect federal LE agencies with the state and local levels. The goal of this research question was to answer, *from the perspective of state and local LE users*, how useful federal criminal justice information systems are perceived to be toward accomplishing LE missions. The question assumed that certain federal criminal justice information systems may be perceived to be more useful than others. As with the first research question, comparisons of subsets of the sample population, based on collected demographics, were conducted to determine if responses to survey items pertaining to this research question differed significantly.

Research question #3: What are state and local LE "user" perceptions regarding the environmental factors that affect criminal justice information system usage and subsequent information sharing between federal and state/local LE levels? There are certain IS *environmental factors* that may influence *user perceptions* about the usefulness of a particular information system, thereby affecting *usage* of those criminal justice information systems and subsequent *information sharing*. For example, the amount of

data accessible through a particular information system may affect how useful that system is perceived to be. For instance, an information system that allows the user access to a great deal of data might be more useful than an information system that allows access to a limited amount of data. Likewise, the quality of information on a system may also affect perceptions about usefulness. For example, an information system with access to large amounts of irrelevant data may be perceived to be less useful than an information system with a smaller amount of pertinent data. Overall, this research question attempted to assess state and local LE criminal justice information system user perceptions regarding the IS environmental factors that may influence information system usage and information sharing. Environmental factors addressed in this study included access, system quality, information quality, and trust as discussed in Chapter 2. As with the first two research questions, comparisons of subsets of the sample population, based on collected demographics, were conducted to determine if responses to survey items pertaining to this research question differed significantly.

Survey Construction.

This section describes the survey formats and advantages of using each format.

Survey Format.

The survey was implemented in two formats: web-based for LE professional organizations and mail-out for CIOs of state bureaus of investigation. While choosing only the web-based format was considered optimal, constraints on the sample population forced the use of both the web-based and mail-out formats. It has been reported that using a mixed method approach can influence research results; however, there are several factors that minimize the effects of this mixed approach. Several studies have found that

response rates for web-based surveys tend to be lower than mail-out surveys (Manfreda et al, 2001; Gonier, 1999; Kwak et al, 1999). Manfreda et al cite "low preference for the web mode" (2001) as a possible contributing factor. For this study, only a small portion of the sample population received the mailed survey (50 out of 15,000). Additionally, studies indicate that there may be statistically significant substantive and data quality differences (e.g. non-response rates for closed ended questions) between the two methods that may impact research results (Manfreda et al, 2001; Gonier, 1999). Simply noted, the researcher is aware of the influences of using a mixed method approach; however, deemed it necessary to complete research objectives. Results from the web-based format and mail-out format were compared to detect statistically significant differences in the responses. The results of this comparison are presented in the "Comparisons" section of Chapter 4.

Web-based Format.

The primary implementation of the survey, a web-based format, was chosen for several reasons. First, "both quantitative and qualitative information can be gathered" (Upcraft et al, 2002). This allows the survey to contain both closed- and open-ended questions. Also, web-based surveys can be more convenient for the respondent (Upcraft et al, 2002)—allowing the respondent to take the survey at their own pace, in their chosen environment, and at their chosen time. Web-based surveys allow the collection of results without recording identifying information which allows anonymity in responses (Upcraft et al, 2002). In addition, the cost of implementing a web-based survey can be considerably less than other alternatives (Upcraft et al, 2002; Solomon, 2001). Consequently, it's possible to reach a wider respondent pool given constrained resources,

even if the audience is dispersed across a wide geographic area (Upcraft et al, 2002; Solomon, 2001). Finally, respondent time to complete a web-based survey can be less than other methods (Upcraft et al, 2002; Solomon, 2001). This aspect was considered very important in maximizing the response rate from the LE community.

Mail-out Format.

Several reasons influenced using the mail-out format as the secondary survey method. First, a mail-out format enhances convenience to the user (Rea et al, 1997). According to Rea et al, this format alleviates time constraints, allowing respondents to think about their answers more clearly. Like the web-based survey, another convenience factor is flexibility: respondents take the survey at their own pace, in their chosen environment, and at their chosen time. A mail-out format also offers respondents anonymity in their responses (Rea et al, 1997).

Survey Composition.

Each survey question included closed-ended items, which offered several advantages to the survey design. One advantage was that "the set of alternative answers is uniform and therefore facilitates comparisons among respondents" (Rea et al, 1997). Answer uniformity allows comparisons across sample population characteristics, such as professional organization affiliation or years of service. Uniform data collection also allows for easier data manipulation during the analysis stage, as data do not require intermediate formatting to ensure conformity (Rea et al, 1997). Closed-ended questions tend to be clearer than open-ended questions: "…the fixed list of response possibilities tends to make the question clearer to the respondent. A respondent who may otherwise

be uncertain about the question can be enlightened as to its intent by the answer categories" (Rea et al, 1997).

Survey Item Construction.

The following sections discuss construction of each question on the survey. A copy of the survey can be found at Appendix D.

Demographics.

The survey first asked four demographic questions: state in which the individual currently works, years in law enforcement, primary duty description, and professional organization. The state in which an individual works was recorded to ensure that responses were collected from a variety of geographic areas. This information was important to determine if responses were received from only one geographic area, which could limit the generalizability of the results. Years in law enforcement indicates the level of experience the respondent has. This was an important factor because the greater the experience level of the respondent, the more exposure to criminal justice information systems they are likely to have had—usually, only the higher ranking officers will have regular access to these systems. Primary duty description was also an important demographic because certain LE jobs don't require access to criminal justice information systems. This demographic information helped to identify individuals who weren't part of the target audience and, therefore, identified responses that should be eliminated from the results. Finally, the professional organization (FOP, IACP, or CIO) to which the individual belongs was recorded. It was posited that responses might be significantly different between the populations and collecting this demographic could help to identify those differences.

Section 1: Degree of Use of Federal Information Systems

The first survey question asked users to indicate the degree to which they used 22 federal criminal justice information systems which they were regularly able to access within their department. Responses could be chosen from a six-point Likert scale, ranging from "never" to "constantly" (Schmitt et al, 1991). For system descriptions of the 22 federal criminal justice information systems cited in this survey, see Appendix B.

Section 2: Perceptions of Usefulness of Federal Information Systems

The next question asked respondents to assess the usefulness of each of the 22 systems they were able to access. Responses could be chosen from a five-point Likert scale, ranging from "not useful" to "extremely useful" (Faculty Exchange Program, 2002; Sheard et al, 2000).

Documentation on the various federal criminal justice information systems contained superficial information about how many users could access the system. However, information about how often users access these systems or how useful each system is perceived to be is not captured (Dempsey, 2001)—thus, prompting the first two survey questions.

Section 3: Perceptions of IS Environmental Factors Influencing Use

The final twenty-four questions asked respondents to judge the degree to which they agreed with statements concerning environmental factors of federal criminal justice information systems. Respondents chose responses from a five-point Likert scale, ranging from "completely disagree" to "completely agree" (Siegle, 2002).

These questions were divided into four sections, corresponding to the IS environmental factor (access, system quality, information quality, and trust) to which the

question applied. Questions for each environmental factor were derived from the IS issues identified as significant to the LE arena in the "Information Systems Environmental Factors" section of Chapter 2. Survey questions 3 through 8 related to the construct of access. The disparity of Congressional testimony statements about the level of federal IS access afforded to state/local LE officials prompted survey questions #3 and #6: #3 asks whether federal LE information systems provide adequate support to state and local LE organizations while #6 asks whether federal LE agencies collaborate well with state and local organizations through information systems. Survey question #7 deals with the concept of technological access discussed in Chapter 2. This question was intended to ascertain whether state/local LE officials support the claim that federal LE information system programs take state/local LE agency IT capabilities into account. References about criminal justice information system access controls that could potentially limit the capabilities of state/local LE officials toward mission effectiveness prompted survey questions #4, #5, and #8: respectively, whether federal LE agencies allow access to case-related information to complete state/local LE missions, whether federal LE agencies allow access to classified information to complete state/local LE missions, and whether state/local LE agencies have access to the federal criminal justice information networks necessary to complete missions effectively.

Survey questions 9 through 12 related to the construct of system quality. Several federal LE agency directors, including the U.S. Attorney General and FBI Director, voiced major concerns about the currency of federal criminal justice information system technology. These concerns prompted survey question #10: whether state/local LE officials perceive federal criminal justice information system technology to be behind-

the-times. Doubts about the currency of federal criminal justice information system technology led to another concern: whether federal criminal justice information systems can support the range of different network implementations that exist at state/local levels. This prompted survey question #9: whether federal LE information systems are flexible enough to support state/local LE agency networks. Due to the sensitivity of information contained on these networks, security is a continual concern. This concern prompted survey question #11: whether state/local LE officials perceive information contained on federal criminal justice information systems to be adequately protected. In the literature review, several documents suggested that interpersonal relationships may still be the preferred method of communicating information in the LE community. These statements prompted survey question #12: whether state/local LE officers feel they get more information from federal LE agencies through interpersonal contact than through electronic systems.

Survey questions 13 through 18 related to the construct of information quality. The disparity between the value of information at the local and federal levels as demonstrated by the Rowley example sparked survey question #13: whether state/local LE officials believe their department is sometimes more informed about situations than federal LE offices. The successful implementation of KCJIS prompted a similar question, survey question #15: whether state/local LE officials believe state-run criminal justice information networks provide more helpful information than federal criminal justice information systems. Doubts about the accuracy of information contained on INS systems prompted survey question #14: whether state/local LE officials believe the information contained on federal criminal justice information networks is accurate.

Update frequency of information contained on criminal justice information systems is another problem associated with INS information systems. This issue prompted survey question #16: whether state/local LE officials believe the information contained on federal criminal justice information networks is updated frequently enough. A study of federal criminal information systems completed by the Center for Democracy and Technology identified the issue of how long information should be kept in IS databases. This issue prompted survey questions #17 and #18: whether state/local LE officials believe the information contained on federal criminal justice information networks is kept long enough or discarded too quickly.

Survey questions 19 through 26 related to the construct of trust. How open a relationship between two entities is can affect the level of trust in the relationship. The literature identified a considerable disparity in the perceived openness of the relationship between federal LEAs and state/local LEAs, and this disparity prompted survey questions #19 and #20: #19 asks whether state/local LE officials believe that federal LE agencies readily share information/resources when a need is identified and #20 asks whether state/local LE officials believe that federal LE agencies quickly respond to requests for information or help. Questions about the accuracy of information contained on federal criminal justice information systems imply the source of information could be the fault. This provoked survey question #21: whether state/local LE officials trust the information received from federal LE agencies. Additionally, perceptions about federal agencies' abilities to carry out duties or effectively complete missions can impact trust. In Congressional testimony, several federal LEA directors testified that the capabilities of their agencies were severely impacted by personnel shortages, funding shortfalls, and

other factors. These staggering statements provoked survey questions #22, #23, and #24: #22 asks whether state/local LE officials trust the capabilities of federal LE agencies to gather effective intelligence about emerging threats, #23 asks whether state/local LE officials trust federal LE agencies' abilities to react to emerging, critical situations, and #24 asks whether state/local LE officials believe federal LE agencies are prepared to deal with the existing level of serious national criminal activities. Finally, the quality of interaction and acceptance of feedback were identified as factors that can affect the level of trust. These concepts sparked the final survey questions, #25 and #26: #25 asks whether state/local LE officials are satisfied with federal LE agencies' day-to-day interactions with their departments and #26 asks whether state/local LE officials believe federal LE agencies are receptive to feedback from their departments.

It is important to note that the survey question sets in this research were not copied from an existing survey instrument. All questions were created by the author based on information gained through the literature review. Survey questions sets were formed to represent the constructs as relating specifically to federal criminal justice information systems.

Sample Population.

The total population of this research effort is defined as all state and local LE employees with on-line capabilities who subscribe to at least one federal criminal justice information system. The total number of individuals in this population is approximately 675,000 (Higgins K., 2002).

The survey's sample population included state bureau of investigations Chief Information Officers (CIOs) and members of LE professional organizations that agreed to

take the survey, including several districts of the International Association of Chiefs of Police (IACP) and the Fraternal Order of Police (FOP). These professional organizations were chosen because they represent a cross-section of U.S. criminal justice information system users. Organizational membership is based on integration within the law enforcement profession and not bounded by race, culture, age, or gender restrictions. Below is a brief description of each professional organization and the reasons for inclusion in the survey sample population.

State Bureau of Investigations CIOs: Each state operates an LE agency similar to the FBI. State-level bureaus perform comparable functions as the FBI, with a limited range of authority—usually within the borders of their parent state with cooperative LE agreements among neighboring states. Each state bureau of investigations employs a CIO to oversee information systems and networks within their jurisdiction. Additionally, CIOs are users of these systems. Because state bureaus of investigation are a primary link between federal LE agencies and state/local LE organizations, the CIOs within these organizations may be able to offer valuable insight on the questions this research seeks to answer. Therefore, CIOs have been chosen as one of the three representative groups in the sample population.

International Association of Chiefs of Police (IACP): The IACP has over 19,000 members in over 100 countries (International Association of Chiefs of Police, 2002). Overall objectives of this LE professional organization are to "advance the science and art of police services…foster police cooperation and the exchange of information and experience among police administrators throughout the world…and to encourage adherence of all police officers to high professional standards of performance and

conduct" (International Association of Chiefs of Police, 2002). The IACP's membership is comprised of high-ranking LE officials in many high population areas, including the major U.S. cities. The IACP was targeted for representation in the sample population because of the broad authority, experience level, and leadership insight that members would be able to provide.

Fraternal Order of Police (FOP): The FOP began in 1915 as a union for law enforcement personnel in order to improve working conditions; however, the organization has expanded its mission to provide improved law enforcement capabilities, enhance professionalism among law enforcement personnel, and encourage community service. Today, the FOP is the largest professional police organization in the US with more than 2,100 local lodges and 300,000 members (Fraternal Order of Police, 2002). FOP members include detectives, beat officers, desk clerks, highway patrol—the wide range of LE specialties at various rank levels. Because FOP membership is not bounded to leadership strata, this organization offers the perspective of the average state/local criminal justice information system user—a valuable perspective for this research effort.

Research Design Quality Considerations.

This section presents considerations for the research design quality of this research. Internal and external validity are addressed. Additionally, the methodology for measuring reliability of each of the constructs is presented.

Internal Validity.

The research methodology attempted to minimize bias. According to Rea et al, use of a survey format reduces interviewer-induced bias: "the mail-out questionnaire exposes each respondent to precisely the same wording on questions. Thus, it is not

subject to interviewer-induced bias in terms of voice inflection, misreading of the questions, or other clerical or administrative errors" (1997).

Attrition bias occurs when respondents submit incomplete responses; e.g., answering only some of the questions on the survey while leaving others blank. This type of bias was addressed by several factors of the survey's design. As mentioned earlier, the survey allows respondents take the survey at their own pace, in their chosen environment, and at their chosen time. These factors, in addition to the survey's brevity, are intended to encourage respondents to complete the survey.

Coverage bias, or systematic omission, occurs when sections of the target population have been omitted from the sample population. For example, coverage bias would be present in the results of a survey about homelessness in New York City if survey participants included only homeless individuals who visited shelters throughout the city. Coverage bias would be introduced because the results would not reflect the characteristics of homeless individuals who do not patronize shelters. The selection of the sample population intended to minimize coverage bias by including the widest possible range of state/local LE officials. Inclusion of the IACP membership was intended to gain perspectives from state/local LE leadership while FOP membership was intended to gain perspectives from all job and rank classes, and inclusion of the CIOs was intended to specifically gain IS manager perspectives. As discussed earlier, utilizing professional organization membership minimizes restrictions on age, race, culture, and gender. Finally, the usage of a web-based survey is justified as the survey is intended to gain assessments on criminal justice information systems from Internet users.

Self-selection within the sample population does introduce some bias (Rea et al, 1997). "Essentially, when people decide to participate in a survey, they select themselves. This decision may reflect some systematic selecting principle or judgement that affects the collected data" (GVU, 1994). Despite this, the amount of self-selection bias has been deemed to be minimal and, therefore, acceptable.

Content Validity.

This research was also concerned about content validity: "the extent to which the content of the measurement instrument reflects what is supposed to be measured" (Shannon et al, 2001). Content validity was assessed using internal consistency measures, which assesses the consistency of items within a measurement instrument (Shannon et al, 2001).

A pretest was conducted to evaluate the face/content validity of the survey instrument. The survey's pretest was threefold. The first phase of pre-testing included a general review by 23 AFIT graduate students. This phase was intended to detect minor items such as typos, unclear wording, confusing design, and survey functionality. During this phase, three minor typos were detected. Participants deemed the survey's design was easy to use and navigate, and the survey's implementation appeared fully functional. A more accurate estimate of the time needed to complete the survey was also gained from this phase of the pilot test. The second phase involved an assessment by AFIT faculty members on my thesis review board. AFIT faculty members reviewed the survey's form, wording, appearance, consistency, execution strategy, and academic support for the concepts incorporated within the questions. In response to feedback from this phase of the pretest, the order of survey questions was rearranged. Each question was reordered

into sections corresponding to the construct to which they applied: access, system quality, information quality, or trust. Additionally, several survey questions were reworded to provide more clarity, and Likert scale wording was changed to correspond to previously proven scales. The final phase of the pretest consisted of a review by law enforcement professionals from two organizations: the Fraternal Order of Police research department and the Ohio Peace Officer Training Academy. These LE experts were asked to review the survey to ensure each question was clear, unambiguous, and relevant. These respondents were also asked to discern if questions were appropriate toward obtaining the stated research objectives. In response to feedback from this phase, minor wording changes were made to provide more clarity to six survey questions.

External Validity.

Due to the cross-sectional design of this survey, the results will be externally valid only if the sample is representative of the total population (Fink, 1995). While the survey did not randomly select participants, the distribution methodology described above was intended to minimize any systematic effect introduced by the sampling method. While this may not be optimal, the survey methodology was deemed valid, given the permission-based constraints of gaining full distribution—or any distribution, for that matter. These factors do not invalidate the findings of this research, however, may constrain the generalizability of the results to the entire LE population (GVU, 1994).

Reliability.

Reliability was tested after both the pretest and the final survey administration to document the instrument's performance. Reliability for the sections regarding the IS environmental factors was measured utilizing SPSS statistical software, which uses the

coefficient alpha to test for consistency. The coefficient alpha "represents the average of all possible split-half estimates" (Shannon et al, 2001). The split-half method demonstrates "the extent to which items perform as consistent measures of a single construct" (Shannon et al, 2001).

All responses to the open-ended question at the end of the survey were examined to determine what additional opinions about federal criminal justice information systems were reported by survey respondents. Any significant comments on federal criminal justice information systems were presented as additional findings in the "Results" section of Chapter 4.

Conduct of the Research

Pilot test.

A pilot test was conducted to ensure the survey's clarity, acceptability, and comprehensiveness. The survey was administered to LE classes (46 total individuals) at the Ohio Peace Officer Training Academy (OPOTA) located in London, Ohio. The purpose and intent of the survey was explained prior to administering. The OPOTA students were then asked to review the survey to assess the following factors: identify questions that were unclear, ambiguous, or otherwise difficult to answer; evaluate whether the length of the questionnaire was acceptable; determine whether information gathered in the survey would invade the privacy of respondents or otherwise violate ethical and moral standards; and judge the relevance of each question and whether response choices demonstrated the complete range of alternatives (Rea et al, 1997).

Coordination for Sample Population.

The research department at the IACP national office recommended the survey be distributed through state-level points of contact in states that agreed to participate in the survey. The line of logic was that membership information would be more accurate at the state level. Contact information (name and phone number and/or email address) for state-level professional organization representatives was gained through a quick Internet search. This information was logged in a master database for future reference.

Each representative was then contacted by phone to enlist their cooperation in distributing the survey web address to their district's membership. Some state offices agreed to cooperate with the research program, and some declined. States that agreed to participate in the survey included Arizona, California, Florida, Illinois, Kansas, Ohio, and Texas.

Mailing addresses for the state bureau of investigations CIOs were also collected from the Internet. CIOs were not contacted by phone in advance. Instead, all 50 CIOs were contacted by mail at the time the survey was implemented.

Human Subject Review.

A human subject review was conducted to ensure that individual safety and privacy were protected throughout the course of this research. A review request was submitted on 6 December, 2002. The Air Force Research Laboratories Experimental Safety Office (AFRL/HEH) at Wright-Patterson Air Force Base, Ohio, convened a review board in accordance with Air Force Instruction 40-402 to assess the safety and privacy considerations of this research effort. The survey methodology was approved on 7 January, 2003; human subject review control number FWR 2003-0040-E.

Data Collection.

The survey consisted of 26 questions (see Appendix D). The survey was executed primarily in an on-line format, accessible from any Internet-capable terminal. During implementation of the survey, 15,000 emails were sent out to law enforcement personnel. The email contained a brief description of the survey and asked recipients to participate in the survey. Recipients could access the survey through a URL attached to the email message. Concurrently, fifty hard-copy mailings containing the same survey were delivered to the CIOs of state bureaus of investigation. According to Rea et al (1997), with the relatively small total population representing the LE community, a minimum number of 348 responses is required to obtain a statistically valid representation.

Data Analysis Strategies.

The following sections present the data analysis strategies for this research.

Data Analysis Strategies for Research Questions #1 and #2.

To answer research questions #1 and #2, the 22 systems studied in this research for frequency of use and perceived usefulness were ranked by a combined frequency of use/perceived usefulness score. The combined score was calculated by multiplying the mean frequency of use for each system by the corresponding mean perceived usefulness. Higher means indicated a greater frequency of use and higher degree of usefulness; therefore, systems were ranked based on the mean scores of these two characteristics. This method does not take into account the standard deviation of responses. Therefore, systems were also ranked via Kendall's tau and differences in the results of each method were analyzed.

As stated in the section discussing the research questions, comparisons will be made between subsets of the sample population to determine if statistically significant differences in responses can be observed. Two comparisons will be made: by service time and by membership in professional organization. To determine if the subset of the population broken out by high or low service time differed significantly, a comparison was made using a z statistic which compares the means of two sample populations. Since both subsets of the population are relatively large (over 30), the CLT can be invoked.

To determine if the subset of the population broken out by professional organization membership differed significantly, a comparison was made using a t test which compares the means of two sample populations. The t test was used in this comparison because the IACP subset of the sample population contained only 16 entries. Because this number does not exceed the threshold for invoking the CLT, the z statistic method used previously would not produce valid results. However, the t test is designed to compare population means when the size of one or both of the subpopulations does not exceed the CLT threshold.

Data Analysis Strategies for Research Question #3.

To determine if mean values of questions about the IS environmental factors differed significantly from the expected mean, a comparison was made between the expected mean and the observed mean using a z statistic, which compares the means of two populations. Because the range of answers is discrete and not continuous, a z-statistic can be used only if it can be shown that the distribution of the z statistic possesses nearly the same shape as the theoretical t distribution for populations that are nonnormal—in other words, the probability distribution must be mound-shaped if not

normally distributed. This is especially true for Likert scale questions, since a Likert scale question with only 5 possible answers cannot possibly possess a normal probability distribution. Therefore, results of these z-tests cannot be used for hard scientific proof, but indications of trends in the data (Shannon et al, 2001). Since the population is relatively large (over 30), the Central Limit Theorem (CLT) can be invoked.

As stated in the section discussing the research questions, comparisons will be made between subsets of the sample population to determine if statistically significant differences in responses can be observed. Two comparisons will be made: by service time and by membership in professional organization. To determine if the subset of the population broken out by high or low service time differed significantly, a comparison was made using a z statistic which compares the means of two sample populations. Since both subsets of the population are relatively large (over 30), the CLT can be invoked.

To determine if the subset of the population broken out by professional organization membership differed significantly, a comparison was made using a t test which compares the means of two sample populations. The t test was used in this comparison because the IACP subset of the sample population contained only 16 entries. Because this number does not exceed the threshold for invoking the CLT, the z statistic method used previously would not produce valid results. However, the t test is designed to compare population means when the size of one or both of the subpopulations does not exceed the CLT threshold.

Comparison of Mail-out vs. Web-based Responses.

As discussed earlier in this chapter, responses must be analyzed to determine if responses differed significantly because of the mixed method approach for data

collection. To determine if the subset of the population broken out by response format differed significantly, a comparison was made using a t test which compares the means of two sample populations. The t test was used in this comparison because the mail-out participant subset of the sample population contains only ten entries. Same as the previous comparison, this number does not exceed the threshold for invoking the CLT; therefore, the z statistic method used previously would not produce valid results. However, the t test is designed to compare population means when the size of one or both of the subpopulations does not exceed the CLT threshold.

Summary

This chapter presented the methodology for this research. The principal factors for choosing a survey-based, quantitative research design were reviewed. The three research questions were further clarified, with in-depth explanations of the intent and verbiage of each question. Procedures for constructing the survey including format and composition considerations were described. The sample population was depicted in an in-depth analysis, including why those sections of the target population were chosen as participants. Validation and reliability issues were also discussed. Additionally, a survey pretest and a three-fold pilot test were conducted to ensure instrument clarity, appropriateness, and effectiveness. The results of these tests were presented in the write-up. Human subject review board results and coordination efforts for distribution of the survey to the target audience were presented. Finally, data collection and data analysis strategies were outlined. The next chapter presents the results of the data collection methodology described above.

IV. Findings and Analysis

Introduction

This chapter presents the results of the data collection phase of this research effort. The following sections include information about the survey's response rate and the demographics of respondents. Procedures for analyzing the data are described, and the results of each survey item are delineated. Segments of the sample population are examined for significant differences in responses with respect to each research question. Finally, responses from the sample population are compared based on response method to detect statistically significant differences due to survey format, a possible limitation of this research effort.

Findings

Response Rate.

During implementation of the survey, 15,000 emails were sent out to law enforcement personnel through the state points of contact. Of the 15,000 law enforcement personnel contacted, 367 accessed the on-line survey. Seven of these responses were incomplete. Incomplete responses were discarded from the results, leaving 360 valid responses to the on-line survey, for an overall 2.4% return rate on the web-based format. Additionally, twelve of the 50 state bureau CIOs returned the mail-out survey, for a 24% return rate on the mail-out format. This response rate (372) exceeded the minimum number of responses (348) necessary to statistically validate research results.

Demographic Analysis.

The following paragraphs present information relating to the demographics collected on the survey. Collected demographics include state in which the respondent works, years in law enforcement, primary duty description, and professional organization to which the respondent belongs.

Responses by State.

The first demographic question asked the respondent in which state they currently work. This information was collected to determine if responses were received from only one geographic area, which could limit the generalizability of the results. Responses were received from 27 states representing a wide geographic dispersion.

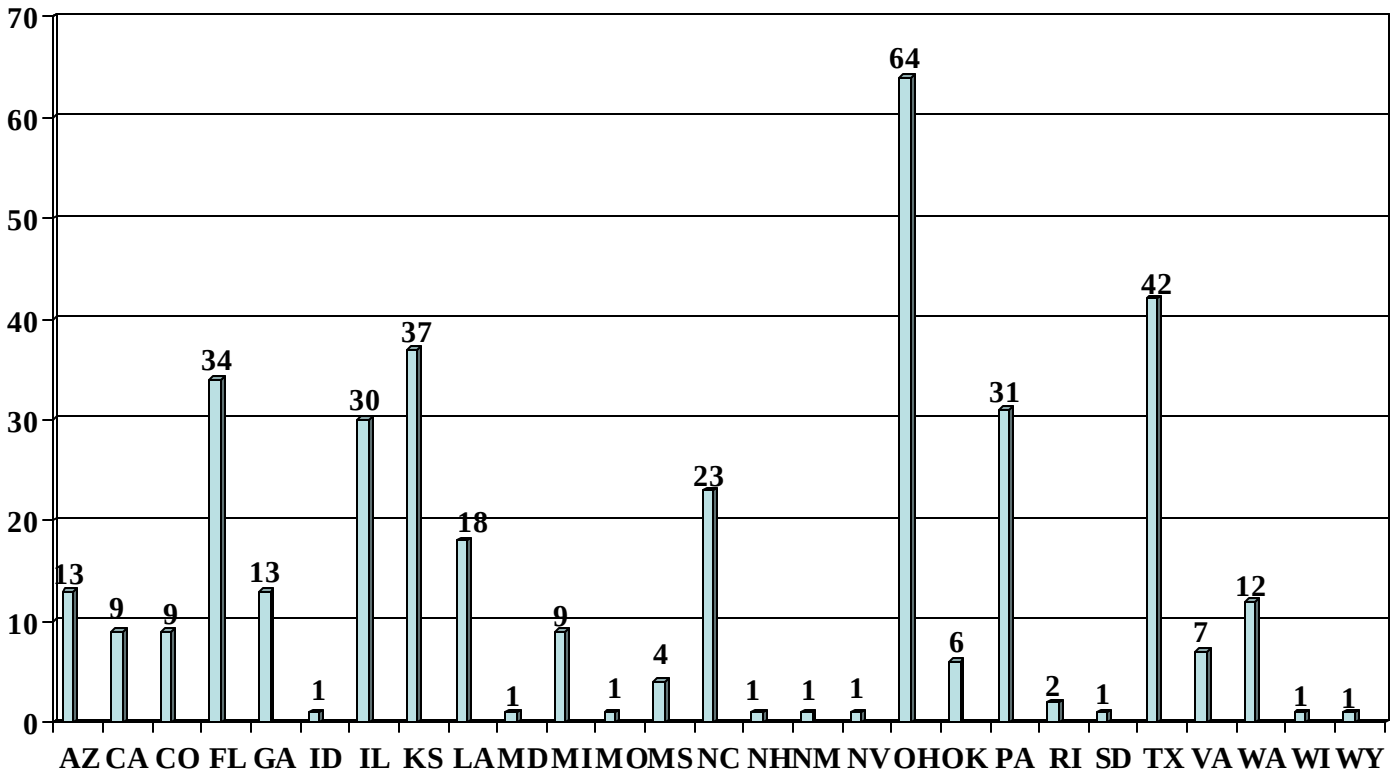

Table 1: Responses by State in Which Respondent Worked

Ohio produced the most responses at 64, followed by Texas (42), Kansas (37), Florida (34), Pennsylvania (31), and Illinois (30). These six states produced almost two-thirds of the total responses; 237 out of the 372 valid responses or 63.97% of the total response rate. The least number of responses came from Idaho, Maryland, Missouri, New Hampshire, New Mexico, Nevada, South Dakota, Wisconsin, and Wyoming—each with one response.

Years in Law Enforcement.

The second demographic question asked the respondent how long they had worked in the law enforcement profession. This was an important factor because the greater the experience level of the respondent, the more exposure to criminal justice information systems they are likely to have had. Years of experience ranged from one year and eleven months to forty years of service. The average amount of experience was nine years and eight months. Out of the total number of valid responses, 161 respondents fell above and 211 respondents fell below the average amount of experience.

Primary Duty Description.

The third demographic question asked respondents to report their primary duty description. This demographic was recorded to identify individuals who may not be part of the target audience and, therefore, identify responses that should be eliminated from the results. Each of the respondents reported at least some experience with federal criminal justice information systems, so none of the 372 complete responses were discarded on the basis of primary duty description.

Participants were given five choices for primary duty description: Patrol, Supervisor, Investigator, Administration, and Other. Of the 372 valid responses, 262

reported "Patrol" as their primary duty description, representing 70.43% of the total responses. Thirty-one respondents reported "Supervisor" and 34 respondents reported "Investigator" as their primary duty description. Only one respondent recorded "Administration" as the primary duty description. Of the 372 respondents, 32 chose "Other." Respondents who chose "Other" were not asked to provide alternate descriptions; however, because each of the respondents indicated some experience with federal CJIS, none of these respondents were removed from the final results. Twelve of the 372 respondents were CIOs.

Professional Organization.

The final demographic question asked respondents to report which professional organization they belonged. Respondents were given three choices for professional organization: Fraternal Order of Police (FOP), International Association of Chiefs of Police (IACP), and Neither. Out of the total number of valid responses, 340 respondents belonged to the FOP, 16 respondents were members of the IACP, and 4 recorded "Neither." The four respondents reporting "Neither" were removed from the final results. CIOs were not asked to report professional organization. The wide gap between the number of responses from the FOP and the number of responses from the IACP is to be expected since the FOP is a much larger organization than the IACP. The FOP reports that its total membership is approximately 300,000 as compared to the total reported IACP membership of 19,000.

Reliability Test Results.

The next sections present the results of the reliability tests performed for both the pilot test and actual results.

Pilot Test Reliability Results.

According to Rea et al (1997), pilot test sample size should be 40-60 individuals. The pilot test sample size for this research was 46 LE students (n = 46) attending classes at the Ohio Peace Officer Training Academy in London, Ohio at the time the pilot test was conducted.

Reliability Results for Frequency of Use and Usefulness.

Since the first two questions asked participants to rate their frequency of use and perceived usefulness of 22 mutually exclusive federal criminal justice information systems, a study of correlation measures would yield unusable information. However, a coefficient alpha was calculated for items one and two of the survey instrument. Q1 yielded a coefficient alpha of .7423, and Q2 yielded a coefficient alpha of .9796. Both values exceed the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). These measures indicate that the 22 subquestions of Q1 and Q2 perform consistently to measure the constructs for each item: frequency of use and perceived usefulness, respectively.

Reliability Results for IS Environmental Factors.

Before reliability tests were conducted on the remaining 24 questions, the items were divided into groups, according to which IS environmental factor they were posited to support: access (questions 3-8), system quality (questions 9-12), information quality (questions 13-18), and trust (questions 19-26).

Reliability Results for the "Access" Construct.

The correlation matrix in Table 2 shows the r values for all questions supporting the IS environmental factor called access. An r value describes how interrelated each

item is with other items. As the r value increases, the more interrelated the items are. With an n = 46 (the number of LE students participating in the pilot test), the minimum r (at p = .05) is .2908 (McClave et al, 2001). The lowest r value in Table 2 is between Q5 and Q8 at .3131, which exceeds the minimum r. The highest r value in the table is between Q3 and Q4 at .7222, which means the highest degree of correlation in this set of questions occurs between Q3 and Q4. These values simply mean that these six survey items collectively represented the construct called "access."

	Q3	Q4	Q5	Q6	Q7	Q8
Q3	1.0000					
Q4	0.7222	1.0000				
Q5	0.3862	0.6706	1.0000			
Q6	0.4600	0.5474	0.5805	1.0000		
Q7	0.5405	0.6088	0.7085	0.5312	1.0000	
Q8	0.4092	0.5009	0.3131	0.5799	0.4692	1.0000

Table 2: Pretest Correlation Matrix for Questions Supporting Access Construct

Table 3 displays the results of several correlative measures between items supporting the IS environmental factor called access. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable. The lowest consistency measure in Table 3 is .5614 (Q8), which exceeds the minimum desired value. The "Squared Multiple Correlation" column indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 3 accounts for a considerable percentage of variance: the lowest value occurs at Q8 at .4587.

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item

consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 3 indicates a Max/Min ratio of 2.3066 with a variance of .0132. The overall coefficient alpha is .8709, which exceeds the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). Again, all these values simply mean that these six survey items correlated to represent the single construct called "access."

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q3	0.6324	0.6044			
Q4	0.7921	0.7292		Max/Min:	2.3066
Q5	0.6605	0.7007		Variance:	0.0132
Q6	0.6807	0.5312			
Q7	0.7257	0.6223			
Q8	0.5614	0.4587			
		Alpha =	0.8709		

Table 3: Pretest ANOVA for Questions Supporting Access Construct

Reliability Results for the "System Quality" Construct.

The correlation matrix in Table 4 shows the r values for all questions supporting the IS environmental factor called system quality. With an n = 46, the minimum r (at p = .05) is .2908. Only one r value in Table 4, between Q10 and Q12 at .3131, exceeds the minimum r. All other r values in the table fall below the minimum, and three r values are negative. This suggests that the items may be mutually exclusive, and they don't adequately represent the "system quality" construct.

	Q9	Q10	Q11	Q12
Q9	1.0000			
Q10	-0.0606	1.0000		
Q11	0.0974	-0.0315	1.0000	
Q12	-0.0540	0.3929	0.0268	1.0000

Table 4: Pretest Correlation Matrix for Questions Supporting System Quality Construct

Table 5 displays the results of several correlative measures between items supporting the IS environmental factor called system quality. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable. The highest consistency measure in Table 5 is .2719 (Q12), far below the minimum desired value. This indicates that these survey items do not correlate to represent a single construct. The "Squared Multiple Correlation" column indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 5 accounts for minor percentages of variance: the highest value occurs at Q10 at .1574. These low correlative measures are further evidence that these items may be mutually exclusive.

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q9	-0.0151	0.0142			
Q10	0.1976	0.1574		Max/Min:	-6.4798
Q11	0.0475	0.0122		Variance:	0.0271
Q12	0.2179	0.1571			
		Alpha =	0.2236		

Table 5: Pretest ANOVA for Questions Supporting System Quality Construct

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item

consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 5 indicates a Max/Min ratio of -6.4798 with a variance of .0271. The overall coefficient alpha is .2236, far below the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). Again, these values suggest that survey items 9-12 did not correlate to represent a single construct.

Reliability Results for the "Information Quality" Construct.

The correlation matrix in Table 6 shows the r values for all questions supporting the IS environmental factor called information quality. With an n = 46, the minimum r (at p = .05) is .2908 (McClave et al, 2001). Only three r values in Table 6 exceed the minimum r. All other r values in the table fall below the minimum, and five r values are negative. These values indicate that these survey items did not correlate well to represent a single construct.

	Q13	Q14	Q15	Q16	Q17	Q18
Q13	1.0000					
Q14	0.0458	1.0000				
Q15	0.2662	0.2989	1.0000			
Q16	-0.1708	0.3536	0.1423	1.0000		
Q17	-0.0978	0.1015	0.0199	0.5110	1.0000	
Q18	0.2069	-0.0283	0.1322	-0.1770	-0.0706	1.0000

Table 6: Pretest Correlation Matrix for Questions Supporting Information Quality Construct

Table 7 displays the results of several correlative measures between items supporting the IS environmental factor called information quality. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable. The highest consistency measure in Table 7 is .3586 (Q15), far below the minimum desired value. The "Squared Multiple Correlation" column indicates how much variance is

accounted for in each item (Shannon et al, 2001). Each item in Table 7 accounts for minor percentages of variance: the highest value occurs at Q16 at .3932. These values simply indicate that these six survey items did not adequately correlate to represent the single construct called "information quality."

	Corrected Item-Total Correlation	Squared Multiple Correlation	Inter-Item Correlation Values	
Q13	0.0890	0.1346		
Q14	0.3035	0.1953	Max/Min:	-2.8877
Q15	0.3586	0.1739	Variance:	0.0385
Q16	0.2037	0.3932		
Q17	0.1611	0.2701		
Q18	0.0502	0.0768		
		Alpha =	0.3951	

Table 7: Pretest ANOVA for Questions Supporting Information Quality Construct

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 7 indicates a Max/Min ratio of -2.8877 with a variance of .0385. The overall coefficient alpha is .3951, far below the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). Again, these values simply indicate that survey items 13-18 did not correlate to represent a single construct.

Reliability Results for the "Trust" Construct.

The correlation matrix in Table 8 shows the r values for all questions supporting the IS environmental factor called trust. With an n = 46, the minimum r (at p = .05) is .2908 (McClave et al, 2001). Six r values in the table fall below the minimum. The

lowest r value in the table is .1616 between Q22 and Q26. The highest r value in the table is between Q22 and Q23 at .8708. These values simply mean that these eight survey items collectively represented the construct called "trust."

	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26
Q19	1.0000							
Q20	0.4297	1.0000						
Q21	0.3308	0.3435	1.0000					
Q22	0.2017	0.1810	0.5332	1.0000				
Q23	0.2951	0.2315	0.5332	0.8708	1.0000			
Q24	0.3156	0.4307	0.3649	0.5724	0.7377	1.0000		
Q25	0.4683	0.5211	0.2311	0.2991	0.3821	0.4239	1.0000	
Q26	0.3231	0.5947	0.3264	0.1616	0.1802	0.2514	0.5695	1.0000

Table 8: Pretest Correlation Matrix for Questions Supporting Trust Construct

Table 9 displays the results of several correlative measures between items supporting the IS environmental factor called trust. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argue that a minimum consistency measure of .5 is desirable. Two values in Table 9 fall below the minimum desired value: Q19 at .4681 and Q26 at .4702. The "Squared Multiple Correlation" column indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 9 accounts for a considerable percentage of variance: the lowest value occurs at Q19 at .3129.

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 9 indicates a Max/Min ratio of 5.3876 with a variance of .0295. The

overall coefficient alpha is .8415, which exceeds the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). Again, these values simply mean that the survey items 19-26 adequately correlated to represent the "trust" construct.

	Corrected Item-Total Correlation	Squared Multiple Correlation	Inter-Item Correlation Values	
Q19	0.4681	0.3129		
Q20	0.5428	0.5177	Max/Min:	5.3876
Q21	0.5505	0.4223	Variance:	0.0295
Q22	0.6030	0.7786		
Q23	0.7060	0.8571		
Q24	0.6589	0.6406		
Q25	0.5870	0.5030		
Q26	0.4702	0.4783		
		Alpha =	0.8415	

Table 9: Pretest ANOVA for Questions Supporting Trust Construct

Misapplication of Reliability Test Results to Survey.

At this point, it is important to point out that the researcher did not change survey to correct faults discovered by the reliability test results. While the reliability test results clearly indicate problems with the systems quality and information quality constructs, these problems were not corrected prior to the survey's final application. This was primarily due to two factors. The first factor was time. The survey's on-line format was constructed concurrently with the collection of pilot test information. The survey was then launched prior to fully completing and analyzing the reliability test results. This mistake was due to the second factor: a lack of experience on the part of the researcher. To put it simply and honestly, the researcher was unaware of this step in the survey design process and skipped it altogether. To correct the problems with the system quality

and information quality constructs, questions in those sections would have been reworded or broken up into multiple questions to better represent the construct. For example, Q10 which asks whether respondents believed that federal CJIS technology was behind-the-times could have been reworded to ask whether respondents believed that federal CJIS technology was behind-the-times such that is was inadequate to fulfill mission needs. Once corrections were made, the pilot test would have been reaccomplished to determine if the new survey items adequately represented the system quality and information quality constructs.

Final Survey Reliability Results.

The final survey reliability results are presented in much the same format as the pilot test reliability results.

Reliability Results for Frequency of Use and Usefulness.

As with the pilot test, the first two questions asked participants to rate their frequency of use and perceived usefulness of 22 mutually exclusive federal criminal justice information systems; therefore, a study of correlation measures would yield unusable information. However, a coefficient alpha was calculated for items one and two of the survey instrument. In the post-implementation analysis, Q1 yielded a coefficient alpha of .8163, and Q2 yielded a coefficient alpha of .8160. Both values exceed the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). These measures indicate that the 22 subquestions of Q1 and Q2 perform consistently to measure the constructs for each item: frequency of use and perceived usefulness, respectively.

Reliability Results for the IS Environmental Factors.

As with the reliability tests for the pretest results, the remaining 24 questions were divided into groups according to which IS environmental factor they supported before reliability tests were conducted: access (questions 3-8), system quality (questions 9-12), information quality (questions 13-18), and trust (questions 19-26).

Reliability Results for the "Access" Construct.

The correlation matrix in Table 10 shows the r values for all questions supporting the IS environmental factor called access. An r value describes how interrelated each item is with other items. As the r value increases, the more interrelated the items are. With an n = 370, the minimum r (at p = .05) is .1034. The lowest r value in Table 10 is between Q5 and Q8 at .2467, which exceeds the minimum r. The highest r value in the table is between Q3 and Q4 at .6486. These values suggest that these six items consistently measure the access construct.

	Q3	Q4	Q5	Q6	Q7	Q8
Q3	1.0000					
Q4	0.6486	1.0000				
Q5	0.2982	0.5674	1.0000			
Q6	0.3524	0.4459	0.4566	1.0000		
Q7	0.4217	0.4913	0.5431	0.4195	1.0000	
Q8	0.3697	0.4609	0.2467	0.4850	0.3752	1.0000

Table 10: Final Survey Correlation Matrix for Questions Supporting Access Construct

Table 11 displays the results of several correlative measures between items supporting the IS environmental factor called access. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable. The lowest

consistency measure in Table 11 is .5159 (Q8), which exceeds the minimum desired value. The "Squared Multiple Correlation" column indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 11 accounts for a considerable percentage of variance: the lowest value occurs at Q8 at .3406.

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 11 indicates a Max/Min ratio of 1.1184 with a variance of .0205. The overall coefficient alpha is .8233, which exceeds the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). These values simply mean that survey items 3-8 adequately correlate to represent the access construct.

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q3	0.5628	0.4593			
Q4	0.7297	0.6072		Max/Min:	1.1184
Q5	0.5598	0.4756		Variance:	0.0205
Q6	0.5787	0.3732			
Q7	0.6060	0.4032			
Q8	0.5159	0.3406			
		Alpha =	0.8233		

Table 11: Final Survey ANOVA for Questions Supporting Access Construct

Reliability Results for the "System Quality" Construct.

The correlation matrix in Table 12 shows the r values for all questions supporting the IS environmental factor called system quality. With an n = 370, the minimum r (at p = .05) is .1034. Only one r value in Table 12, between Q10 and Q12 at .2618, exceeds

the minimum r. All other r values in the table fall below the minimum, and the r value between Q9 and Q12 is negative. This suggests that items may be mutually exclusive and that they do not consistently measure the system quality construct.

	Q9	Q10	Q11	Q12
Q9	1.0000			
Q10	0.0210	1.0000		
Q11	0.0812	0.0113	1.0000	
Q12	-0.0582	0.2618	0.0487	1.0000

Table 12: Final Survey Correlation Matrix for Questions Supporting System Quality Construct

Table 13 displays the results of several correlative measures between items supporting the IS environmental factor called system quality. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable. The highest consistency measure in Table 13 is .1749 (Q10), far below the minimum desired value. The "Squared Multiple Correlation" column indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 13 accounts for minor percentages of variance: the highest value occurs at Q12 at .0752. These low correlative measures are further evidence that these items may be mutually exclusive.

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q9	0.0182	0.0119			
Q10	0.1749	0.0699		Max/Min:	1.0609
Q11	0.0767	0.0095		Variance:	0.0076
Q12	0.1386	0.0752			
		Alpha =	0.2071		

Table 13: Final Survey ANOVA for Questions Supporting System Quality Construct

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 13 indicates a Max/Min ratio of 1.0609 with a variance of .0076. The overall coefficient alpha is .2071, far below the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). Given this outcome, construct of system quality was not supported as a singular concept by the items in this section; therefore, the construct was thrown out.

Reliability Results for the "Information Quality" Construct.

The correlation matrix in Table 14 shows the r values for all questions supporting the IS environmental factor called information quality. With an n = 370, the minimum r (at p = .05) is .1034. Six r values in Table 14 exceed the minimum r. All other r values in the table fall below the minimum, and seven r values are negative. These values indicate that these survey items did not consistently measure the information quality construct as a single construct.

	Q13	Q14	Q15	Q16	Q17	Q18
Q13	1.0000					
Q14	-0.0226	1.0000				
Q15	0.2027	0.2612	1.0000			
Q16	-0.1376	0.2829	0.1553	1.0000		
Q17	-0.1095	0.0692	-0.0001	0.4127	1.0000	
Q18	0.1548	-0.0405	0.0596	-0.1221	-0.0438	1.0000

Table 14: Final Survey Correlation Matrix for
Questions Supporting Information Quality Construct

Table 15 displays the results of several correlative measures between items supporting the IS environmental factor called information quality. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable. The highest consistency measure in Table 15 is .2907 (Q15), far below the minimum desired value. The "Squared Multiple Correlation" column indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 15 accounts for minor percentages of variance: the highest value occurs at Q16 at .2637.

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 17 indicates a Max/Min ratio of 1.1605 with a variance of .0370. The overall coefficient alpha is .3160, far below the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). Again, these values suggest that the survey items 13-18 did not adequately correlate to measure "information quality" as a single construct.

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q13	0.0288	0.0882			
Q14	0.2178	0.1314		Max/Min:	1.1605
Q15	0.2907	0.1295		Variance:	0.0370
Q16	0.2132	0.2637			
Q17	0.1178	0.1778			
Q18	0.0186	0.0374			
		Alpha =	0.3160		

Table 15: Final Survey ANOVA for Questions Supporting Information Quality Construct

Because the correlation values between items supporting the information quality construct were so low, the researcher examined how the overall coefficient alpha would be affected by removing items with the lowest correlative measures. Table 16 shows the effects of removing Q13 and Q18, items with low correlative measures, from the reliability test. Though the overall coefficient alpha did not jump above the minimum desirable level, it did improve to .4961. Because the coefficient alpha did not exceed the minimum alpha, this construct was also thrown out.

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q14	0.3058	0.1298			
Q15	0.1940	0.0788		Max/Min:	1.1383
Q16	0.4406	0.2438		Variance:	0.0355
Q17	0.2348	0.1758			
		Alpha =	0.4961		

Table 16: Maximized Post-Implementation ANOVA for Questions Supporting Information Quality Construct

Reliability Results for the "Trust" Construct.

The correlation matrix in Table 17 shows the r values for all questions supporting the IS environmental factor called trust. With an n = 370, the minimum r (at p = .05) is .1034. The lowest r value in Table 17 is between Q22 and Q26 at .1310, which exceeds the minimum r. The highest r value in the table is between Q22 and Q23 at .7044. These values indicate that these survey items consistently measured the trust construct.

	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26
Q19	1.0000							
Q20	0.3745	1.0000						
Q21	0.2996	0.2426	1.0000					
Q22	0.1715	0.1481	0.4518	1.0000				
Q23	0.2009	0.1965	0.4643	0.7044	1.0000			
Q24	0.2626	0.3993	0.3038	0.5416	0.6131	1.0000		
Q25	0.3465	0.4543	0.1347	0.2077	0.3157	0.3499	1.0000	
Q26	0.2362	0.5638	0.2264	0.1310	0.1729	0.2717	0.4644	1.0000

Table 17: Final Survey Correlation Matrix for Questions Supporting Trust Construct

Table 18 displays the results of several correlative measures between items supporting the IS environmental factor called trust. The "Corrected Item-Total Correlation" column indicates how consistent items are with the scale to total. Shannon et al (2001) argues that a minimum consistency measure of .5 is desirable.

	Corrected Item-Total Correlation	Squared Multiple Correlation		Inter-Item Correlation Values	
Q19	0.3995	0.2289			
Q20	0.5078	0.4502		Max/Min:	1.2864
Q21	0.4665	0.3244		Variance:	0.1108
Q22	0.5350	0.5394			
Q23	0.6136	0.6089			
Q24	0.6226	0.4872			
Q25	0.4889	0.3592			
Q26	0.4369	0.3836			
		Alpha =	0.8000		

Table 18: Final Survey ANOVA for Questions Supporting Trust Construct

Four values in Table 18 fall below the minimum desired value: Q19 at .3995, Q21 at .4665, Q25 at .4889, and Q26 at .4369. The "Squared Multiple Correlation" column

indicates how much variance is accounted for in each item (Shannon et al, 2001). Each item in Table 18 accounts for a considerable percentage of variance: the lowest value occurs at Q19 at .2289.

The "Inter-Item Correlation Values" column compares the minimum and maximum r values from the correlation matrix, which helps to determine inter-item consistency. A ratio of 1:1 is desirable with a variance as close to 0 as possible (Shannon et al, 2001). Table 18 indicates a Max/Min ratio of 1.2864 with a variance of .1108. The overall coefficient alpha is .8000, which exceeds the minimum desired coefficient alpha of .7 (Hair et al, 1995; Nunnally, 1978). These values simply mean that survey items 19-26 adequately correlate to represent the trust construct.

Results.

The following sections present the results of the survey and comparisons of the sample based on years of service and membership in professional organizations as they pertain to each research question.

Research Questions 1 & 2: Frequency of Use and Perceived Usefulness.

This section presents results which help to answer research questions #1 and #2. Research question #1 asked the extent to which existing federal criminal justice information systems are used by state and local departments. Research question #2 asked about user perceptions regarding the usefulness of federal criminal justice information systems in accomplishing LE missions at the state and local levels. The first two survey questions were specifically geared to answer these research questions. These survey items asked respondents to rate how frequently they accessed 22 federal criminal justice information systems and then rate how useful those systems were toward accomplishing

LE missions. Both questions relied on a five-point Likert scale on which participants rated frequency of use from "never" (1) to "constantly" (5) and rated usefulness from "not useful at all" (1) to "extremely useful" (5). The results of these questions are presented in Table 19.

System	Freq Mean	Freq Std. Dev.	Use Mean	Use Std. Dev.	Combined Score	Kendall's Tau
NCIC Net	4.280	0.984	4.340	0.808	18.575	45.391
NLETS	2.610	1.576	2.840	1.487	7.412	44.279
UCR/NIBRS	2.410	1.718	2.280	1.360	5.495	48.601
NICS	2.250	1.353	2.370	1.240	5.333	43.761
LE websites	2.110	0.816	2.130	1.040	4.494	40.250
IAFIS	1.750	1.212	2.040	1.544	3.570	19.943
III	1.630	1.325	1.740	1.456	2.836	12.842
LEO	1.280	0.797	1.420	1.109	1.818	8.451
CODIS	1.140	0.459	1.260	0.844	1.436	6.808
CJIS WAN	1.070	0.264	1.140	0.500	1.220	5.735
NDPIX	1.100	0.379	1.090	0.383	1.199	5.285
RISS	1.050	0.299	1.120	0.603	1.176	3.974
IDENT-INS	1.040	0.221	1.090	0.489	1.134	3.642
NIBIN	1.060	0.245	1.060	0.229	1.124	4.888
JABS	1.040	0.251	1.060	0.494	1.102	2.516
FinCen	1.050	0.224	1.040	0.187	1.092	3.640
OLES	1.040	0.255	1.040	0.261	1.082	3.301
AGILE	1.000	0.000	1.070	0.448	1.070	0.000
CWIN	1.030	0.234	1.030	0.240	1.061	2.284
GCJIN	1.020	0.157	1.030	0.311	1.051	2.034
PSWN	1.020	0.138	1.020	0.148	1.040	2.726
NIPC	1.010	0.091	1.020	0.229	1.030	1.754

Table 19: Federal Criminal Justice Information Systems Ranked by Combined Score (Frequency of Use x Perceived Usefulness)

The means of the results for each question are presented in the second and fourth columns. "Frequency Mean" presents the overall mean for responses to Q1, which asked respondents to record how frequently they used each system. "Usefulness Mean"

presents the overall mean for responses to Q2, which asked respondents to record how useful they perceived the system was toward accomplishing LE missions.

Table 19 also shows the 22 systems in a ranked order. The systems were ranked by analyzing means of frequency of use/perceived usefulness characteristics. The 22 systems studied in this research for frequency of use and perceived usefulness were ranked by a combined frequency of use/perceived usefulness score. The combined score was calculated by multiplying the mean frequency of use for each system by the corresponding mean perceived usefulness. Higher means indicated a greater frequency of use and higher degree of usefulness; therefore, systems were ranked based on the mean scores of these two characteristics. The combined frequency of use/perceived usefulness score is shown in the sixth column, labeled "combined score."

As the table shows, National Crime Information Center Network (NCIC Net) outscored all other systems by a wide margin. Rounding out the top five, in order, were the National Law Enforcement Telecommunications System (NLETS), Uniform Crime Reporting/National Incident-Based Reporting System (UCR/NIBRS), National Instant Criminal Background Check System (NICS), and federal LE websites. The bottom five systems included Cyber Warning Information Network (CWIN), Global Criminal Justice Information Network (GCJIN), Advanced Generation for Interoperability in Law Enforcement (AGILE), Public Safety Wireless Network (PSWN), and National Infrastructure Protection Center (NIPC).

The previous method, however, does not take into account the standard deviation of responses. Therefore, systems were also ranked via Kendall's tau. Kendall's tau is a nonparametric measure of association. Its value indicates the strength of a relationship

with larger values indicating stronger relationships (Shannon et al, 2001). "Kendall's tau is used when all variables involved are ordinal, which means they have direction or order, such as age or education" (Smith, 2001). Table 20 shows combined score and Kendall's tau ranking values for each of the 22 systems.

System	Combined Score Rank	Kendall's Tau Rank
NCIC Net	1	2
NLETS	2	3
UCR/NIBRS	3	1
NICS	4	4
LE websites	5	5
IAFIS	6	6
III	7	7
LEO	8	8
CODIS	9	9
CJIS WAN	10	10
NDPIX	11	11
RISS	12	13
IDENT-INS	13	14
NIBIN	14	12
JABS	15	18
FinCen	16	15
OLES	17	16
AGILE	18	22
CWIN	19	19
GCJIN	20	20
PSWN	21	17
NIPC	22	21

Table 20: Federal CJIS Rank Comparison (Combined Score vs. Kendall's Tau)

As shown by Table 20, the combined score and Kendall's tau rankings do not completely agree, primarily because Kendall's tau takes standard deviation into account and the combined score does not. The differences between ranking systems are minor.

The high and low scoring information systems do not change using either ranking system, though the exact order of these two groups of systems would change between ranking methods. In total, either ranking method is statistically sound and produces valid ranking results; however, this research used the combined scores as the primary ranking scheme.

Comparisons of Sample Population Subsets.

Demographics were collected in order to compare responses between subsets of the sample population to determine if responses to survey items pertaining to each research question differed significantly. This section presents the results of those comparisons of segments of the sample population with respect to research questions #1 and #2. These comparisons do not contribute to directly answering the research questions, but merely demonstrate differences or similarities in responses between subsets of the sample population. Two demographics were collected specifically to study whether segments of the sample population differed significantly. These demographics include years of service and membership in particular professional organizations.

Comparison Based on Years of Service.

The average years of service among respondents in the sample population was nine years and eight months. Of the total responses, 161 respondents fell above and 211 fell below the average. This section will examine whether there is a significant difference in the responses of respondents who fell above and respondents who fell below the average years of experience.

This comparison was made using a z statistic which compares the means of two sample populations. Since both subsets of the population are relatively large (over 30), the Central Limit Theorem can be invoked. At $a = .05$, $z_a = 1.645$. Therefore, in

comparing the sample populations, any z statistic greater than 1.645 indicates a statistically significant difference in responses from subsets of the population differing in years of service. Tables 21 and 22 show the results of independent sampling tests of these subsets of the sample population. Bolded values indicate a z statistic greater than the 1.645 threshold.

	Total Response Mean	**High Service Time Mean**	**Low Service Time Mean**	**z statistic**
AGILE	1.00	1.00	1.00	0.000
PSWN	1.02	1.03	1.01	1.285
OLES	1.04	1.05	1.04	0.361
GCJIN	1.02	1.01	1.02	0.640
RISS	1.05	1.01	1.08	**2.537**
JABS	1.04	1.03	1.04	0.376
INDENT	1.04	1.06	1.02	1.547
NIPC	1.01	1.02	1.00	**1.750**
UCR/NIBRS	2.41	2.59	2.29	1.627
LEO	1.28	1.23	1.31	0.970
NICS	2.11	2.19	2.05	0.961
NIBIN	1.06	1.05	1.08	1.189
CODIS	1.14	1.19	1.11	1.579
IAFIS	1.75	1.71	1.79	0.625
III	1.63	1.61	1.64	0.210
CJIS WAN	1.07	1.07	1.08	0.360
NCIC Net	4.28	4.32	4.24	0.775
FinCEN	1.05	1.06	1.05	0.410
NLETS	2.61	2.52	2.67	0.892
NDPIX	1.10	1.10	1.10	0.000
CWIN	1.03	1.03	1.03	0.000
LE websites	2.25	2.21	2.27	0.700
				za=1.645

Table 21: High/Low Service Time Mean Test Results for Q1

	Total Responses Mean	High Service Time Mean	Low Service Time Mean	z statistic
AGILE	1.07	1.05	1.09	0.893
PSWN	1.02	1.03	1.02	0.615
OLES	1.04	1.03	1.05	0.753
GCJIN	1.03	1.01	1.05	1.405
RISS	1.12	1.03	1.19	**2.825**
JABS	1.06	1.05	1.07	0.386
INDENT	1.09	1.12	1.07	0.912
NIPC	1.02	1.04	1.00	1.400
UCR/NIBRS	2.28	2.40	2.19	1.444
LEO	1.42	1.36	1.46	0.860
NICS	2.13	2.19	2.10	0.675
NIBIN	1.06	1.04	1.07	1.272
CODIS	1.26	1.34	1.21	1.409
IAFIS	2.04	2.00	2.07	0.427
III	1.74	1.69	1.78	0.578
CJIS WAN	1.14	1.13	1.15	0.382
NCIC Net	4.34	4.39	4.30	1.073
FinCEN	1.04	1.04	1.03	0.492
NLETS	2.84	2.77	2.90	0.811
NDPIX	1.09	1.11	1.09	0.474
CWIN	1.03	1.03	1.03	0.000
LE websites	2.37	2.50	2.28	**2.002**
				za=1.645

Table 22: High/Low Service Time Mean Test Results for Q2

As the tables show, the responses from these subsets of the sample population did not differ significantly, as only four of the 44 items differed at a statistically significant level. Based on this, regardless of service time, participants responded similarly to survey items in Q1 and Q2.

Comparison Based on Professional Organization.

Most respondents to this survey belonged to the Fraternal Order of Police: 340 out of 360 total responses. Sixteen of the remaining respondents belonged to the

International Association of Chiefs of Police. This section will examine whether there are significant differences in responses of FOP and IACP respondents.

	Total Responses Mean	FOP Mean	IACP Mean	t-value
AGILE	1.00	1.00	1.00	0.000
PSWN	1.02	1.01	1.25	**216.647**
OLES	1.04	1.03	1.44	**107.248**
GCJIN	1.02	1.01	1.31	**217.947**
RISS	1.05	1.04	1.38	**60.730**
JABS	1.04	1.01	1.50	**140.091**
INDENT	1.04	1.04	1.00	**12.387**
NIPC	1.01	1.01	1.00	**18.549**
UCR/NIBRS	2.41	2.43	1.94	**2.533**
LEO	1.28	1.26	1.75	**11.854**
NICS	2.11	2.12	2.12	0.000
NIBIN	1.06	1.06	1.13	**17.658**
CODIS	1.14	1.14	1.13	0.556
IAFIS	1.75	1.74	2.13	**4.074**
III	1.63	1.61	1.94	**2.871**
CJIS WAN	1.07	1.07	1.25	**39.702**
NCIC Net	4.28	4.28	4.00	**4.400**
FinCEN	1.05	1.04	1.31	**86.595**
NLETS	2.61	2.59	2.94	**2.160**
NDPIX	1.10	1.09	1.25	**16.910**
CWIN	1.03	1.01	1.38	**113.205**
LE websites	2.25	2.22	2.81	**13.701**
				ta=1.649

Table 23: FOP/IACP Mean Test Results for Q1

This comparison was made using a t test which compares the means of two sample populations. The t test was used in this comparison because the IACP subset of the sample population contains only 16 entries. Because this number does not exceed the threshold for invoking the CLT, the z statistic method used previously would not produce valid results. However, the t test is designed to compare population means when the size of one or both of the subpopulations does not exceed the CLT threshold. Tables 23 and 24 show the results of t tests of these subsets of the sample population.

	Total Responses Mean	FOP Mean	IACP Mean	t-value
AGILE	1.07	1.04	1.69	**53.455**
PSWN	1.02	1.01	1.25	**186.768**
OLES	1.04	1.03	1.38	**83.915**
GCJIN	1.03	1.02	1.31	**47.030**
RISS	1.12	1.10	1.56	**19.559**
JABS	1.06	1.04	1.50	**29.476**
INDENT	1.09	1.09	1.13	**2.522**
NIPC	1.02	1.02	1.06	**11.466**
UCR/NIBRS	2.28	2.29	1.94	**2.890**
LEO	1.42	1.41	1.75	**4.192**
NICS	2.13	2.15	1.94	**2.079**
NIBIN	1.06	1.06	1.06	0.000
CODIS	1.26	1.26	1.19	1.498
IAFIS	2.04	2.03	2.37	**2.173**
III	1.74	1.71	2.38	**4.855**
CJIS WAN	1.14	1.13	1.50	**22.861**
NCIC Net	4.34	4.36	3.88	**11.308**
FinCEN	1.04	1.03	1.25	**100.988**
NLETS	2.84	2.82	3.25	**2.988**
NDPIX	1.09	1.09	1.31	**22.949**
CWIN	1.03	1.01	1.44	**130.132**
LE websites	2.37	2.36	2.50	**1.969**
				ta =1.649

Table 24: FOP/IACP Mean Test Results for Q2

At a = .05, ta = 1.649. Therefore, in comparing the sample populations, any t value greater than 1.649 indicates a statistically significant difference in responses from subsets of the population differing in years of service. Bolded values indicate a t value greater than the 1.649 threshold.

The results indicated there were far more significant differences in the responses of subsets of the sample population broken out by professional organization than differences in responses of subsets of the sample population broken out by years of service. Only five of the forty-four items on the survey did not differ at a statistically

significant level between these two subsets of the sample population. Based on this information, participants who belonged to FOP responded to survey items in Q1 and Q2 in a very different manner than participants who belonged to IACP.

Research Question 3: Access and Trust Constructs.

The following sections present results which help to answer research question #3. Research question #3 asked about state and local LE "user" perceptions regarding the environmental factors that may affect criminal justice information system usage and information sharing between federal and state/local LE levels.

Access Construct.

The next six survey questions (Q3-Q8) were designed to measure the IS environmental factor called access. Respondents were asked to rate how much they agreed or disagreed with statements about their abilities to access information on federal criminal justice information systems.

Each question relied on a five-point Likert scale on which participants rated their agreement with the statement from "completely disagree" (1) to "completely agree" (5). A comparison was made between the expected mean and the observed mean using a z statistic, which compares an observed mean with an expected mean. The middle value of the Likert scale (3) was used as the expected mean. Because the range of answers is discrete and not continuous, a z-statistic can be used only if it can be shown that the distribution of the z statistic possesses nearly the same shape as the theoretical t distribution for populations that are nonnormal—in other words, the probability distribution must be mound-shaped if not normally distributed. This is especially true for Likert scale questions, since a Likert scale question with only 5 possible answers cannot

possibly possess a normal probability distribution. Therefore, results of these z-tests can not be used for hard scientific proof, but indications of trends in the data (Shannon et al, 2001). A frequency analysis of the results showed that the probability distribution is, in fact, mound-shaped. Table 25 shows an example of a frequency analysis on Q3. As the figure shows, responses to this question were mound-shaped. All other survey items showed similar results.

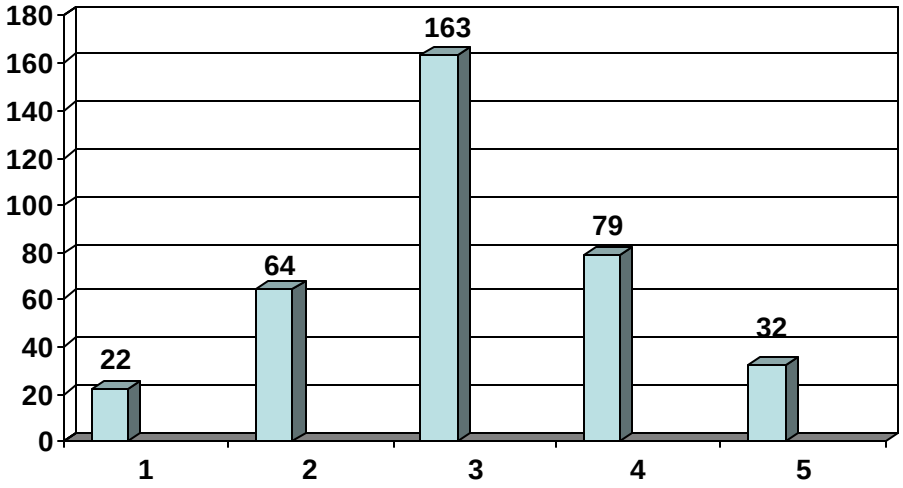

Table 25: Frequency Analysis of Q3

Since the population is relatively large (over 30), the Central Limit Theorem (CLT) can be invoked. At a = .05, za = 1.645. Therefore, in comparing the sample populations, any z statistic greater than 1.645 indicates a statistically significant difference in sample population responses from the expected mean. Table 26, showing the results of the survey, also indicates the results of the independent sampling tests. Bolded values indicate a z statistic greater than the 1.645 threshold.

	Mean	Std. Deviation	Z Statistic
Q3	3.11	.994	1.345
Q4	3.00	.975	0.136
Q5	2.78	.889	**3.271**
Q6	3.03	.952	0.412
Q7	2.78	.833	**3.215**
Q8	3.06	.950	0.824

Table 26: Results of Questions Supporting Access Construct

Because the observed mean falls outside the expected probability distribution, a statistically high or low mean suggests the item is perceived to be a problem area for state and local LE personnel relating to access to federal criminal justice information systems. In other words, given a standard deviation of .889 for Q5 (or .833 for Q7), a mean of 2.78 falls statistically significantly outside the expected mean range. This means that the observed means for these items are statistically significantly lower than the expected mean, suggesting that these two access items are a concern for state and local LE personnel with respect to federal criminal justice information systems. These items measured access to classified case-related information and whether federal agencies took state/local LE organization's IT capabilities into account. Since these observed means were statistically significantly lower than the expected means, the results indicate that state/local LE personnel perceive that they do not have adequate access to classified case-related information and also perceive that federal LE agencies do not take their organization's IT capabilities into account.

Trust Construct.

The final eight survey questions (Q19-Q26) were designed to measure the IS environmental factor called trust. Respondents were asked to rate how much they agreed or disagreed with statements about how much they trust federal LE information sources.

Each question relied on a five-point Likert scale on which participants rated their agreement with the statement from "completely disagree" (1) to "completely agree" (5). The results of these questions are presented in Table 27. The same z-test was conducted here as with Q3-8.

	Mean	Std. Deviation	Z Statistic
Q19	3.06	.872	0.858
Q20	2.93	.890	0.992
Q21	3.52	.870	**7.444**
Q22	3.66	.966	**9.007**
Q23	3.59	.958	**8.084**
Q24	3.33	1.050	**4.318**
Q25	2.91	.846	1.304
Q26	2.84	.800	**2.371**

Table 27: Results of Questions Supporting Trust Construct

Because the observed mean falls outside the expected probability distribution, a statistically high or low mean suggests the item is perceived to be a problem area for state and local LE personnel relating to trust in federal LE information sources. The observed means for Q21, Q22, Q23, and Q24 are statistically significantly higher than the expected mean while Q26 is statistically significantly lower than the expected mean. This suggests that these items supporting the trust construct are concerns for state and local LE personnel with respect to federal criminal justice information systems. Q21 measured how much state/local LE personnel trust the information gained from federal sources. The statistically high observed mean for this question suggests that state/local LE personnel perceive information gained from federal sources to be trustworthy. Q22-24 measured how much state/local LE officials trust the capabilities of federal LE agencies to gather intelligence and react to emerging, critical threats within the U.S. The

statistically high observed means for these questions suggest that state/local LE personnel perceive that federal LE agencies are adequately capable of gathering intelligence and reacting to emerging, critical threats within the U.S. Q26 measured how responsive to feedback federal agencies were perceived to be by state/local LE personnel. The statistically low observed mean for this question suggests that state/local LE personnel perceive federal LE agencies to be unresponsive to feedback from their organizations.

Comparisons of Sample Population Subsets.

Demographics were collected in order to compare responses between subsets of the sample population to determine if responses to survey items pertaining to each research question differed significantly. This section presents the results of those comparisons of segments of the sample population with respect to research question #3. These comparisons do not contribute to directly answering the research questions, but merely demonstrate differences or similarities in responses between subsets of the sample population. Two demographics were collected specifically to study whether segments of the sample population differed significantly. These demographics include years of service and membership in particular professional organizations.

Comparison Based on Years of Service.

The average years of service among respondents in the sample population was nine years and eight months. Of the total responses, 161 respondents fell above and 211 fell below the average. This section examines whether there is a significant difference in the responses of respondents who fell above from those who fell below that average.

This comparison was made using a z statistic which compares the means of two sample populations. Since both subsets of the population are relatively large (over 30),

the Central Limit Theorem can be invoked. At a = .05, za = 1.645. Therefore, in comparing the sample populations, any z value greater than 1.645 indicates a statistically significant difference in responses from subsets of the population. Tables 28 and 29 show the results of independent sampling tests of these subsets of the sample population. Any bolded values indicate a z statistic greater than the 1.645 threshold.

	Total Responses Mean	**High Service Time Mean**	**Low Service Time Mean**	**z statistic**
Q3	3.10	3.08	3.11	0.280
Q4	2.99	2.92	3.05	1.233
Q5	2.77	2.72	2.80	0.837
Q6	3.03	3.09	2.98	1.065
Q7	2.78	2.80	2.76	0.436
Q8	3.06	3.07	3.04	0.285
				za =1.645

Table 28: High/Low Service Time Mean Test Results for Q3-Q8

	Total Responses Mean	**High Service Time Mean**	**Low Service Time Mean**	**z statistic**
Q19	3.06	2.99	3.10	1.157
Q20	2.93	2.93	2.94	0.104
Q21	3.52	3.43	3.59	**1.737**
Q22	3.66	3.74	3.60	1.382
Q23	3.59	3.67	3.53	1.401
Q24	3.33	3.43	3.26	1.524
Q25	2.91	2.89	2.93	0.425
Q26	2.84	2.85	2.84	0.115
				za =1.645

Table 29: High/Low Service Time Mean Test Results for Q19-Q26

As the tables show, the responses from these subsets of the sample population did not differ significantly. Only one of the fourteen items differed at a statistically

significant level between these two subsets of the sample population. Based on this information, regardless of service time, participants responded to survey items in Q3-8 and Q19-26 in a very similar manner. Therefore, responses to questions relating to the IS environmental factors (research question #3) did not differ significantly by service time.

Comparison Based on Professional Organization.

Membership in particular professional organizations was also collected in the demographics. Most of the respondents to this survey belonged to the Fraternal Order of Police (FOP): 340 out of 360 total responses. Sixteen of the remaining respondents belonged to the International Association of Chiefs of Police. This section will examine whether there are significant differences in responses of FOP and IACP respondents.

This comparison was made using a t test which compares the means of two sample populations. The t test was used in this comparison because the IACP subset of the sample population contains only 16 entries. Because this number does not exceed the threshold for invoking the CLT, the z statistic method used previously would not produce valid results. However, the t test is designed to compare population means when the size of one or both of the subpopulations does not exceed the CLT threshold. At a = .05, ta = 1.649. Therefore, in comparing the sample populations, any t value greater than 1.649 indicates a statistically significant difference in responses from subsets of the population differing in years of service. Tables 30 and 31 show the results of t tests of these subsets of the sample population. Bolded values indicate a t value greater than the 1.649 threshold.

	Total Responses Mean	FOP Mean	IACP Mean	t-value
Q3	3.10	3.12	2.94	**2.824**
Q4	2.99	3.01	3.00	0.162
Q5	2.77	2.76	2.94	**3.543**
Q6	3.03	3.03	3.19	**2.693**
Q7	2.78	2.78	2.75	0.667
Q8	3.06	3.06	3.00	1.003
				ta =1.649

Table 30: FOP/IACP Mean Test Results for Q3-Q8

	Total Responses Mean	FOP Mean	IACP Mean	t-value
Q19	3.06	3.04	3.38	**6.933**
Q20	2.93	2.93	3.13	**3.876**
Q21	3.52	3.52	3.25	**5.455**
Q22	3.66	3.65	3.63	0.326
Q23	3.59	3.59	3.50	1.500
Q24	3.33	3.34	3.13	**2.943**
Q25	2.91	2.91	2.88	0.651
Q26	2.84	2.84	3.00	**3.860**
				ta =1.649

Table 31: FOP/IACP Mean Test Results for Q19-Q26

The results indicated there were more significant differences in the responses of subsets of the sample population broken out by professional organization than differences in responses of subsets of the sample population broken out by years of service. Eight of the fourteen items relating to IS environmental factors differed at a statistically significant level between these two subsets of the sample population. Based on this information, participants who belonged to FOP responded to survey items in Q3-8 and Q19-26 in a different manner than participants who belonged to IACP for over half the

items. Therefore, responses to questions relating to the IS environmental factors (research question #3) differed by membership in professional organization.

Comparison of Sample Population Based on Response Method

Two different response formats were offered during this survey: a web-based format and a mail-out version send only to CIOs of state bureaus of investigation. Most of the participants in this survey responded via the web-based format: 360 out of 372 total responses. The six remaining participants were CIOs who responded via the mail-out format. This section will examine whether there are significant differences in responses based on the response format.

This comparison was made using a t test which compares the means of two sample populations. The t test was used in this comparison because the mail-out participant subset of the sample population contains only six entries. Because this number does not exceed the threshold for invoking the CLT, the z statistic method used previously would not produce valid results. However, the t test is designed to compare population means when the size of one or both of the subpopulations does not exceed the CLT threshold.

At a = .05, ta = 1.649. Therefore, in comparing the sample populations, any t value greater than 1.649 indicates a statistically significant difference in responses from subsets of the population differing in response format. Tables 32-35 show the results of the independent sampling tests of these subsets of the sample population. Bolded values indicate a t value greater than the 1.649 threshold.

The results indicated there were significant differences in the responses of subsets of the sample population broken out response format. Only seven of the fifty-eight items

on the survey did not differ at a statistically significant level between these two subsets of the sample population. Based on this information, participants who responded via the mail-out format answered survey items in a very different manner than participants who responded via the web-based version.

	Total Responses Mean	Web-based Response Mean	Mail-out Response Mean	t statistic
AGILE	1.00	1.00	1.17	**192.773**
PSWN	1.02	1.02	1.67	**115.964**
OLES	1.04	1.04	1.00	**3.681**
GCJIN	1.02	1.02	1.00	**4.855**
RISS	1.05	1.05	2.75	**44.524**
JABS	1.04	1.04	1.00	**3.799**
IDENT	1.04	1.04	1.00	**4.901**
NIPC	1.01	1.01	1.67	**202.337**
UCR/NIBRS	2.41	2.41	2.75	1.347
LEO	1.28	1.28	3.25	**35.163**
NICS	2.11	2.11	3.58	**9.220**
NIBIN	1.06	1.06	1.42	**53.882**
CODIS	1.14	1.14	1.58	**20.298**
IAFIS	1.75	1.75	3.33	**12.053**
III	1.63	1.63	3.83	**14.390**
CJIS WAN	1.07	1.07	3.67	**196.807**
NCIC Net	4.28	4.28	4.75	**5.771**
FinCEN	1.05	1.05	1.92	**94.261**
NLETS	2.61	2.61	4.75	**10.284**
NDPIX	1.10	1.10	2.25	**66.250**
CWIN	1.03	1.03	1.33	**52.651**
LE websites	2.25	2.25	3.25	**17.210**
				ta=1.649

Table 32: Web-Based vs. Mail-out Response Mean Test Results for Q1

	Total Responses Mean	Web-based Response Mean	Mail-out Response Mean	t statistic
AGILE	1.07	1.07	1.25	**9.596**
PSWN	1.02	1.02	1.83	**123.378**
OLES	1.04	1.04	1.17	**19.775**
GCJIN	1.03	1.03	1.00	**1.856**
RISS	1.12	1.12	2.92	**48.202**
JABS	1.06	1.06	1.00	1.471
IDENT	1.09	1.09	1.17	**3.835**
NIPC	1.02	1.02	1.83	**112.625**
UCR/NIBRS	2.28	2.28	2.58	**1.903**
LEO	1.42	1.42	3.25	**17.311**
NICS	2.13	2.13	3.58	**10.744**
NIBIN	1.06	1.06	1.50	**62.583**
CODIS	1.26	1.26	1.58	**5.070**
IAFIS	2.04	2.04	3.25	**5.874**
III	1.74	1.74	3.92	**11.935**
CJIS WAN	1.14	1.14	3.58	**86.128**
NCIC Net	4.34	4.34	4.75	**7.442**
FinCEN	1.04	1.04	2.75	**160.030**
NLETS	2.84	2.84	4.42	**8.388**
NDPIX	1.09	1.09	2.17	**60.142**
CWIN	1.03	1.03	1.67	**40.423**
LE websites	2.37	2.37	3.17	**8.585**
				ta =1.649

Table 33: Web-Based vs. Mail-out Response Mean Test Results for Q2

It is important to take into consideration that there may be more than one variable affecting the differences in responses between those who responded via the mail-out version and those who responded via the web-based version. Recall from Chapter 3 that the portion of the sample population that received the mail-out version of the survey were the CIOs of state bureaus of investigation, a portion of the total LE population specifically attuned to CJIS issues; whereas, the portion of the sample population receiving the web-based version of the survey were not specifically IS professionals—rather, those who received the web-based version were general users of federal criminal

justice information systems. This variable could account for some of the variation in responses between these two subsets of the sample population; however, it's difficult, if not impossible, to measure how much of the total variation is accounted for by this variable and how much of the total variation is accounted for due to differences in responses influenced by the mail-out format versus the web-based format. Therefore, the results of this comparison are influenced by more than one particular variable: the difference between survey formats and inferences based on these statistics can not be completely reliable.

	Total Responses Mean	**Web-base Response Mean**	**Mail-Out Response Mean**	**t statistic**
Q3	3.10	3.10	3.75	**7.761**
Q4	2.99	2.99	3.08	1.095
Q5	2.77	2.77	2.83	0.865
Q6	3.03	3.03	2.92	1.398
Q7	2.78	2.78	2.75	0.498
Q8	3.06	3.06	3.42	**4.604**
				ta =1.649

Table 34: Web-Based vs. Mail-out Response Mean Test Results for Q3-8

	Total Responses Mean	**Web-based Response Mean**	**Mail-out Response Mean**	**t statistic**
Q19	3.06	3.06	2.92	**2.131**
Q20	2.93	2.93	3.00	1.021
Q21	3.52	3.52	3.75	**3.579**
Q22	3.66	3.66	3.25	**5.097**
Q23	3.59	3.59	3.25	**4.295**
Q24	3.33	3.33	3.08	**2.679**
Q25	2.91	2.91	3.25	**5.589**
Q26	2.84	2.84	3.00	**2.863**
				ta =1.649

Table 35: Web-Based vs. Mail-out Response Mean Test Results for Q19-26

Summary

This chapter presented the findings and analysis for this research. The response rate to the survey instrument was discussed. Next, the demographics collected at the beginning of the survey instrument were analyzed to describe characteristics of the sample population. The results of the survey were then presented, highlighting statistically significant deviations from the expected mean. Finally, a comparative analysis of two subsets of the sample population was presented to determine if responses from these subsets differed significantly. The next chapter presents the conclusions obtained from the results of this research.

V. Conclusions

Introduction

This final chapter reviews conclusions about the findings in the previous chapter including additional findings of the research, management implications based on the results presented in this research, limitations of this research effort, and suggestions for future research in this area.

Conclusions

NCIC Net, NLETS, UCR/NIBRS, NICS, LE websites, and IAFIS scored high on the frequency of use/perceived usefulness scale. This suggests that state/local LE personnel utilize these systems on a fairly regular basis and perceive the systems to be useful toward accomplishing LE missions. The bottom five systems, including CWIN, GCJIN, AGILE, PSWN, and NIPC, scored poorly on the combined scale. This would indicate that these systems are not used very much at all at the state and local levels and/or their information is perceived to provide little value to the accomplishment of LE missions.

Of the four IS environmental factors studied in this research, all were deemed to be influential in some way. Of the six items under the IS environmental factor called access, two items were identified as statistically significant toward detracting state/local LE personnel from utilizing federal criminal justice information systems. The inaccessibility of classified information to complete LE missions was identified as a major detractor for state/local LE personnel. Additionally, state/local LE officials perceive that federal agencies do not adequately take their department's capabilities into

account when fielding criminal justice information systems, a factor that significantly influences whether state/local LE personnel will use or be able to use the system.

Finally, four of the eight items under the IS environmental factor called trust were ascertained to be statistically significant. In general, respondents indicated a high degree of trust in federal LE agencies to gather effective intelligence about emerging threats and to react to those identified threats. Respondents also specified a high degree of trust in the information received from federal LE agencies. Q21 asked respondents to rate how much they trust information received from federal LE agencies. Q22 asked respondents to rate how much they trusted federal LE capabilities to gather effective intelligence about emerging threats. Q23 asked respondents to rate how much they trusted federal LE capabilities to react to emerging, critical situations. Each question scored significantly higher than other items in this section. Based on these results, it could be inferred there is a high degree of trust among state/local LE personnel in federal LE agencies to carry out LE missions. These indications of high trust were mitigated by a strong suggestion that federal LE agencies are unreceptive to feedback from state and local LE agencies. Q26 asked respondents to rate how responsive federal LE agencies were to feedback from their departments. Since this statistic was significantly lower than the expected mean, it could be inferred that state/local LE personnel perceive federal LE agencies as indifferent toward feedback from the state/local tiers of the LE community.

Management Implications

In reaction to shocking events such as the Columbine High School shooting, terrorist attacks of 9/11, and the D.C. sniper shootings, federal LE agencies are sharing information on an unprecedented scale. Two important realizations may be positively

impacting the amount of access federal LE agencies grant to state and local LE personnel. One of these realizations is that information is an extremely valuable weapon in combating crime. New capabilities such as DNA testing and forensic entomology show just how powerful a little information in the hands of the criminologist can be toward identifying a perpetrator and proving that perpetrator's guilt beyond a shadow of a doubt. The second realization centers on how much federal LE agencies rely on state/local personnel to complete LE missions. A poignant example of this reliance is how much the INS relies on state/local LE personnel to identify illegal aliens. Given the small number of INS agents in each state, it's more likely that a state or local LE official will encounter the illegal alien before the INS does. Obviously, it would be advantageous for the INS to cooperate with state/local LE agencies. However, to take advantage of this reliance, the INS must first share information about the identities of known illegal aliens.

Despite the number of references in the literature review suggesting that information technology in the federal LE sector is obsolete, respondents to the survey did not identify technology as a significant issue (Q10). While information technology at the federal level may indeed be behind current capabilities, the level of technology at the state and local levels is equally poor. Thus, the obsolescence of information technology has gone relatively unnoticed, from a mission-capability perspective. For instance, the majority of police work is done in the field. Forensics are collected at the crime scene and examined in the lab. Patrol officers spend much of their duty day in a vehicle, not behind a desk. Quite frankly, the reliance on information technology that has been evident in other fields may not have permeated the LE community quite yet. If this is so, the obsolescence of information technology in the federal sector would be a minor issue.

This perspective may be supported by the results of Q12 (which correlated well with Q10 in the factor analysis), where respondents indicated a stronger reliance on interpersonal contact with federal LE agencies over electronic systems.

Recommendations

As stated at the beginning of this thesis, the federal government expends a great deal of money on networks; however, little planning has been given to whether these expensive systems will be able to exchange information with other related, federally developed systems. Compounding that situation, even less thought has been given as to how these systems will communicate with state and locally run LE information systems, where the information may be required to carry out public safety missions.

The increasing complexity of public safety threats has compounded the need for criminal justice information at all levels of the LE community. Consequently, federal LE agencies should continue to develop information-sharing tools and encourage an open information-sharing culture in order to distribute vital criminal justice information and support public safety missions at the state and local levels.

Additionally, shrinking budgets at all levels of government have made resource allocation a primary issue. Based on information presented in the research, government organizations feel an increasing need for interdependency among other agencies (Prout, 2002; Mueller, June 2002; Canterbury, 2002). The FBI, INS, Drug Enforcement Administration (DEA) and other federal law enforcement agencies continue to rely on each other to cover the myriad of law enforcement challenges facing the US. Many of these challenges cross organizational boundaries: border control, drug interdiction, and intelligence gathering, among others. Federal agencies are seeking to reduce duplication

of effort in order to conserve resources and make the most of capabilities. This effort is slowly bringing to light a greater dependence on collaborative efforts with state and local agencies to improve mission effectiveness (Public Safety Wireless Networks, 2002; AGILE, 2002). Enabling collaborative efforts with state and local agencies implies that enhanced access to federal information systems will eventually need to be granted to state and local agencies. Likewise, information systems developed at the state and local levels should be capable of communicating with federal information systems.

The prevailing attitudes toward sharing information may be changing in the federal tier of the LE community. As the D.C. sniper case demonstrated, federal LE agencies are willing to consider sharing vital information with state/local LE organizations in dire situations. However, information sharing continues to be a problem for the LE community on the whole. Open information sharing practices should be adopted outside of large-scale incidents such as the Columbine High School shooting, Murrah Federal Building bombing, and 9/11 terrorist attacks with the goal of detecting and, consequently, preventing further tragedies through collaborative LE operations and intelligence analysis. Success in this arena depends on the ability to share information among agencies that may reasonably play a part in detecting and/or preventing the situation.

As with the III program, interoperability must be planned into the development of information-sharing tools. Interoperability must also be introduced into contingency plans—developed cooperatively among the three tiers of government. This implies a shift away from the territorial mindset that exists today toward a more collaborative environment where personnel, equipment, information, and other resources are more

openly shared between federal, state, and local law enforcement organizations that share a similar goal: the protection of the people.

Limitations of Research

Every research effort has its limitations. The following limitations of this research effort are noted. As noted in Chapter 3, self-selection of survey respondents to complete the survey introduces some bias into the results. An additional limitation was the non-probability aspect of the sampling methodology. While the survey did not randomly select participants, the distribution methodology described in Chapter 3 was intended to minimize any systematic effect introduced by the sampling method. While this may not be optimal, the survey methodology was deemed valid, given the permission-based constraints of gaining full distribution—or any distribution, for that matter. These factors do not invalidate the findings of this research, however, may constrain the generalizability of the results to the entire LE population (GVU, 1994). One final limitation with the distribution of the survey was the method of distribution. The researcher relied on POCs within the LE professional organizations to distribute the survey via email. These POCs reported that they distributed the survey as agreed upon, and the researcher held great confidence that this had been accomplished; however, it cannot be conclusively demonstrated that all the POCs distributed the survey as planned.

The survey design introduced some limitations as well. As noted in Chapter 3, the mixed methodology for the survey's distribution provides limitations as well. Using a mixed method approach has been shown to influence research results. Several studies have found that response rates for web-based surveys tend to be lower than mail-out surveys (Manfreda et al, 2001; Gonier, 1999; Kwak et al, 1999). Manfreda et al cite "low

preference for the web mode" (2001) as a possible contributing factor. Countering this limitation is the fact that such a small portion of our population will receive the mailed survey (50 out of 15,000). Additionally, studies have indicated that there may be statistically significant substantive and data quality differences (e.g. non-response rates for closed ended questions) between the two methods that may impact research results (Manfreda et al, 2001; Gonier, 1999). A comparison was conducted between responses from the mail-out format versus responses from the web-based version, and the responses were found to be statistically significantly different. However, it is important to consider that more than one variable influenced the differences in responses. Not only were responses recorded from different formats, but each format was distributed to dynamically different subsets of the total population: the mail-out version went to LE CJIS professionals while the web-based version was sent to general LE users of federal CJIS. This additional variable could account for a significant portion of the variance in responses; however, the exact amounts of variance accounted for by each variable are difficult, if not impossible to measure.

Additionally, pilot test reliability results showed that survey items supporting the system quality and information quality constructs did not correlate well. This problem was not addressed before the final implementation of the survey instrument, resulting in coefficient alphas that did not meet the minimum standard of .7 to provide statistically reliable conclusions about these constructs. Consequently, the system quality and information quality constructs were discarded from the final analysis.

The researcher introduced another limitation associated with the pilot test. Though reliability test results clearly indicated aforementioned problems with the

systems quality and information quality constructs, the researcher did not correct these problems prior to the survey's final application. As mentioned in Chapter 4, this oversight in the survey's application was due to time constraints and lack of experience of the researcher.

One final limitation involved the collection of demographics. When constructing the question collecting primary duty description, five choices were given to survey participants: patrol, investigator, supervisor, administrator, and other. It was expected that the number of respondents choosing "other" would be relatively low compared to the other responses; however, the number of participants choosing "other" nearly equaled the numbers of participants who chose "investigator" or "supervisor." This increased the influence of "other" respondents in the survey results and introduced a question about who fell into the "other" category. Because respondents who chose the "other" option were not asked to provide an alternate duty description, the nature of these respondents could not be ascertained. Along these lines, it is unknown how the four respondents who answered neither for the professional organization demographic received the survey, since the survey was distributed through professional organization representatives and the CIOs were not asked to provide their professional organization. This may suggest that email recipients forwarded the survey to friends or coworkers, which would change the sample size of the population. Unfortunately, this irregularity cannot be resolved and so remains a limitation of the research methodology.

Suggestions for Future Research

The following paragraphs discuss prospective future research topics relating to this thesis project. These topics include interoperability in the federal LE community,

information-sharing between LEAs and the private sector, identifying and protecting U.S. critical infrastructure, and interoperability between departments of the federal government.

Longitudinal Study

The LE community is expected to change in many respects as the terrorism and other complex public safety threats continue to evolve. Repeating this study at a later date could reveal how these events are shaping communication in the LE community.

Technology Independence in the LE Community

Though system quality could not be conclusively studied, one of the four items under the IS environmental factor called system quality was determined to be statistically significant. State and local LE personnel reported a definitive preference to interpersonal contact over electronic systems when communicating with federal LE agencies. During factor analysis, this item correlated highly with the item studying attitudes about the obsolescence of federal LE information technology. If the items are connected, this could point to a technology-independent attitude in the LE community—a subject area that might require further study.

Federal Law Enforcement IS Interoperability

While this paper discussed the communications and information-sharing capabilities of federal law enforcement agencies with state and local law enforcement organizations, many articles suggested there would be value in studying how federal law enforcement agencies communicate and share information resources among themselves.

Information-Sharing Between LEAs and the Private Sector

Many of the articles reviewed during this research discussed collaborative efforts between law enforcement agencies and industry. Financial crime investigations involve both the Treasury Department's law enforcement personnel and private banking/trading institutions (FINCEN, 2002). In February 2002, the new administration for homeland security held a conference involving federal agencies, military commanders, state/local law enforcement associations, non-profit organizations, and private industry leaders to discuss major issues concerning domestic U.S. defense. An entire session was dedicated to examining how the public and private sectors can work together to combat terrorism.

Critical IT Infrastructure

Critical infrastructure throughout the U.S. includes capabilities relating to banking, power production, drinking water availability, transportation structures, and telecommunications. Facilities that support infrastructure include nuclear power plants, dams, railroads, highways, water purification and sewage treatment plants, phone and electric lines, and fiber optic cable. As noted in the Homeland Security Conference Report, the federal government has so far failed to "establish an effective mechanism for determining which of the country's vast infrastructure are vital to national security missions and economic activity…" (Homeland Security Monitor, 2002). The absence of a critical infrastructure protection (CIP) plan remains a blatant hole in national strategy and the "weak link in the national homeland security posture….failure to define critical infrastructure could result in a disproportionate allocation of resources" (Homeland Security Monitor, 2002). A study that assesses U.S. criminal justice IT infrastructure

toward developing a CIP for the LE community would be one viable research route in this area.

Federal Department IS Interoperability

Though each department in the federal government covers a substantially different set of legislative responsibilities, collaborative efforts between these different departments could yield significant gains in bureaucratic productivity. For example, the INS deports only 112,000 of the 275,000 illegal aliens who enter the US each year (Prout, 2001). How could information sharing initiatives with the Department of the Interior or Department of Agriculture help the INS identify and apprehend fugitives? Major computer viruses attack federal networks each year. How could a collaborative network provide essential cyber-threat information to all federal agencies to prevent the spread of and minimize the damage done by malicious programs? Again, there are a substantial number of avenues a researcher could take in this area.

Summary

This chapter elaborated on conclusions about the results of the survey presented in the previous chapter. The implications of these conclusions for the federal LE community were then presented. Additionally, the limitations of this research effort were discussed, and suggestions for future research in this area were presented in hopes that succeeding researchers will continue to advance our knowledge of the nature of communication in the LE community.

Appendix A.
Federal Law Enforcement Agency Descriptions

Brief descriptions of nine prominent federal agencies and website information on 14 other federal law enforcement agencies are provided below.

Air Force Office of Special Investigations (AFOSI)

AFOSI was created in 1948 under the Department of the Air Force. It is the primary investigations office for major criminal activities within AF. According to the AFOSI website, "the organization seeks to identify, investigate, and neutralize espionage, terrorism, fraud and other major criminal activities that may threaten AF and DoD resources." (AFOSI, 2002) AFOSI's four main focus areas include counterintelligence, violent crime, cyber threats, and acquisition fraud. The agency consists of 2,274 active duty personnel, of which 1,672 are special agents.

Bureau of Alcohol, Tobacco, and Firearms (ATF)

In 1789, the first Congress imposed a tax on imported spirits in order to pay some of the new nation's Revolutionary War debt. The Department of the Treasury assumed these duties under the Office of Internal Revenue, later the IRS. In 1972, these duties were transferred to a separate, newly created bureau—the ATF—under Treasury Department Order No. 120-1. The ATF's initial authority included all matters related to alcohol, tobacco, firearms, and explosives; however, these duties were expanded to include arson investigations when arson was deemed by Congress to be a federal crime by the Anti-Arson Act of 1982. According to the ATF website, "charged as it were with fiscal oversight of some of the most controversial topics in Western civilization, ATF strives to maintain professional neutrality while giving a 35-to-1 return on every dollar it

spends" and collects over $13B revenue annually. (ATF, 2002) This view aligns with the ATF's mission: "a law enforcement agency…with unique responsibilities dedicated to reducing violent crime, collecting revenue, and protecting the people." (ATF, 2002) Among the bureau's activities, ATF personnel license and regulate 9,500 explosives industry members, regulate 104,000 federal firearms licensees to ensure compliance with federal firearms laws, administer the Firearms Trafficking Program, staff the National Tracing Center which tracked approximately 200,000 crime guns in FY99, investigate illegal alcohol and tobacco diversion cases, and review 74,000 alcohol labels to ensure proper classification and product disclosure. In addition, the ATF provides gang-resistance education programs to schools and trains canines to detect explosives, spent cartridges, and fire accelerants. (ATF, 2002)

United States Coast Guard (USCG)

The Revenue Cutter Service was created by Congress in 1790 to protect the nation's ports and enforce customs directives on incoming trade. In 1915, the Revenue Cutter Service merged with the Life-Saving Service to create the USCG. The USCG operates within the Department of the Treasury during peacetime; however, authority falls to the Secretary of the Navy during war or when the President directs. In addition to the USCG's national defense mission, the organization is "charged with a broad scope of regulatory, law enforcement, humanitarian, and emergency response duties." (USCG, 2002) The USCG has five strategic objectives: maritime safety which includes search and rescue, marine safety, recreational boating safety, and international ice patrol; maritime mobility which includes navigation aids, icebreaking services, bridge administration, vessel traffic, and waterways management; maritime security which

includes drug interdiction, alien migrant interdiction, living marine resource management, and law/treaty enforcement; national defense which includes general defense duties, homeland defense, port and waterways security, and polar icebreaking; and protection of natural resources which includes foreign vessel inspections, living marine resources protection, marine and environmental science, and marine pollution education, prevention, response, and enforcement. (USCG, 2002) The USCG is responsible for 95,000 miles of US coastlines and 3.4 million square miles of ocean defining the US Exclusive Economic Zones. (USCG, 2002)

United States Customs Service

The Customs Service is a branch of the US Treasury and acts as the primary law enforcement agency protecting US borders. The Tariff Act of 1789 authorized the US government to collect revenue from imported goods and led to the establishment of the Customs Service later that year. (US Customs, 2002) Customs officials clear international travelers into the US, examine baggage, control imports, and provide smuggler/alien interdiction services. As a result of their revenue collection duties, Customs returns approximately $22B annually to the US Treasury with a 16-to-1 return ration for every dollar appropriated. Customs provides the nation's second largest source of revenue (second only to IRS tax collection revenues). Customs revenues paid for the territories of Louisiana, Oregon, Florida, and Alaska and funded construction of the City of Washington and important infrastructure such as the National Road, the Transcontinental Railroad, and all of the nation's lighthouses. More recently, the Customs Service has been directed to research methods to help automate commercial import processes, which is expected to streamline import procedures, lower the cost of

trade compliance, and decrease the amount of paperwork associated with importation. (US Customs, 2002) In addition to protecting US borders, Customs officials provide drug interdiction services, help prevent cybercrime and money laundering, and combat terrorism. (US Customs, 2002)

Drug Enforcement Administration (DEA)

The DEA was formed in 1973 as a Department of Justice initiative. This agency oversees all federal domestic drug enforcement programs and coordinates through offices abroad on international drug investigations. The DEA employs 9,629 personnel, of which 4,680 are special agents. Drug enforcement agents are tasked with discovering and apprehending individuals who grow, manufacture, or distribute controlled substances within the US. (DEA, 2002) DEA programs include demand reduction, marijuana eradication, mobile enforcement teams, and the Organized Crime Drug Enforcement Task Force. The DEA also operates eight laboratories located across the US and the El Paso Intelligence Center, which provides security, training, and intelligence assistance along the southern US border. The current major drug threats facing the US include methamphetamine, Ecstasy, OxyContin, and cocaine.

Federal Bureau of Investigations (FBI)

The FBI was formed in 1908 by the US Attorney General as the investigative arm of the Department of Justice. The agency consists of 30 departments and administers 56 field offices, 400 satellite offices, and 40 foreign liaison posts staffed by 11,000 special agents and 16,000 support personnel. The FBI's investigative functions cover a variety of national concerns including civil rights, counterterrorism, foreign counterintelligence, organized crime, drug interdiction, violent crimes, major offenders, and financial crimes.

In addition, the FBI provides training, information services, and investigative assistance to local, state, other federal, and international law enforcement agencies. The FBI's information services include fingerprint identification, laboratory services, and criminal history files. (FBI, 2002)

Immigration and Naturalization Services (INS)

The Department of Justice administers the INS, which oversees all naturalization functions and enforces admission standards for persons wishing to enter the US. INS enforcement responsibilities include border control, port-of-entry inspections, detention/removal of criminal aliens, apprehension of illegal aliens, deportations, exclusions, and document fraud. The INS also provides refugee and asylum services for the federal government. The agency employs 29,000 personnel and administers a headquarters in Washington, DC, three regional offices, 33 district offices, and 21 border patrol sectors throughout the US as well as three district offices and 39 area offices outside the US. Immigration functions have been performed by the federal government since 1864; however, the Immigration Act of 1891 was the first law establishing federal control and guidelines over immigration. Naturalization functions were performed by the courts until Congress executed the Naturalization Act of 1906, taking federal control of all naturalization functions. An Executive Order in 1933 combined the two functions under the INS, then belonging to the Department of Labor. In 1940, INS jurisdiction was transferred to the Department of Justice. Today, the INS performs over 510 million inspections of individuals entering the US and oversees 6,000 miles of border with Mexico and Canada and 250 ports of entry into the US. In 2001, the INS apprehended

1,235,000 illegal aliens along the Southwest border and received 7.9 million applications for immigration benefits. (INS, 2002)

Secret Service

The Secret Service operates as an agency within the Department of the Treasury. The agency was enacted in 1865 to suppress counterfeiting activities; however, it was not recognized as a distinct law enforcement division until 1883. In 1894, the agency took on part-time protection of the President. After President McKinley's assassination in 1901, Congress requested the Secret Service protect the President full time; however, funding was not appropriated for these duties until the Sundry Civil Services Act of 1907 was passed. In 1930, the White House Police merged with the Secret Service. The agency's financial crimes duties were expanded in 1984 to include credit/debit card fraud and identity theft. (US Treasury, 2002) The Secret Service's official mission is two-fold and includes the protection of the President, Vice President, their immediate families, heads of state, and other designated personnel. The second mission involves law enforcement concerning counterfeiting and other financial crimes encompassing device fraud, financial institution fraud, identity theft, computer fraud, telecommunications fraud, and cyber crimes. (US Treasury, 2002) The Secret Service employs 2,100 special agents, 1,200 Uniformed Division officers, and 1,700 support personnel in 125 offices located both within the US and abroad. (US Treasury, 2002)

United States Marshals Service (USMS)

The USMS was created by the Judiciary Act of 1789, which also established the federal judicial system. The agency is administered by the Department of Justice. The early mission of the USMS was expansive. They served subpoenas, summons, writs,

warrants, and other court documents. The USMS rented courtrooms, hired bailiffs, ensured jurors were available, and kept watch over prisoners. They represented the federal government at the local level and even took the national census until 1870. (USMS, 2002) Today, the USMS mission includes protecting federal courts and ensuring the judicial system operates efficiently and within legal guidelines. US Marshals also provide protection for judges, transport prisoners, execute the witness protection program, and manage seized assets. The USMS is responsible for 55 percent of arrests of all federal fugitives. (USMS, 2002) The agency employs 4,000 agents and support personnel in 350 offices across the US, Guam, Northern Mariana Islands, Puerto Rico, and the Virgin Islands. (USMS, 2002)

Other Federal Law Enforcement Agencies

The following list includes all other federal law enforcement agencies and weblinks to their respective homepages:

Environmental Protection Agency: www.epa.gov

Federal Communications Commission: www.fcc.gov

Federal Aviation Administration: www.faa.gov

Federal Trade Commission: www.ftc.gov

Financial Crimes Enforcement Division: www.treas.gov/fincen

Internal Revenue Service Criminal Investigative Division: www.treas.gov/irs/ci/index.html

National Security Agency: www.nsa.gov

Office of the US Attorney General: www.usdoj.gov/ag/index.html

Office of the Inspector General: oig.gsa.gov

Postal Inspection Service: www.usps.gov/wesites/depart/inspect

Securities and Exchange Commission: www.sec.gov

State Department Bureau of Diplomatic Security: ds.state.gov/index.html

US Army Military Police Corps: www.wood.army.mil/usamps/default.htm

US Federal Protection Service Police: members.aol.com/usfpsfl/usfps.htm

Appendix B.
Criminal Justice Information Systems

There are several criminal justice information systems currently operating across the US, each with a different purpose, scope, and capability. While most of these systems are funded and administered at the federal level, a few regional systems, through cooperative efforts among state government agencies, have matured into prominent information-sharing tools for law enforcement agencies. In addition, the federal government has commissioned many programs designed to enhance the interoperable capabilities of law enforcement and public safety organizations across federal, state, and local tiers. Here is a brief overview of the more significant information systems and interoperability programs.

Advanced Generation of Interoperability for Law Enforcement (AGILE)

AGILE is a federal program sponsored by the National Institute of Justice, an agency within the Department of Justice. One of AGILE's research missions specifically focuses on interoperability capabilities at all levels of law enforcement and public safety, both in wireless public safety telecommunications and information technology applications. AGILE's mission statement is "to assist state and local law enforcement agencies to effectively and efficiently communicate with one another across agency and jurisdictional boundaries…helping bridge the gap in emergency communication by identifying, adopting, and developing interoperability solutions that include open architecture standards for voice, data, image, and video communication systems" (AGILE, 2002). One of AGILE's current initiatives is the INFOTECH program—the goal of which is to develop easy-to-use, secure information technology systems that

provide inter-regional information sharing capabilities among law enforcement agencies, while minimizing cost and federal restrictions to state and local agencies (AGILE, 2002). AGILE is also involved with testing state-of-the-art radio switching technologies for field use, developing a national program for quickly disseminating information on kidnapped and missing children, and providing grants/funding to state and local law enforcement and public safety agencies for procuring telecommunications/IT equipment and applications.

Public Safety Wireless Network (PSWN)

Information Technology initiative 04 (IT04), a product of the National Performance Review of 1993, prompted the program's creation. IT04 envisioned "the nationwide development of interoperable systems for all types of public safety agencies at the local, state, and federal levels of government" (Public Safety Wireless Networks, 2002). Like AGILE, PSWN is a federally funded program and remains a joint effort between the Departments of the Treasury and Justice to "promote effective public safety communication and to foster interoperability among local, state, and federal communication systems" (Public Safety Wireless Networks, 2002). It is a two-phased, multi-year project designed to meet three primary objectives: establish nationwide interoperable communications across federal, state and local tiers; establish Public Safety Wireless Interoperability National Standards (WINS), and maximize the effectiveness of interoperability assistance efforts (Public Safety Wireless Networks, 2002). PSWN's first phase concentrates on collecting information on current operations, standards, and best practices to form a national knowledge base. The second phase centers on maintaining that knowledge base and assisting law enforcements agencies with the

implementation of standards developed under the WINS. PSWN planning initiatives began in 1997, and the program's execution phase (which began in early 2002) is projected for completion in 2006.

Global Criminal Justice Information Network (GCJIN):

GCJIN is administered by the Bureau of Justice Administration in the Department of Justice. GCJIN envisions the ability of law enforcement officers to electronically access criminal justice information anytime, anywhere—even in a police cruiser after pulling over a suspect. GCJIN was developed by the Global Advisory Committee, comprised of local, state, and federal law enforcement officers. Like the AF Portal, GCJIN is an all-encompassing window into various law enforcement databases and IT systems. GCJIN provides the capability to link different systems to provide complete access to critical criminal justice information to the law enforcement officer (Robinson, 2002).

Office of Law Enforcement Standards (OLES)

OLES belongs to the Electronics and Electrical Engineering Laboratory within the National Institute of Standards and Technology. In response to a national financial crisis among law enforcement agencies, Congress directed the Department of Justice to develop a program that could provide sound procurement guidance to state and local law enforcement agencies. To fulfill this mandate, the Department of Justice created OLES in 1971 (Higgins K., 2001). OLES' original mission was to provide a list of equipment tested and approved for safe, effective use in law enforcement activities; however, OLES has expanded its mission in response to growing law enforcement research needs. The organizational vision is "to apply science and technology to the needs of the criminal

justice community" (National Institute of Standards and Technology, 2002), and OLES currently has five core program areas: weapons and protective systems, detection and inspection technologies, chemical systems and materials, forensic sciences, and public safety communications standards (Higgins K., 2001). OLES serves as "the principal agent for standards development for the criminal justice and public safety communities….Through its programs, OLES helps criminal justice and public safety agencies acquire, on a cost-effective basis, the high quality resources they need to do their jobs" (National Institute of Standards and Technology, 2002).

Regional Information Sharing Systems Program (RISS)

RISS is a program administered by the Institute for Intergovernmental Research of the Department of Justice. RISS contains six regional centers (see figure below) that operate independently, however, share information to combat criminal networks that may operate over vast territories such as organized crime, drug trafficking, cybercrime, terrorism, and gang activities (Edwards, 2002). According to their website, RISS has over 6,000 members and spans across all 50 states, two Canadian provinces, the District of Columbia, Australia, Guam, the US Virgin Islands, England, and Puerto Rico. Member agencies range across all three law enforcement tiers: over 4,000 municipal and county departments, 360 state agencies, and 750 federal agencies (Edwards, 2002).

IDENT-INS

IDENT-INS is a fingerprint catalog maintained by the Immigration and Naturalization Service. IDENT-INS logs electronically recorded imprints of the index fingers and criminal histories of all aliens the INS has apprehended within the US (Dempsey, 2000). IDENT currently contains over 400,000 records. The system was

created in 1994; however, IDENT wasn't widely distributed until 1997-1998 when network technology was able to support common usage. IDENT now has over 400 access points at border control facilities, international airports, asylums, and district offices. In conjunction with IDENT's geographical expansion, the INS conducted formalized training on IDENT and published standards of use for the system. In 2000, IDENT and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) began planning a merger between databases (Immigration and Naturalization Services, 2002).

National Infrastructure Protection Center (NIPC)

NIPC is an FBI initiative which monitors threats against critical US infrastructure and provides warning, response, and assessment services to local and state agencies as well as the private sector. NIPC was established in 1998 and serves as the federal government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. NIPC defines infrastructures to include telecommunications, banking, energy, water systems, government operations, and emergency systems (National Infrastructure Protection Center, 2002). NIPC now encompasses one of its predecessor programs, Infragard. Infragard was conceptualized in 1996 when the Cleveland FBI office surveyed local computer professionals about how to better protect critical information systems (Infragard, 2002). The Infragard program now contains 5,369 members at the federal, state, and local levels as well as in the private sector.

National Law Enforcement Telecommunications System (NLETS)

NLETS is a secure, fully redundant communications network with a standardized nationwide addressing scheme that provides electronic communications capability to law enforcement agencies. The project began in 1966 as the Law Enforcement Teletype System, based on punched paper tape switching equipment technology and connected to all 50 states using only six telecommunications lines from headquarters in Phoenix, AZ. Since then, NLETS has grown into much more sophisticated computer-based message switching network that links local, state, and federal law enforcement agencies located across the US. NLETS is the backbone for most law enforcement information-sharing applications and provides the capability to exchange many types of information (voice, video, imaging, and text). In 1990, NLETS expanded its range to include connections with the Royal Canadian Mounted Police and Interpol (National Law Enforcement Telecommunications System, 2002).

Uniform Crime Reporting/National Incident-Based Reporting System (UCR-NIBRS)

UCR-NIBRS is the combined efforts of two distinct, yet related, law enforcement data collection programs. UCR began in the 1920s as the Uniform Crime Records program, initiated by the International Association of Chiefs of Police. The UCR program is like a census on crime in the US and attempts to measure levels of crime by collecting data from over 17,000 local, state, and federal law enforcement agencies. UCR publishes reports and statistics on all types of crime in the US and tracks numbers of law enforcement officers killed or assaulted in the line of duty. NIBRS grew out of the UCR program during the 1980s. NIBRS attempted to "enhance the quantity, quality, and

timeliness of crime data collection by law enforcement" and to update data collection, storage, processing, and distribution methodologies of the original UCR program (Federal Bureau of Investigations, 2002).

Law Enforcement On-Line (LEO)

Created in 1995, LEO is a secure interactive Internet-based communication system for 32,500 federal, state, and local law enforcement officers (Federal Bureau of Investigations, 2002). It is primarily an educational and information sharing tool using electronic communication applications to disseminate best practices and technological instruction to law enforcement professionals across the US. LEOs capabilities include e-mail, news groups, chat, feedback, special event calendars, electronic library, and distance learning (Federal Bureau of Investigations, 2002). As LEO program coordinator Special Agent Craig Sorum states, "…the most important aspect of LEO is the fact that the Director's been mandated to facilitate communications between state and local officials" (Sorum, 2002).

National Instant Criminal Background Check System (NICS)

NICS was established in 1998 by the Attorney General's Office in response to provisions of the Brady Handgun Violence Prevention Act of 1994, requiring all licensed gun sales establishments to perform background checks on individuals attempting to purchase a firearm. Currently, 26 states have full or partial access to NICS. The other 24 states must contact the FBI for NICS information (Federal Bureau of Investigation, 2002). NICS searches four databases containing millions of criminal history records from all 50 states on persons who are disqualified from receiving firearms. NICS

typically returns information within 30 seconds of the request (Federal Bureau of Investigation, 2002).

National Integrated Ballistics Information Network (NIBIN)

The Bureau of Alcohol, Tobacco, and Firearms administers the NIBIN program, which provides ballistic identification equipment to "state and local law enforcement agencies for use in imaging and comparing crime gun evidence" (NIBIN, 2002). NIBIN allows law enforcement agencies to share and acquire ballistic information and images on bullets and cartridge casings. According to the NIBIN website, this program allows state and local law enforcement agencies access to ballistic intelligence capabilities that they may not be able to afford on their own. NIBIN was initiated in 2000 as a multi-year project. The NIBIN program will install ballistics identification equipment in 233 locations positioned in major population centers across all 50 states (NIBIN, 2002). NIBIN's networking capabilities allow specialists to compare ballistic information across jurisdictional boundaries, enabling collaborative capabilities for law enforcement officials to curb violent crimes (South Dakota Division of Criminal Investigation, 2002).

Combined DNA Index System (CODIS)

CODIS is a national DNA database created in 1998 and administered by the FBI. CODIS is a nationally fielded, Internet-based system allowing local, state, and federal law enforcement agencies to exchange and compare DNA profiles. According to the CODIS website, the DNA Identification Act of 1994 authorized the FBI to establish a national DNA index for law enforcement purposes (Federal Bureau of Investigation, 2002). As of June 2002 CODIS contained 1,013,746 profiles, including 35,851 forensic profiles and 977,895 criminal offender profiles. Ohio, for example, has contributed

31,768 offender profiles and 1,091 forensic samples to the system through 10 CODIS labs located throughout the state. This information has aided 100 investigations (Federal Bureau of Investigation, 2002).

Integrated Automated Fingerprint Identification System (IAFIS)

IAFIS is the FBI's electronic fingerprint identification database. IAFIS was brought on-line in 1998 as Lockheed-Martin Corporation developed the software, scanners, and matching equipment needed to deploy the system. Scanners encode a latent fingerprint sample which can then be electronically submitted to IAFIS. IAFIS then searches its database for matches and reports any possible matches. The FBI plans to make this information available to state and local agencies; however, unlike NIBIN, IAFIS is not a federally funded project and state/local agencies must purchase their own equipment (Criminal Justice Information Systems, 2002).

Criminal Justice Information Services Wide Area Network (CJIS WAN)

CJIS WAN describes the infrastructure supporting IAFIS. It is a secure pipeline through which IAFIS data can be exchanged. CJIS was brought on-line in 1999 and is still in its developmental stage. The FBI's short-term plans to expand CJIS services include the addition of DNA information sharing capabilities (Dempsey, 2000).

Interstate Identification Index (III)

III is a commercially developed Internet-based information-sharing tool allowing federal, state, and local law enforcement agencies to exchange criminal history, mugshot, and fingerprint data. It was developed to replace the Identification Division Automated Services (IDAS) system, an FBI legacy system that relied on manual input and paper

product transfers making it inefficient. Under IDAS, inquiry responses could take up to 10 days to complete (SAIC, 2002).

National Crime Information Center Network (NCIC)

NCIC is a network of databases and services providing information on criminal activities, suspects, missing persons, unidentified persons, terrorist cells, and stolen property. NCIC's mission is to promptly disclose information about criminals and crimes in order to expedite investigations. NCIC is administered by the FBI and contains links to other FBI programs such as III and LEO. NCIC is accessible to law enforcement agencies in all 50 states, Puerto Rico, and all US Possessions and Territories. Limited access has also been granted to the Royal Canadian Mounted Police. In the long-term, the FBI plans to merge NCIC with CJIS under one program (Pike, 2002)

Financial Crimes Enforcement Network (FinCEN)

FinCEN links federal law enforcement agencies and financial institutions in order to share account and transaction information that may involve terrorist activity or money laundering (Department of the Treasury, 2002). FinCEN was created in 1990 by the Department of the Treasury under provisions included in the Bank Secrecy Act. FinCEN is accessible at the local, state, federal, and international levels. The program was intended to create a collaborative environment for tracking criminals engaging in financial crimes (Department of the Treasury, 2002).

Cyber Warning Information Network (CWIN)

CWIN is an early warning/detection network designed by the White House Office of Cyberspace Security to combat cyber crime and terrorism. CWIN links local, state, and federal agencies with the private sector through a national network providing

information sharing capabilities on emerging cyber threats. Any individual, whether on the CWIN network or not, can alert any of the information sharing and assurance centers of a cyber attack. These centers will then push warnings out to government and private organizations about the emerging threat. Organizations would then enact operational plans to minimize the impact of the threat on the networks they control. It's a proactive method of decreasing the damage any one attack may inflict. "This is a case where the government doesn't know best or first. So you need a public-private partnership to reach out to these nodes in the private sector….that see viruses first," says Richard Clark, special adviser on cyberspace security to President Bush (Vaida, 2001).

National Drug Pointer Index (NDPIX)

NDPIX is administered by the Drug Enforcement Administration and was brought on-line in 1997. NDPIX is available to local, state, and federal law enforcement agencies across the NLETS backbone. The system allows law enforcement officials to determine if drug suspects are being investigated by other law enforcement organizations allowing transfer of vital crime information, maximizing collaborative capabilities, and minimizing duplication of effort (Drug Enforcement Administration, 2002). According to NLETS Executive Director Timothy Sweeney, NDPIX is currently populated with over 120,000 suspects and leads (Drug Enforcement Administration, 2002).

Federal law enforcement agency websites

Each federal law enforcement agency maintains its own website with information pertaining to their area of expertise. (The major federal law enforcement agencies are identified and briefly described in Appendix A.) These websites also contain links to related sites which may contain pertinent law enforcement information.

Appendix C.
History of Influential Federal Information Systems

ARPANET

The Advanced Research Projects Agency (ARPA) was formed in reaction to the former Soviet Union's launch of Sputnik in 1957 (Hauben, 2002), which became a political harbinger that the US' technological superiority had been trounced. Though ARPA was a military agency, its primary focus was technological research. Thus, many of the agency's projects did not have direct battlefield applications. In 1962, ARPA was directed to research command and control applications utilizing computer technology (Hauben, 2002). This directive launched the development of ARPANET, commonly held as the forerunner of the Internet.

ARPA scientists teamed with researchers from US universities in a collaborative effort to fulfill the objectives of ARPA's mission. These universities included Stanford, the University of California at Los Angeles, the University of California at Santa Barbara, and the University of Utah (Hauben, 2002). The researchers were essentially starting from scratch and had to create tools and concepts commonly attached to networking including protocols, topologies, and even the nodes upon which the network was implemented. After nine years of planning, constructing and testing, ARPANET was brought on-line in 1971. "After the ARPANET was up and running, the computer scientists using it realized that assisting human communication was the most fundamental advance that the ARPANET made possible" (Hauben, 2002). Since 1971, the basic network that ARPA and its associates brought into being has slowly evolved into the Internet.

National Communications System (NCS)

Development of the first federal communications system began in 1962, fueled by communications difficulties experienced between US government agencies, foreign entities, NATO, and the diplomatic corps during the Cuban missile crisis. President Kennedy ordered an investigation into interoperability issues affecting US secure communications capabilities. The National Security Council headed this investigation, which resulted in the creation of the NCS. The system's purpose as outlined in a 1963 Presidential Memorandum was to "provide better communications support to critical government functions during emergencies…linking, improving, and extending the communications facilities and components of various federal agencies, focusing on interconnectivity and survivability" (National Communications System, 2002). Though communications technology has evolved quite a bit since 1962, the purpose of NCS remains relatively unchanged. In 1984, President Reagan broadened the NCS' national security and emergency preparedness capabilities scope under Executive Order 12472. National security and emergency preparedness capabilities refer to "services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or that degrades or threatens the national security/emergency preparedness posture of the United States (National Communications System, 2002). Also under this mandate, NCS membership grew from six members to 22 (see Table A-1).

Table A-1: NCS Membership

US Department of State	Nuclear Regulatory Commission
US Department of the Treasury	The Joint Staff
US Department of Defense	General Services Administration
US Department of Justice	Department of Veterans Affairs
US Department of the Interior	National Aeronautics and Space Administration
US Department of Commerce	National Security Agency
US Department of Health and Human Services	United States Postal Service
	Federal Reserve Board
US Department of Transportation	Federal Communications Commission
US Department of Energy	Federal Emergency Management Agency
US Department of Agriculture	National Telecommunications and Information Agency
Central Intelligence Agency	

Source: National Communications System, 2002

Current NCS projects include a range of telecommunications interoperability initiatives. The Shared Resources High Frequency Radio Program (SHARES) provides "a single, interagency emergency message handling system by bringing together existing HF radio resources of federal, state, and industry organizations when normal communications are destroyed or unavailable for the transmission of national security and emergency preparedness information" (National Communications System, 2002). The SHARES program has allocated 1,071 radio stations utilizing 215 HF frequencies for use in such situations. These stations are located in every US state and at 20 overseas locations.

The Telecommunications Service Priority (TSP) Program ensures that national telecommunications services supporting national security or emergency preparedness missions receive priority treatment across national infrastructure. The TSP governing body also provides regulatory guidance and administrative support to the program's two primary components, restoration and provisioning activities for resources contained within NCS national security and emergency preparedness telecommunications

programs. Restoration refers to prioritizing the repair or continuance of service of TSP-identified services before non-TSP services in order to ensure minimal interruption to public safety, national security, and emergency preparedness. Provisioning refers to the prioritization of telecommunications service installations for TSP-identified projects over non-TSP telecommunications projects when it is deemed that these telecommunications projects are critical to continuance of effective national security and emergency preparedness activities (National Communications System, 2002).

The Government Emergency Telecommunications Service (GETS) addresses two denial of service issues: disruption and congestion. Disruption occurs when telephonic services are crippled due to natural disaster, power outages, cable cuts, or software glitches. Congestion occurs when telecommunications circuits are loaded to capacity, such as the Mother's Day Phenomenon, and calls cannot be connected due to circuit unavailability. GETS is an NCS-sponsored dialing plan that utilizes Personal Identification Number verification methods to maintain a high likelihood of call completion even during severe conditions of telecommunications congestion or disruption. The program supports federal, state, and local government organizations as well as private industry and non-profit organization personnel who hold a stake in national security/emergency preparedness. GETS encompasses major long distance networks (AT&T, MCI, WorldCom, Sprint), government-leased networks (FTS and DISN), and local networks (independent local exchange carriers, cellular carriers, and personal communications services) (National Communications System, 2002).

Other NCS programs include the Advanced Intelligent Network (AIN), Alerting and Coordination Network (ACN), National Coordinating Center (NCC), Priority Access

Service (PAS), Wireless Priority Services (WPS) , and Training, Planning, and Operational Support (TPOS). Information about these programs can be accessed through the NCS homepage at www.ncs.gov/ncs/html/ncsprojects.html.

The NCS was the federal government's first endeavor to provide telecommunications interoperability for critical governmental functions, recognizing the critical nature of the ability to communicate in crisis situations. Though NCS programs were first concerned with radio and telephonic interoperability and accessibility capabilities, the program has evolved to include network, wireless, and other emerging technologies. This program continues to influence the way government organizations view telecommunications and interoperability capabilities at national, state, and local levels.

Kansas Criminal Justice Information System (KCJIS)

The Kansas Bureau of Investigations (KBI), a state government version of the FBI, pioneered the use of information technology to aid law enforcement with the development of the KCJIS. According to the KBI Director, "Four years ago, Kansas ranked at the bottom of criminal history—we were a joke. Now, Kansas is the only state allowed to send FBI criminal history information over the Internet" (Wartell, 2000). Since its inception in 1996, the KCJIS has been considered an influential leader in criminal justice information system architecture, management, and security (Rohrer, 2001)—as evidenced by the FBI's singular approval for KCJIS to transmit sensitive FBI information (such as mugshots, fingerprints, and criminal history records) across the Internet.

The KCJIS program rose from a need recognized by the KBI to efficiently disburse criminal justice information to law enforcement agencies, judicial system users, and state government offices. Sentencing Guidelines passed by the State of Kansas in 1994 signaled the need for better records management in the criminal justice system. The courts identified a need "to quickly access complete criminal history information for sentencing purposes, and at the time, it was not readily available" (Wartell, 2000). A 1995 audit of Kansas' criminal history repository revealed "a large percentage of records not entered, inaccurate, or missing information" (Wartell, 2000). Law enforcement agencies identified other problems with the transference of information within the criminal justice community: limited accessibility, slow network connections, and the lack of imaging capability for fingerprints and mugshots. With the emergence of web-based technologies in the mid-1990s, the KBI realized that an electronic solution might best fill their needs. Consequently, the KBI developed the following system objectives: (1) it would contain open system architecture, but with adequate network security, (2) security hardware and software would meet national standards, (3) reliability and availability would be guaranteed via system redundancy, (4) the system would be able to share data electronically with local, state, and federal criminal justice agencies, and (5) users would be able to access the system using common Internet service providers (Rohrer, 2001).

KCJIS is a secure Internet-based application and was implemented across the existing Kansas state public network, KANWIN, which can be accessed using a dedicated frame relay or dial-up connection—a key feature contributing to reduced system operational and installation costs. These features give the system a great deal of

flexibility and allow KCJIS to support a variety of users with different telecommunications capabilities. KANWIN services all state and local government agencies across the 105 counties in Kansas. These agencies include K-12 schools, universities, hospitals, law enforcement organizations, and other municipal functions (Rohrer, 2001). Currently, KCJIS supports over 7,000 users from law enforcement, judicial system, and state and local government organizations. Because KCJIS can be accessed through any Internet service provider (ISP), all of Kansas' criminal justice agencies can afford to use it through a virtual private network, regardless of how small they may be—this is especially noteworthy since many local Kansas ISPs provide free Internet access to government agencies (Rohrer, 2001).

KCJIS supports several criminal justice data systems that were operational prior to KCJIS' inception. These data systems include the Computerized Criminal History System which records arrest records, court dispositions, custody and supervision decisions, etc; the Kansas Incident-Based Reporting System which logs police incident reports; the Automated Fingerprint Identification System; and the Automated Statewide Telecommunications and Records Access Network which joins geographically separated law enforcement units on a single network (Wartell, 2000).

According to Rohrer (2001), the system has already paid for itself. The original system cost the State of Kansas $675,000 to implement. Average cost avoidance each year since installation has topped $2M. Approximately half of this cost avoidance occurs at the local level due to decreased paper costs, less paper handling, and freeing personnel to accomplish other tasks than chasing criminal records. At the state level, KBI has been able to install and maintain KCJIS without hiring additional staff (Rohrer, 2001).

Given the sensitive nature of the information contained on the system, security is considered a key feature of KCJIS. According to Rohrer (2001), "…most users choose passwords poorly….passwords are not safe as hackers have several tools such as "Cracker" and "Social Engineering" available to steal passwords." To remedy this, KBI purchased key fob tokens which choose the user's password. Passwords are used one time only, which further protects the system from stolen or intercepted passwords. Since the token maintains passwords for the user, KCJIS customers are relieved from managing their own passwords which further simplifies system use. These security features have been tested. The criminal justice organization SEARCH attempted unsuccessfully to breach the system with 20 of its agents. Additionally, the KCJIS firewall identifies and logs network probes on the system—none of these probes have infiltrated the system. In light of this, when the FBI created their network security guidelines, they used KCJIS as a model for security assurance (Rohrer, 2001).

KCJIS has streamlined the criminal justice process in many other areas as well. The system has greatly reduced the time needed to retrieve criminal history records for court appearances. Transaction times for completing a criminal history request have been drastically reduced from six weeks to ten minutes. With KCJIS' image processing capabilities, electronically stored mugshots and fingerprints have increased accuracy in identifying suspects. Additionally, now that data is handled and entered at the local level, the accuracy of data entering the system has improved (Rohrer, 2001).

KCJIS remains a model for state government-sponsored criminal justice information systems and has catapulted the State of Kansas from the bottom of the technological heap to a forerunner in utilizing IT to enhance law enforcement

capabilities. The project's implementation is far more than an incremental improvement and has completely reengineered records management in the criminal justice community.

The FBI's Trilogy Project

Even before the terrorist attacks on September 11, 2001, the FBI had plans to upgrade their available infrastructure and networking capabilities to increase interoperability among federal, state, and local law enforcement agencies. In May 2001, the FBI contracted out the Trilogy project, a three-year, $400M effort to upgrade 27,000 personal computers and 350 servers at 650 locations (Dean, 2001). The FBI's network will migrate to a common operating system utilizing Microsoft products (Windows 2000, Outlook, and Exchange) and an Oracle database management system. The agency's LAN will be upgraded to Fast Ethernet, and the backbone will be upgraded to asynchronous transfer mode (ATM) technology (Dizard, 2002). Trilogy was inspired by several high-profile incidents which led to the FBI's conclusion that system upgrades were necessary. Just before Timothy McVeigh, convicted of the terrorist bombing of the Murrah Federal Building which killed 168 people in Oklahoma City, OK, was scheduled to be executed, government officials discovered that more than 3,000 misplaced documents pertaining to the McVeigh investigation were not released to McVeigh's lawyers during the discovery phase of the trial. It was determined that the FBI's obsolete information technology and records management systems contributed heavily to the misplacement of these documents (Dean, 2001). McVeigh's execution was delayed until the records mishap could be resolved by the courts, and the FBI and US Attorney General's office took heavy criticism from Congress and the press over the situation. Earlier that year, the House Judiciary Committee reviewed the FBI's computer systems.

In a letter to then FBI Director Louis Freeh, the committee commented that "it was 'concerned that the FBI has information technology systems that are slow, unreliable [and] obsolete—systems that are unable to address the bureau's critical needs'" (Dean, 2001). The final punch came when the newly appointed FBI Director Robert Mueller toured the FBI facilities at FBI Headquarters in Washington, DC. During the tour, he noticed a diversity of computer brands on employees' desks, ranging from UNIX-based Sun Mircosystems to Apple to IBM-compatibles Compaq and Dell. In response to his question about why there were so many dissimilar systems, Mueller heard that "… 'every division had a separate computer system until a year or two ago'" (Puzzanghera, 2002). The disparity of the FBI's departmental computer systems had led to much larger problems by 2001, despite that the FBI had spent over $1.7B on major IT projects since 1993 (Puzzanghera, 2002). Agents were unable to send emails externally from their desktops, electronic files could not be searched by more than a single word, and many computers—some located in the same building—still couldn't talk to each other over the current network (Puzzanghera, 2002). These IT deficiencies were causing serious detriments to productivity and mission fulfillment within the FBI, and many suspect IT problems may have contributed to the inability to detect clues that may have helped prevent the 9/11 disaster (Puzzanghera, 2002).

One of the assumptions in the National Strategy for Homeland Security, published in July 2002, is that homeland defense will rely heavily on IT and the nation's infrastructure. Information sharing across interoperable federal systems is a key asset to future national homeland defense strategy (Federal Computer Week, 2002). A necessary component toward fulfilling the information-sharing requirement is the information

infrastructure necessary to enhance federal agencies' ability to collect, store, search, retrieve, and analyze information (Higgins S., 2002) across networks administered by the myriad of organizations that operate within the homeland defense strategy. In keeping with that vision, the overall direction of the Trilogy Project aims to replace the current "green screen" environment (which requires the user to perform 12 separate steps in order to simply store a document) with a windows based, point-and-click operating system with web-based applications (Higgins S., 2002).

The Trilogy Project is an important milestone in federal communications because every agency within the federal government suffers from similar problems. Since 1993, the US government has spent over $370B on computers, software, and infrastructure. However, through investments in highly "customized computer systems that are incapable of communicating with each other" (Puzzanghera, 2002), federal organizations have inherited stovepiped legacy systems bereft of interoperability and interconnectivity qualities. These systems severely limit the abilities of federal agencies to share information across network boundaries, and the only way to remedy the situation is through billions of dollars of further IT investments to upgrade existing networks toward common network environments across all agencies (no matter what department they belong to) that meet federal standards on IT operations. The success of Trilogy will impact the futures of planned IT projects in the Coast Guard, INS, and Customs whose assets have been frozen until interoperability and interconnectivity concerns have been satisfactorily addressed (Puzzanghera, 2002).

After the terrorist attacks on September 11, 2001, Congress requested the Trilogy project be expedited. The original completion date for Phase 1 of the project was set for

October of 2003; however, Congress would like to accelerate its completion to December 2002 (Dizard, 2002). Trilogy is a fully funded project, rated #24 of 39 federal IT projects on the FEDSIM Millenia Activity List, the GSA's official contract IT project prioritization document (FEDSIM, 2002).

Appendix D.
Survey Instrument

Introduction: My name is Capt David Dethlefs. Currently, I'm obtaining my master's degree in Information Systems Management from the Air Force Institute of Technology.

Purpose: My thesis research studies federal information-sharing capabilities with state and local LEAs. This survey will provide a basis of understanding state and local LEA's perception of the information-sharing systems provided by federal LEAs. No personal information will be recorded to ensure that your answers will remain completely anonymous. However, if you would like a copy of the results of this research, I'll provide it to you upon request.

How You Were Selected: You were selected to take this survey because you belong to one of the organizations that have agreed to participate in this research effort: the International Association of Chiefs of Police or the Fraternal Order of Police.

Time Required: This survey should take no longer than 15 minutes to complete.

a. What state do you currently work in? _____

b. Years in Law Enforcement: ____ Years ____ Months

c. Primary Duty Description: (circle one)

Patrol Investigator Laboratory Administration/Clerical

Supervisor Other

d. Professional Organization: (circle one) FOP IACP

Section 1

1. How frequently do you personally use each system/program listed below:

1 – never
2 – not very often
3 – often
4 – frequently
5 – constantly

	1	**2**	**3**	**4**	**5**
a. AGILE (Advanced Generation of Interoperability for Law Enforcement)	☐	☐	☐	☐	☐
b. PSWN (Public Safety Wireless Network)	☐	☐	☐	☐	☐
c. OLES (Offices of Law Enforcement Standards)	☐	☐	☐	☐	☐
d. GCJIN (Global Criminal Justice Information Network)	☐	☐	☐	☐	☐
e. RISS (Regional Information Sharing System)	☐	☐	☐	☐	☐
f. JABS (Joint Automated Booking System)	☐	☐	☐	☐	☐
g. IDENT-INS	☐	☐	☐	☐	☐
h. NIPC (National Infrastructure Protection Center)	☐	☐	☐	☐	☐
i. UCR/NIBRS (Uniform Crime Reporting/ National Incident Based Reporting System)	☐	☐	☐	☐	☐
j. LEO (Law Enforcement On-Line)	☐	☐	☐	☐	☐
k. NICS (National Instant Criminal Background Check System)	☐	☐	☐	☐	☐
l. NIBIN (National Integrated Ballistics Information Network)	☐	☐	☐	☐	☐
m. CODIS (Combined DNA Index System)	☐	☐	☐	☐	☐
n. IAFIS (Integrated Automated Fingerprint Identification System)	☐	☐	☐	☐	☐
o. III (Interstate Identification Index)	☐	☐	☐	☐	☐
p. CJIS WAN (Criminal Justice Information Services Wide Area Network)	☐	☐	☐	☐	☐
q. NCIC Net (National Crime Information Center Network)	☐	☐	☐	☐	☐
r. FinCEN (Financial Crimes Enforcement Network)	☐	☐	☐	☐	☐
s. NLETS (National Law Enforcement Telecommunications Network)	☐	☐	☐	☐	☐
t. NDPIX (National Drug Pointer Index)	☐	☐	☐	☐	☐
u. CWIN (Cyber Warning Information Network)	☐	☐	☐	☐	☐
v. Federal law enforcement agency websites	☐	☐	☐	☐	☐

Section 2

2. In your opinion, how effectively does each system/program help you to accomplish your duties:

1 – not useful at all
2 – slightly useful
3 – somewhat useful
4 – very useful
5 – extremely useful
n/a – either don't use the system or don't have access

	1	**2**	**3**	**4**	**5**	
a. AGILE (Advanced Generation of Interoperability for Law Enforcement)	☐	☐	☐	☐	☐	n/a
b. PSWN (Public Safety Wireless Network)	☐	☐	☐	☐	☐	n/a
c. OLES (Offices of Law Enforcement Standards)	☐	☐	☐	☐	☐	n/a
d. GCJIN (Global Criminal Justice Information Network)	☐	☐	☐	☐	☐	n/a
e. RISS (Regional Information Sharing System)	☐	☐	☐	☐	☐	n/a
f. JABS (Joint Automated Booking System)	☐	☐	☐	☐	☐	n/a
g. IDENT-INS	☐	☐	☐	☐	☐	n/a
h. NIPC (National Infrastructure Protection Center)	☐	☐	☐	☐	☐	n/a
i. UCR/NIBRS (Uniform Crime Reporting/ National Incident Based Reporting System)	☐	☐	☐	☐	☐	n/a
j. LEO (Law Enforcement On-Line)	☐	☐	☐	☐	☐	n/a
k. NICS (National Instant Criminal Background Check System)	☐	☐	☐	☐	☐	n/a
l. NIBIN (National Integrated Ballistics Information Network)	☐	☐	☐	☐	☐	n/a
m. CODIS (Combined DNA Index System)	☐	☐	☐	☐	☐	n/a
n. IAFIS (Integrated Automated Fingerprint Identification System)	☐	☐	☐	☐	☐	n/a
o. III (Interstate Identification Index)	☐	☐	☐	☐	☐	n/a
p. CJIS WAN (Criminal Justice Information Services Wide Area Network)	☐	☐	☐	☐	☐	n/a
q. NCIC Net (National Crime Information Center Network)	☐	☐	☐	☐	☐	n/a
r. FinCEN (Financial Crimes Enforcement Network)	☐	☐	☐	☐	☐	n/a
s. NLETS (National Law Enforcement Telecommunications Network)	☐	☐	☐	☐	☐	n/a
t. NDPIX (National Drug Pointer Index)	☐	☐	☐	☐	☐	n/a
u. CWIN (Cyber Warning Information Network)	☐	☐	☐	☐	☐	n/a
v. Federal law enforcement agency websites	☐	☐	☐	☐	☐	n/a

Section 3

To what extent do you agree with the following statements:

1 – completely disagree
2 – somewhat disagree
3 – neither agree nor disagree
4 – somewhat agree
5 – completely agree

	1	2	3	4	5
3. Federal LE information systems provide adequate support to my department.	☐	☐	☐	☐	☐
4. Federal law enforcement agencies allow my department access to necessary case-related information to complete our job	☐	☐	☐	☐	☐
5. Federal law enforcement agencies allow my department access to classified information to complete our job	☐	☐	☐	☐	☐
6. Federal law enforcement agencies collaborate well with my department through information systems	☐	☐	☐	☐	☐
7. Federal LE information system programs have taken my department's capabilities into account	☐	☐	☐	☐	☐
8. I believe I have access to the federal criminal justice information networks I need to do my job effectively	☐	☐	☐	☐	☐
9. In this question, "flexible" refers to the ability of an information system to accommodate different network operating systems: Federal LE information systems are flexible enough to support my department's network	☐	☐	☐	☐	☐
10. Information systems technology in federal law enforcement agencies is behind-the-times	☐	☐	☐	☐	☐
11. I believe the information contained on federal criminal justice information networks is adequately protected	☐	☐	☐	☐	☐
12. I believe I get more information from federal law enforcement agencies through interpersonal contact than I get through electronic systems	☐	☐	☐	☐	☐
13. I think my department is sometimes more informed about situations than federal law enforcement offices	☐	☐	☐	☐	☐
14. I believe the information contained on federal criminal justice information networks is accurate	☐	☐	☐	☐	☐

	1	2	3	4	5
15. I believe that state-run criminal justice information networks typically provide more helpful information than federal criminal justice information networks	☐	☐	☐	☐	☐
16. I believe the information contained on federal criminal justice information networks is updated frequently enough	☐	☐	☐	☐	☐
17. I believe the information contained on federal criminal justice information networks is kept long enough	☐	☐	☐	☐	☐
18. I believe the information contained on federal criminal justice information networks is discarded too quickly	☐	☐	☐	☐	☐
19. Federal law enforcement agencies readily share information/ resources when I need/identify them	☐	☐	☐	☐	☐
20. Federal law enforcement agencies quickly respond to my requests for help/information.	☐	☐	☐	☐	☐
21. I trust the information I receive from federal law enforcement agencies	☐	☐	☐	☐	☐
22. I trust the capabilities of federal law enforcement agencies to gather effective intelligence about emerging threats	☐	☐	☐	☐	☐
23. I trust the federal law enforcement agencies' abilities to react to emerging, critical situations	☐	☐	☐	☐	☐
24. I believe federal law enforcement agencies are prepared to deal with the existing level of serious national criminal activities	☐	☐	☐	☐	☐
25. I'm satisfied with federal law enforcement agencies' day-to-day interactions with my department	☐	☐	☐	☐	☐
26. I believe federal law enforcement agencies are receptive to feedback from my department	☐	☐	☐	☐	☐

Comments: Please provide any additional comments about federal criminal justice information systems and/or information sharing between federal and state/local LE agencies in the area provided below.

Thank you for completing this survey.

Bibliography

AFOSI. 2002. *Fact Sheet: Air Force Office of Special Investigations.* Washington DC: Author.

AGILE. 2002. *Standards for Wireless Interoperability and Information Sharing.* Washington DC: National Institute of Justice.

ATF. 2001. *ATF Snapshot – 2001.* Washington DC: Author.

Canterbury, C. 2001. *Homeland Defense and Sharing Information with Local Law Enforcement.* Washington DC: Author.

CIA. 2002. *Factbook on Intelligence.* Retrieved on September 18, 2002 from www.odci.gov.

CIO Magazine. 2001. Why Integrate? July 1: 19-26.

Cohen, W. 1994. *Computer Chaos: Billions Wasted Buying Federal Computer Systems.* Washington DC: Author.

Columbine Review Commission. 2001. *The Report of Governor Bill Owens' Columbine Review Commission.* Denver, CO: State of Colorado.

Council on Foreign Relations. 2002. *FBI and Law Enforcement.* Washington DC: Author.

Criminal Justice Information Systems (CJIS). 2002. *Integrated Automated Fingerprint Identification System.* Washington DC: Federal Bureau of Investigations.

Darden, P. 1998. *Federal Government Agrees to Share Radio Frequencies with State of Wisconsin for Interoperability Test Project.* Washington DC: Department of Commerce.

DEA. 2002. *DEA Mission Statement.* Washington DC: Author.

Dean, J. 2001. FBI Awards Contract to Update Aging Computers. *DailyFed*, 21(1): 1.

Dempsey, J. X. 2000. *Overview of Current Criminal Justice Information Systems.* Washington DC: Center for Democracy and Technology.

Department of Justice. 2002. *Department of Justice Requests $30.2 Billion to Prevent and Combat Terrorism, Continue the Fight Against Drugs, Ensure Civil Rights.* Washington DC: Author.

Department of the Treasury. 2002. *Treasury Announces USA Patriot Act Regulations to Improve Information Sharing.* Washington DC: Author.

Dizard III, W. P. 2002. Project Will Bring Multimedia Case Files to Agents' Desktops. *Government Computer News*, 21(2): 178.

Drug Enforcement Administration. 2002. *Making the Department More Efficient and More Responsive.* Washington DC: Author.

Drug Enforcement Administration. 2002. *National Drug Pointer Index*. Washington DC: Author.

Edwards, B. 2002. *Regional Information Sharing System.* Washington DC: Institute for Intergovernmental Research.

FBI. 2002. *About Us.* Washington DC: Author.

Federal Bureau of Investigation. 2002. *CODIS – Mission Statement and Background.* Washington DC: Author.

Federal Bureau of Investigation. 2002. *Headquarters and Programs.* Washington DC: Author.

Federal Bureau of Investigation. 2002. *LEO: Law Enforcement Online.* Washington DC: Author.

Federal Bureau of Investigation. 2002. *National Instant Criminal Background Check System Fact Sheet.* Washington DC: Author.

Federal Bureau of Investigation. 2002. *Uniform Crime Reporting/National Incident-Based Reporting System.* Washington DC: Author.

Federal Computer Week. 2002. Take a Lesson From Trilogy. July 29: 86-87.

FEDSIM. 2002. *FEDSIM Millennia Activity List*. Washington DC: General Services Administration.

Fine, G. 2001. *Technology, Terrorism, and Government Information.* Washington DC: Author.

Fink, A. 1995. *How to Design Surveys*. Thousand Oaks, CA: Sage.

Fraternal Order of Police. 2002. "Building on a Proud Tradition: The Voice of Law Enforcement Professionals." Retrieved September 18, 2002 from www.grandlodgefop.org/index.html.

Friel, B. & Saldarini K. 1999. Legal Briefs: Who's a Cop? *DailyFed*, 17(1): 176.

Gonier, D. E. 1999. *The Emperor Gets New Clothes*. New York: Advertising Research Foundation.

GVU. 1994. "GVU's 2nd WWW User Survey." Retrieved December 12, 2002 from www.gvu.gatech.edu/user_surveys/survey-09-1994.htm.

Hair, J. F., R. E. Anderson, R .L. Tatham, and W. C. Black. 1995. *Multivariate Data Analysis with Readings* (4th ed.), New York: Prentice-Hall Inc.

Hauben, M. 2002. History of ARPANET. Retrieved October 1, 2002 from www.dei.isep.ipp.pt/docs/arpa.html.

Higgins, K. 2002. *NIST & Law Enforcement: Technical Partnerships for Public Safety and Security*. Washington DC: Nation Institute of Standards and Technology.

Higgins, S. 2002. *FBI Infrastructure.* Washington DC: Author.

Homeland Security Monitor. 2002. "Homeland Security Conference Report." Retrieved August 4, 2002 from www.homelandsecuritymonitor.com/ConferenceReport.htm.

Iacono, C. S. & Weisband S. 1997. *Developing Trust in Virtual Teams.* Presented at the 30th Annual Hawaii International Conference on System Sciences, Honolulu.

Immigration and Naturalization Service. 2001. *Immigration and Naturalization Service Restructuring Proposal.* Washington DC: Author.

Infragard. 2002. "About Infragard." Retrieved October 4, 2002 from www.infragard.net.

INS. 2002. *Mission, Strategies, and Performance.* Washington DC: Author.

International Association of Chiefs of Police. 2002. "About IACP." Retrieved October 5, 2002 from www.theiacp.org/about/about.htm.

Johnson, K. 2002. "Police Infuriated Over FBI Program." Retrieved September 18, 2002 from 209.157.64.200/focus/news/726764/posts.htm.

Jordan, R. J. 2002. *Information Sharing Initiatives.* Washington DC: Author.

Kling, R. 1999. What is Social Informatics and Why Does It Matter? *D-Lib Magazine*, January: 99-104.

Kling, R. 2000. Learning about Information Technologies and Social Change: The Contribution of Social Informatics. *The Information Society*, 16(3): 217-232.

Kling, R. 2001. Social Informatics. In *Encyclopedia of LIS*. Norwell, MA: Kluwer Publishing.

Kwak, N. & Radler B. T. 1999. *A Comparison Between Mail and Web-based Surveys: Response Pattern, Data Quality, and Characteristics of Respondents.* Presented at 1999 Annual Research Conference, Chicago.

Leahy, P. 1998. *Crime Identification Technology Act of 1998, S. 2022*. Washington DC: Author.

Legal Information Institute. 2002. "Title 5, Part III, Subpart G, Chapter 84, Subchapter 1, Section 8401." Retrieved November 26, 2002 from www4.law.cornell.edu/cgi-bin/htm.

Litwin, M. 1995. *How to Measure Survey Reliability and Validity.* Thousand Oaks, CA: Sage.

Manfreda, K. L., Vehovar, V., & Batagelj Z. 2001. Web Versus Mail Questionnaire for an Institutional Survey. In A. Westlake et al (Ed.), *The Challenge of the Internet*: 1-11. Chesham, UK: Association for Survey Computing.

McClave, J. T., Benson, P. G., & Sincich, T. 2001. *Statistics for Business and Economics: Eighth Edition*. Upper Saddle River, NJ: Prentice Hall.

Meyerson, D., Weick, K. E., & Kramer, R. M. Swift trust and Temporary Groups. In R. M. Kramer & T. R. Tyler (eds.), *Trust in Organizations* (pp. 166-195). Thousand Oaks, CA: Sage Publications.

Miller, J. J. 2001. A Junior al-Qaeda…Right Here at Home: Meet al-Fuqra. *National Review*, 52: 19-20.

Motorola Corp. 2002. Utah Public-Safety Agencies Honor Governor Leavitt for Role in New Shared Communications System. May 16: 2020.

Mueller III, R. S. April 2002. *Press Release.* Washington DC: Author.

Mueller III, R. S. May 2002. *FBI Reorganization.* Washington DC: Author.

Mueller III, R. S. June 2002. *A New FBI Focus.* Washington DC: Author.

Mueller III, R. S. July 2002. *Press Release.* Washington DC: Author.

National Communications System. 2002. *Background and History*. Washington DC: Author.

National Infrastructure Protection Center. 2002. *What's New*. Washington DC: Author.

National Infrastructure Protection Center. 2002. *Outreach.* Washington DC: Author.

National Institute of Standards and Technology. 2002. *Office of Law Enforcement Standards: Mission.* Washington DC: Author.

National Law Enforcement Telecommunications System. 2002. *NLETS History.* Washington DC: Author.

Newton, H. & Horak, R. 2002. *Newton's Telecom Dictionary: The Authoritative Resource for Telecommunications, Networking, the Internet and Information Technology (18th Edition).* Gilroy, CA: CMP Books.

NIBIN Branch. 2002. *ATF's NIBIN Program.* Washington DC: Author.

NLECTC. 2002. *'Why Can't We Talk?' When Lives Are at Stake.* Washington DC: National Institute of Justice.

Nunnally, J. C. 1978. *Psychometric Theory*. New York: McGraw-Hill.

Pike, J. 2002. *National Crime Information Center (NCIC).* Washington DC: Federal Bureau of Investigation.

Prout, M. J. 2001. *INS Restructuring.* Washington DC: Author.

Public Safety Wireless Networks. 2002. *PSWN Strategic Plan.* Washington DC: Author.

Puzzanghera, J. 2002. Defending the U.S. *San Jose Mercury News*, 30(1): 1.

Quijas, L. F. 2002. "Ask the FBI: Law Enforcement Coordination." Retrieved September 18, 2002 from www.usatoday.com/community/chat/2002-06-18-fbi.htm.

Rea, L. M. & Parker, R. A. 1997. *Designing and Conducting Survey Research*. San Francisco, CA: Jossey-Bass Inc.

Robinson, M. D. 2002. *The Global Justice Information Network Initiative.* Detroit, MI: Author.

Rohrer, R. 2002. *Securing Kansas Criminal Justice Information*. Topeka, KS: Kansas Bureau of Investigation.

Rowley, C. M. 2002. *Oversight Hearing on Counterterrorism.* Washington DC: Author.

SAIC. 2002. "Case Study: SAIC's Federal Bureau of Investigation (FBI) Interstate Identification Index (III) Program." Retrieved September 18, 2002 from www.saic.com/integration/fbi.html.

Schmitt, N. W. & Klimoski, R. J. 1991. Assessing Employee Attitudes and Opinions. In *Research Methods in Human Resources Management*, 326-368. Cincinnati, OH: South-Western Publishing.

Shannon, David M. & Davenport, Mark A. 2001. *Using SPSS to Solve Statistical Problems: A Self-Instructing Guide*. Columbus, OH: Merrill-Prentice Hall.

Sheard, J., Carbone, A & Markham, S. 2000. "Survey of Student Reactions to Learning Visual Basic and COBOL." Retrieved December 19, 2002 from www.cerg.csse.monash.edu.au/reports/vb_cobol.htm.

Siegle, D. 2002. "Likert Scale." Retrieved December 19, 2002 from 137.99.89.70:8001/siegle/research/instrument.htm.

Smith, H. 2001. "Statistical Measures." Retrieved March 29, 2003 from home.wlu.edu/~journalism/J203/statistic.htm.

Solomon, D. J. 2001. "Conducting Web-based Surveys." Retrieved December 21, 2002 from ericae.net/pare/getvn.asp.

Sorum, C. 2002. *Law Enforcement On-Line.* Washington DC: Federal Bureau of Investigation.

Souder, M. 2001. *U.S. Representative Mark Souder (R-IN) Holds Hearing on the Role of Federal Law Enforcement in Long-Term Homeland Security.* Washington DC: Author.

South Dakota Division of Criminal Investigation. 2002. *National Integrated Ballistics Information Network (NIBIN).* Pierre, SD: Author.

Tritak, J. S. 2002. *Critical Infrastructure Assurance.* Washington DC: Author.

Upcraft, M. L. & Wortman, T. I. 2002. "Web-based Data Collection and Assessment in Student Affairs." Retrieved December 21, 2002 from www.studentaffairs.com/ejournal/Fall_2000/art1.htm.

US Customs. 2002. *Who Are the United States Customs Service?* Washington DC: Author.

US Treasury. 2002. *Secret Service History.* Washington DC: Author.

USCG. 2002. *The Essence of the Coast Guard: America's Maritime Guardians.* Washington DC: Author.

USDA Faculty Exchange Program. 2001. "Outcome I – Expansion of Knowledge." Retrieved December 19, 2002 from fep.vsau.ru/info/mary/outcomeI.htm.

USMS. 2002. *United States Marshals Service: America's Oldest Federal Law Enforcement Agency*. Washington DC: Author.

Vaida, B. 2001. Cybersecurity Chief Pushes Early-Warning System. *DailyFed*, 47(1): 1.

Ward, M. 2002. "Hacking with a Pringle's Tube." Retrieved October 4, 2002 from http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm.

Wartell, J. 2000. *Technology Acquisition Project Case Study: Kansas Criminal Justice Information System.* Washington DC: National Institute of Justice.

Whiting, R. & Chabrow, E. 2001. Safety in Sharing. *Information Week*, 40: 2-6.

Ziglar, J. W. 2001. *Federal Law Enforcement.* Washington DC: Author.

Vita

Captain David R. Dethlefs was commissioned in September, 1995, through the Officer Training School at Maxwell AFB, Alabama. His first assignment was the 38th Engineering and Installation Squadron at Tinker AFB, Oklahoma, where he worked as a program manager for various communications systems including meteorological and navigation, tactical secure voice, and information transfer systems. While there, Captain Dethlefs deployed to Egypt in support of Operation PEACE VECTOR.

Captain Dethlefs was then assigned to Cannon AFB, New Mexico where he filled various communications officer roles supporting the 27th Fighter Wing. He first served as the Support Flight commander in the 27th Communications Squadron. After seven months as the Support Flight commander, Captain Dethlefs was transferred to the Information Systems Flight where he served as the Chief of the Network Control Center. While serving in this role, Captain Dethlefs deployed to Sarajevo, Bosnia-Hercegovina in support of Operation JOINT FORGE. While deployed, he supported voice and video teleconferencing capabilities throughout the area of responsibility, including Bosnia and Croatia and expanding to include Albania and Macedonia after the Kosovo crisis began. Upon return from Bosnia, Captain Dethlefs moved to the 27th Logistics Group where he served as the executive officer for the remainder of his tour.

He then volunteered for an overseas remote tour at Kunsan AB, Republic of Korea where he served as the wing executive officer for 14 months. And for the past 18 months, Captain Dethlefs has been a student in the Information Systems Management program at the Air Force Institute of Technology.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
09-04-2003	**Master's Thesis**	Jun 2002 – Mar 2003

4. TITLE AND SUBTITLE

INFORMATION SHARING AND INTEROPERABILITY IN LAW ENFORCEMENT: AN INVESTIGATION OF FEDERAL CRIMINAL JUSTICE INFORMATION SYSTEMS USE BY STATE/LOCAL LAW ENFORCEMENT ORGANIZATIONS.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dethlefs, David R., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/03-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis investigates the frequency of use and perceptions of usefulness of federal criminal justice information systems among state and local law enforcement personnel and certain IS environmental factors that affect usage. The study is predicated by a demonstrated need for increased information sharing, interoperability, and collaboration among the three tiers of law enforcement as public safety threats within U.S. borders increase in complexity; e.g., the Murrah Federal Building bombing, Columbine High School shooting, 9/11 terrorist attacks, and D.C. sniper case. The results of this research indicate high usage and perceived usefulness of the National Crime Information Center Network (NCIC Net), National Law Enforcement Telecommunications System (NLETS), Uniform Crime Reporting/National Incident Based Reporting System (UCR/NIBRS), National Instant Criminal Background Check System (NICS), and federal LE websites. The results also indicated that the IS environmental factors information quality and trust influenced the usage and perceived usefulness of federal criminal justice information systems.

15. SUBJECT TERMS

Law Enforcement, Information Sharing, Information Technology, Criminal Justice Information Systems, Interoperability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Summer E. Bartczak, Lt Col, USAF (ENV)
U	U	U	UU	169	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4826; e-mail: summer.bartczak@afit.edu