EXECUTIVE SUMMARY

JUSTICE INFORMATION TECHNOLOGY FOCUS GROUP

Assessing the Implications of the Terrorist Attacks on America for Justice Information and Technology

BJA Bureau of Justice Assistance, U.S. Department of Justice

SEARCH The National Consortium for Justice Information and Statistics

This Executive Summary was written by Linda Townsdin, Writer-Editor, SEARCH Corporate Communications, and David J. Roberts, SEARCH Deputy Executive Director.

This report was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Gerald E. Wethington, Chairman, and Gary R. Cooper, Executive Director, as a product of a project funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, under Cooperative Agreement No. 1999-DD-BX-0069, awarded to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831. (916) 392-2550. www.search.org. Contents of this document do not necessarily reflect the views or policies of the Bureau of Justice Assistance or the U.S. Department of Justice.

Assessing the Implications of the Terrorist Attacks on America for Justice Information and Technology

The tragic events of September 11 have profoundly changed the world. In light of these unprecedented events, a host of legislative and policy measures have been planned or implemented to bolster security at the nation's airports and international borders, as well as key government buildings and critical infrastructure. In addition to these direct enhancements of physical/plant security, there are growing calls for programs and technologies to establish and verify the positive identity of people — flight training applicants, airline passengers, airline/airport employees, visa/admissions applicants — and a need to link these systems for positive identification to critical databases for background screening.

On December 11-12, 2001, three months after the attacks on the World Trade Center and the Pentagon, over 50 experts from local, state, and federal governments, and the private sector gathered in Washington, D.C., to assess the implications of the terrorist attacks on America for justice information and technology.

The *Justice Information Technology Focus Group: Assessing the Implications of the Terrorist Attacks on America for Justice Information and Technology*, was co-sponsored by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice and SEARCH, The National Consortium for Justice Information and Statistics.[1] The principal objectives of this one-and-one-half day Focus Group included: 1) examining federal policy, legislative, and regulatory initiatives that have emerged since the September 11 attacks; 2) evaluating the technical and operational capabilities of available technologies to address the broad objectives of the initiatives, and the range of information available in existing and planned databases; and 3) assessing the information technology (IT) and business practice implications of these initiatives for state and local justice agencies.

[1] The Bureau of Justice Assistance is a component of the Office of Justice Programs within the U.S. Department of Justice. The Office also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. SEARCH, The National Consortium for Justice Information and Statistics, is a nonprofit consortium, created by and for the states, governed by a Membership Group of governor appointees, and dedicated to improving the criminal justice system through better information management and the effective application of information and identification technology and responsible law and policy. A detailed report summarizing observations and issues discussed at the *Justice Information Technology Focus Group: Assessing the Implications of the Terrorist Attacks on America for Justice Information and Technology*, will be available in Spring 2002.

The Focus Group made the following key observations:

- There have been two primary federal legislative initiatives since September 11: l) the USA Patriot Act; and 2) the Aviation and Transportation Security Act. Both authorize new background checks, and both reference the use of biometric technologies. The Aviation and Transportation Security Act suggests a passenger screening system.

- The activity in Washington now shifts from the legislative arena to the Executive Branch and, specifically, to the Department of Transportation and the new Under Secretary for Security; to the Federal Aviation Administration; to the intelligence agencies; and to the FBI and the Department of Justice.

- The one remaining legislative priority is to enact substantive immigration reform, including the application of numerous biometric and other technologies to identify individuals entering the country; to keep track of those individuals while they are in the country; and to validate the event when these individuals leave the country.

- No one biometric or other technology is a magic bullet. Rather, a combination of technologies is required.

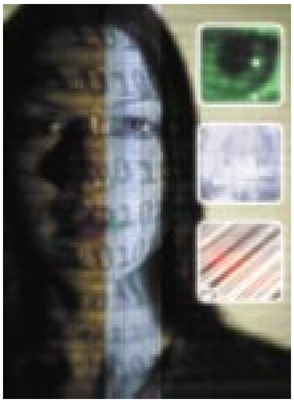
- Information sharing and overall cooperation and teaming is required for the war on terrorism. This includes not only cooperation from federal, state, and local public sector entities, but also assistance from private sector entities.

- The state and local infrastructure needs development and specifically, federal assistance, in order to interface effectively with the federal IT infrastructure.

- It is critical for the nation to define its goals in the war on terrorism, and to develop suitability standards for access to secure areas and or participation in particular programs (such as a passenger screening program). At present, the substantive criterion for admission and/or participation is undefined or unclear and, therefore, the information and IT resources that should be brought to bear are similarly unclear and/or undefined.

Following is a more detailed summary of the initiatives, the technologies behind the initiatives, and IT implications for state and local justice agencies.

Information sharing ... is required for the war on terrorism.



No one biometric or other technology is a magic bullet. Rather, a combination of technologies is required.

State and Federal Policy, Legislative, and Regulatory Initiatives

Legislative and policy initiatives emerging as a result of the terrorist attacks share several common objectives: identification, tracking, and exclusion of known terrorists, increasing use of identity verification and biometric technologies, and expanded use of background investigations to determine suitability and security clearance for access to key resources.

A *biometric* technology refers to unique and measurable physical, biological, or behavioral characteristics that can be processed electronically, to establish identification, identity verification, or automated recognition of a living person. *Identification* refers to the use of these technologies to identify a single individual from an entire population. *Identity verification* seeks to verify the identity of a person by comparing a contemporaneous biometric measure (e.g., a fingerprint) with comparable information stored in an identification card or database. *Suitability* customarily refers to an assessment (based on factors as yet undefined) of the trustworthiness and the security of a person for access or admission to secure locations and resources.

The Aviation and Transportation Security Act, for example, is one of the initiatives that emphasizes identity verification using biometric technologies. This and other programs may enable voluntary expedited security screening of participating passengers using "available" technologies, including a computer-assisted passenger prescreening system to score passengers. The USA Patriot Act also promotes identity verification initiatives that use biometric technologies — a fingerprint scanning system with access to the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Primary objectives of these and other federal and state initiatives are:

1) To identify and exclude known terrorists from entering the country, boarding planes, or gaining access to critical areas or structures; and

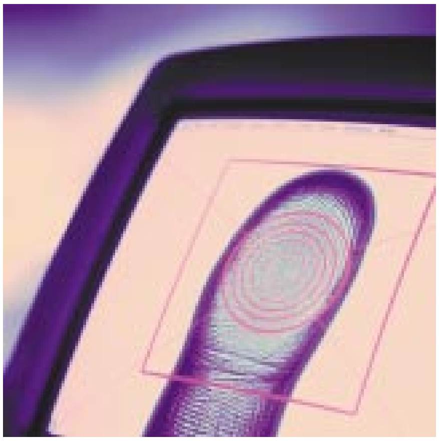
2) To assess the suitability of people to have access to secured areas and resources through identity verification and background checks.

Focus Group participants discussed the importance of information sharing and linkage of information systems among federal agencies to identify who is entering the country, determine how long they are allowed to stay, and when they leave. Systems currently in place are unable to accomplish this level of tracking.

One of the central issues discussed by Focus Group participants was the importance of having a biometrically based national identification capability. The group recognized concerns regarding creation of a national identification system. American Association of Motor Vehicle Administrators (AAMVA) representatives discussed their initiative to strengthen the current driver's license identification system through the development of uniform standards and procedures, and the addition of a biometric identifier(s) (e.g., digital photograph, fingerprint, etc.). The Focus Group acknowledged that state-issued driver's licenses and other identification cards have effectively become *de facto* standards for identification throughout the nation, and expanding upon the use of the license as a means of identification would be less intrusive than creating a new national ID system. Concerns were raised, however, over the need to establish a method to authenticate identity before the license or other identification card is issued.

Technologies Behind the Initiatives

The counter-terrorism initiatives presume the existence of a broad range of biometric technologies that can securely and positively establish the identity of an individual. The Focus Group discussed a number of these technologies, including DNA profiles, facial recognition, hand geometry, retinal and iris scans, fingerprint imaging, voice recognition, and other biometric measures. Participants debated key issues surrounding the technologies, such as accuracy and effectiveness, public support, operational implementation and support factors, environmental limitations, initial and on-going costs, subject cooperation, forensic capabilities, and the existence, size, and quality of databases relative to each of these biometric technologies. Further, the Focus Group recognized potential benefits that might be derived by layering or deploying combinations of biometric technologies.



In addition to the range of available biometric technologies, participants discussed complex issues related to the different purposes and the suitability of these technologies. For example, inconspicuous facial recognition cameras placed at strategic locations can scan airport crowds and match people to a computer database of known terrorists. The effectiveness of this application, however, is contingent not only on the capabilities of the technology, but also on the existence of a database of known terrorists with images of sufficient quality and immediate access. The implementation of a "trusted passenger" travel card, voluntarily used by airline passengers to validate identity and expedite their movement through security processes, requires rather different technologies and access to appropriate databases.

Focus Group participants recognized the potential privacy implications of many of these technologies, yet noted that since the September 11 attacks, surveys have indicated that the public is increasingly willing to surrender some personal privacy to improve security. Participants observed that application objectives, costs, and environmental implementation issues will determine which biometric technology is most appropriate in any given setting, and multiple measures will most likely be required. The Focus Group agreed that no single biometric technology is the answer for all applications, and the challenge for any immediate deployment of technologies is to assist Congress and agency administrators in identifying the benefits and limitations of these technologies.

Information Technology Implications for State and Local Justice Agencies

Focus Group participants agreed that cooperation among federal, state, and local jurisdictions, as well as industry, is crucial to successful implementation of the new initiatives. A primary observation by the Focus Group was the importance of clearly articulating objectives for the initiatives, and identifying and defining suitability and security criteria. Linkage and development of appropriate databases and broad information sharing are critical factors in addressing the national initiatives, but this can only be effectively accomplished once valid and reliable suitability and security criteria are defined.

Participants also recognized the significant operational implications of substantial increases in background investigations. Participants acknowledged that many agencies at state and local levels are already pushing the limits of available resources for conducting background checks, and that jurisdictions may need assistance in responding to what may be unprecedented growth in background investigations as these legislative and policy initiatives are implemented.

For successful and widespread implementation of the new technologies at the state and local levels, the IT Focus Group emphasized the following needs:

- Establishing and verifying subject identity at key decision points is increasingly important, particularly in light of the attacks on September 11. Different technologies will be appropriate in different applications. The risks and consequences of decisions should be weighed with the nature, effectiveness, and costs of technologies in determining which (or in what combinations) should be employed at any given point;
- Current legislative and policy initiatives presume significant levels of automation and online reporting and access capabilities among justice and governmental agencies throughout the nation. Substantial investment and expansion of these technical capabilities is essential

in meeting the objectives;

- Significant federal resources should be immediately focused on the development and testing of valid, reliable, and appropriate suitability and security measures. National databases and information-sharing capabilities may need to be developed, broadly supported, and universally accessible; and
- The federal government will need to make significant investment (perhaps $20 billion or more) in infrastructure development, research, equipment procurement and implementation, and systems development and integration at and between local, state, and federal information systems to accomplish the objectives of current legislative and policy initiatives.

Conclusion

Focus Group participants observed that the emerging technologies can accomplish many of the objectives of the legislative and policy initiatives, but infrastructure development is a key issue for state and local agencies to implement effective identification strategies. Additionally, support is needed for expanded levels of automation at the state and local levels, and for standards development efforts to enable broad scale sharing of critical data in support of the national initiatives. Participants also supported development of appropriate national databases and expansion of nationwide telecommunication capabilities. National leadership and funding for these initiatives must be provided if we are to achieve the objectives, and the American public must be shown how these efforts will improve public safety.

Roster of Participants

Justice Information Technology Focus Group: Assessing the Implications of the Terrorist Attacks on America for Justice Information and Technology

December 11-12, 2001
Washington D.C.

Ms. Lana Adams
Senior Program Analyst
Investigations Service
U.S. Office of Personnel Management

Mr. Francis X. (Paco) Aumand, III
Director
Division of Criminal Justice Services
Vermont Department of Public Safety

Mr. Sheila J. Barton
Deputy Executive Director and In-house Counsel
SEARCH

Mr. Robert R. Belair
SEARCH General Counsel
Mullenholz, Brimsek and Belair

Mr. George H. Bohlinger
Executive Associate Commissioner
Immigration and Naturalization Service
U.S. Department of Justice

Mr. Francis L. Bremson
Director, Courts Program
SEARCH

Mr. Gary R. Cooper
Executive Director
SEARCH

Mr. Tom Coty
Senior Program Manager
Office of Science and Technology
National Institute of Justice
U.S. Department of Justice

Ms. Katy Crooks
Counsel, Subcommittee on Crime
Committee on the Judiciary
U.S. House of Representatives

Ms. Laura DeOrio
Meeting Planner
SEARCH

Mr. Jeffrey Dodge
Senior Vice President
Corporate Development & Strategy
Equifax, Inc.

Mr. Douglas Domin
Vice President
SAIC

Mr. Steven Emmert
Director
Government and Industry Affairs
Reed Elsevier/Lexis/Nexis

Mr. Rusty Featherstone
Director
Information Services Division
Oklahoma State Bureau of Investigation

Mr. John Ford
Chief Privacy Officer
Equifax, Inc.

Mr. Owen M. Greenspan
Justice Information Services Specialist
SEARCH

Mr. Robert E. Greeves
Consultant
Office of Justice Programs
U.S. Department of Justice

Ms. Kelly J. Harris
Director
Justice Information Technology Services
SEARCH

Dr. Thomas A. Henderson
Executive Director
Office of Government Relations
National Center for State Courts

Mr. Bill Holcombe
Director, E-Business Technology
U.S. General Services Administration

Mr. John Hooks, Jr.
Section Chief
Resource Management Section
Criminal Justice Information Services Division
Federal Bureau of Investigation

The Bureau of Justice Assistance, U.S. Department of Justice, and SEARCH would like to thank all participants for their valuable time and expertise in helping to understand and evaluate these complex issues. This dialogue will be useful for legislators and policymakers at the state and local levels, and for federal agencies who are managing the resources critical to achieving these objectives.

Ms. Carol G. Kaplan
Chief, National Criminal History
Improvement Programs
Bureau of Justice Statistics
U.S. Department of Justice

Ms. Linda Lewis
President and Chief Executive Officer
American Association of Motor
Vehicle Administrators

Mr. Anthony Lowe
Minority Senior Legislative Counsel
Subcommittee on Antitrust, Business
Rights & Competition
Committee on the Judiciary
U.S. Senate

Mr. George P. March
Director
Office of Information Technology
Regional Information Sharing
Systems

Mr. J. Patrick McCreary
Special Assistant
Bureau of Justice Assistance
U.S. Department of Justice

Mr. Joe McDevitt
Vice President, Large System Sales
Pelco

Ms. Elizabeth Miller
Executive Director
National Association of State Chief
Information Officers

Mr. Frank Minice
Director of Operations
National Law Enforcement
Telecommunications System

Ms. Mary J. Mitchell
Program Executive
Electronic Government Policy
U.S. General Services Administration

Mr. Samir Nanavati
Partner
International Biometric Group, LLC

Mr. Allen Nash
Management Analyst
Programs Development Section
Criminal Justice Information
Services Division
Federal Bureau of Investigation

Mr. Richard R. Nedelkoff
Director
Bureau of Justice Assistance
U.S. Department of Justice

Mr. Thomas J. O'Reilly
Administrator
Department of Law and
Public Safety
New Jersey Office of the
Attorney General

Mr. Rock Regan
Chief Information Officer
Connecticut Department of
Information Technology

Mr. David J. Roberts
Deputy Executive Director
SEARCH

Col. Michael D. Robinson
Director
Michigan State Police

Mr. William H. Romesburg
Consultant
SEARCH

Mr. Daniel N. Rosenblatt
Executive Director
International Association of
Chiefs of Police

Mr. Thom Rubel
Director
State Information Technology
Policy
Center for Best Practices
National Governors' Association

Mr. Theron A. Schnure
Assistant Division Director
Policy Development and Planning
Division
Connecticut Office of Policy and
Management

Mr. Charles W. Sexson
Assistant Director
Criminal Justice Information
Services Division
Kansas Bureau of Investigation

Mr. James F. Shea
Assistant Director
Office of Systems
New York State Division of Criminal
Justice Services

Mr. David M. Smith
Transportation Specialist
Safety Core Business Unit
Federal Highway Administration
U.S. Department of Transportation

Ms. Teri B. Sullivan
Justice Information Systems
Specialist
SEARCH

Detective D. W. Todd
Tampa, Florida, Police Department

Ms. Linda Townsdin
Writer/Editor
Corporate Communications
SEARCH

Mr. Richard W. Velde
Attorney-Advisor

Mr. Richard H. Ward, III
Deputy Director
Bureau of Justice Assistance
U.S. Department of Justice

Mr. Paul K. Wormeli
Chairman, Industry Working Group
Viking Technology, Inc.