

A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)

by

**The Global Infrastructure/Standards
Working Group**

December 9, 2004

Global Infrastructure/Standards Working Group (GISWG)

GISWG Members

Lieutenant John F. Aerts
Consolidated Criminal History Reporting
System
Records and Identification Bureau
Los Angeles County, California,
Sheriff's Department

Mr. D. J. Atkinson
U.S. Department of Commerce Laboratories
National Telecommunications and
Information Administration

Chief Philip Broadfoot
Danville, Virginia, Police Department

Tom Clarke, Ph.D.
Supreme Court of Washington

Mr. Steven Correll
National Law Enforcement
Telecommunication
System

Mr. Paul Embley
Practitioner Resource Group

Mr. Scott Fairholm
National Center for State Courts

Mr. Kael Goodman
New York, New York, Departments of
Correction and Probation

Mr. Ronald Hawley
SEARCH, The National Consortium for
Justice
Information and Statistics

Thomas A. Henderson, Ph.D.
National Center for State Courts

Ms. Jennifer Hicks Zeunik
Law Enforcement Information Technology
Standards Council Technology Center
International Association of Chiefs of Police

Mr. John Loverude
Joint Task Force on Rap Sheet
Standardization
Information and Technology Command
Illinois State Police

Mr. John Matthias
Northrop Grumman Mission Systems

Mr. Harlin McEwen
Communications and Technology Committee
International Association of Chiefs of Police

Mr. Michael Ryan
Minnesota Office of Technology

Mr. Bob Slaski
Advanced Technology Systems, Inc.

Mr. Robert Sykora
Minnesota Board of Public Defense

Mr. George Thomas
U.S. General Services Administration

Ms. Richelle Uecker
Superior Court of California

U.S. Department of Justice Participants

Mr. Ken Gill
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Mr. Bob Greeves
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Mr. J. Patrick McCreary
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

GISWG Staff

Ms. Donna Lindquist Rinehart
Institute for Intergovernmental Research

PREFACE

On September 29, 2004, the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) unanimously adopted the following resolution.

The GAC adopts this report (as amended to address privacy and information quality issues) of the Global Infrastructure/Standards Working Group (GISWG), titled *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*.

Global:

- Recognizes SOA as the recommended framework for development of justice information sharing systems;
- Adopts the report's action agenda for its activities to further the utility of SOA for the justice community; and,
- Urges the members of the justice community to take corollary steps in the development of their own systems.

Global's approval was based on the understanding that SOA is an approach that is most likely to result in an infrastructure that will support its vision of how information should be shared among the justice community. That vision can be stated as follows:

Any member of the justice community can access the information they need to do their job, at the time they need it, in a form that is useful, regardless of the location of the data.

Several things about this statement are important. First, the emphasis is upon access to information, not the origin of the data. Second, the focus is on the form, utility, and content of the message that the user receives. And third, it expects that information sharing will cross agency, discipline, and government boundaries. This is an ambitious vision that requires an equally ambitious action agenda.

The report that follows is intended for the manager and policymaker who are responsible for providing the leadership, resources, and management of the justice community. Technologists are already addressing the questions of design, software, and hardware. The more important issues of how SOA will serve the business concerns of the justice community must still be confronted. Only the police, prosecutors, public defenders, judges, court managers, probation officers, corrections officers, and their cohorts in relevant fields, who are responsible for leading and managing their agencies, can resolve these issues. It is to them we commend this report.

Introduction

Information sharing is a long-standing practice among justice agencies, particularly within the law enforcement community. As society becomes more mobile, the importance of sharing data to improve police effectiveness grows exponentially. The technology available has been critical to the ability to share, particularly to the scope of the practice. The kinds of information, the working partnerships, and the types of data exchanged have been transformed as we have moved from paper, telegraphs, telephone, and teletype machines to computers and wireless communications. The arrival of the World Wide Web (the Web) and the technologies that support it have spawned a brave new world of information sharing that goes beyond exchanges among specific partners to embrace the whole of the justice community—law enforcement, prosecutors, defense counsel, courts, probation, corrections—and a host of corollary disciplines such as homeland security, fire, emergency services, health, education, transportation, and motor vehicle licensing.

The purpose of this report is to describe the recommendation of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) for the design and development of an information system architecture that will support both the operational requirements of justice agencies and the requirements for a national system for information sharing among the justice community. Global¹ was created to advise the U.S. Attorney General on strategies for improving the ability of local, state, tribal, and federal justice agencies to share data and information. Global's concept of what justice information sharing means is an ambitious vision of a justice community that is defined in the broadest terms possible, reaching across disciplines, levels of government, and branches of government.

Global's concept of what justice information sharing means is an ambitious vision of a justice community that is defined in the broadest terms possible, reaching across disciplines, levels of government, and branches of government.

The thesis of this report is that the technology now exists to support Global's ambitious vision of justice information sharing and that there is a conceptual framework for exploiting that technology to meet Global's objectives. The technology consists of the standards, specifications, and protocols that have been developed to support the Internet; the conceptual framework is called Service-Oriented Architecture (SOA). Together they hold the promise of building upon the existing information sharing approaches that focus on specific disciplines and subject areas, such as the National Law Enforcement Telecommunication System (NLETS) and the Federal

¹ Global membership is made up of 32 individuals representing the spectrum of justice system entities. It includes 9 local, 14 state, and 9 federal officials. It operates through four working groups titled Privacy and Information Quality, Intelligence, Security, and Infrastructure/Standards. This paper was developed by the Infrastructure/Standards Working Group.

Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division, to define an architecture that can serve the entire justice community.

Public policymakers and justice system managers are critical to the success of the SOA recommended in this paper. The discussion of SOA is drawn from technical literature, but its importance is as much a challenge to how policymakers and managers approach automation and information sharing as it is a guide to technology experts. Policymakers and managers cannot stand back and "leave it to the experts"; instead, they must become active participants in the design, development, and implementation of information systems.

The most important principle articulated in this report is the strong leadership role that policymakers and managers must take in the development of information systems if they are to support information sharing among the justice community. SOA focuses on the business requirements of an agency or process. It assumes an evolutionary approach to system design and development, and it treats funding as a series of strategic investment decisions. These are the provinces of policymakers, not the expertise of technologists.

The most important principle articulated in this paper is the strong leadership role that policymakers and managers must take in the development of information systems if they are to support information sharing among the justice community.

Requirements Analysis

The requirements for an architecture that will support Global's vision are formidable. We begin the discussion with a review of six requirements that the architecture must address.

The architecture must recognize innumerable independent agencies and funding bodies from local, state, tribal, and federal governments.

For anyone connected to the justice community, this requirement is self-evident. One factor has not changed throughout American history: the business of justice is largely the province of local, state, and tribal government. Statistics underscore the enormity of local and state contributions to the American justice community.

Personnel	LOCAL/STATE	FEDERAL	
Law Enforcement ²	666,000	88,500	
Prosecution Personnel	79,000 ³	5,100 ⁴	
Courts	140,000 ⁵	201 ⁶	
Corrections ⁷	330,000	25,379	
Annual Funding⁸ (In millions)	LOCAL \$74,442	STATE \$49,964	FEDERAL \$22,148

Given this organizational landscape, it is not surprising that the Global vision of information sharing among the entire justice community is so revolutionary. The technology available to us for the last forty years was ill-suited to the enormous task this pattern posed. Moving information among a set of workstations across dedicated channels through a central switching point is feasible so long as the number of participants is limited and the purposes are finite. However, the difficulty of the task increases exponentially as the number of participants increase, quickly reaching a point where it becomes tangled spaghetti, impossible to conceive, let alone organize.

Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions.

It is difficult, if not impossible, to define precisely the boundaries of the justice community. The obvious list of participants—law enforcement, prosecution, courts, defense counsel, probation, and corrections—is only the beginning. Accurate, timely, and appropriate justice information sharing among the entities is necessary for effective apprehension, prosecution, adjudication and punishment of an offender. However, these are only some of the objectives.

This same information, or portions of it, is necessary to meet the business requirements of related justice, public safety, and homeland security agencies. For example, this information is required to regulate the sale of firearms; complete criminal background checks of employees at schools, child care services, and elder care facilities; identify aliens who have been convicted of crimes or have entered the country illegally; notify the local community of the release and location of sexual predators; prevent training in the operation of aircraft by aliens or other designated

² Information found at <http://www.ojp-usdoj.gov/lawenf.htm>.

³ Information found at <http://www.ojp-usdoj.gov/bjs/pros.htm>. Even when deducting the inclusion of “support staff” numbers, the local and state prosecutors’ number is much higher than the federal statistic, especially considering the local/state statistic was obtained a year earlier than the federal number and does not factor annual personnel employment increases into the comparison.

⁴ This statistic was derived from compiling information from <http://www.usdoj.gov/usao/eousa/> and http://trac.syr.edu/tracreports/pros/ausa_pctdecG.html.

⁵ Per phone interview with research staff at the National Center for State Courts, <http://www.ncsconline.org>.

⁶ According to <http://www.uscourts.gov/>.

⁷ According to <http://www.ojp-usdoj.gov/bjs/pub/pdf/csf95ex.pdf>.

⁸ According to <http://www.ojp-usdoj.gov/bjs/glance/tables/expgovtab.htm>.

individuals who may present a risk to aviation and national security; or do background checks of those transporting hazardous materials.

For information sharing purposes, the boundaries of the justice community must be redefined to take into account a host of new faces. The justice community now includes nongovernmental agencies performing public services—a practice that “has increased dramatically in the past decade as local, state, tribal, and federal agencies have searched for ways to cut costs while still meeting their mandated responsibility to provide various services. . . . The criminal justice system has been . . . affected by this trend, with a growing movement to privatize correctional facilities at all levels of government.”⁹

The events of September 11, 2001, resulted in the creation of the U.S. Department of Homeland Security (DHS) with its constituent agencies, such as the newly formed Bureau of Citizenship and Immigration Services (formerly Immigration and Naturalization Services), U.S. Border Patrol, and the U.S. Coast Guard. September 11 also elevated the importance of information sharing between and among public safety agencies such as fire, emergency medical services, and other first-responder organizations.

The list would not be complete without the recognition of the numerous entities outside of the justice and public safety communities—such as schools, child care services, transportation, and licensing agencies—that need critical justice-related information to perform daily business activities, such as hiring new personnel, approving gun purchases, or granting professional licenses.

Finally, the list of relevant constituencies also includes the public, who expect greater accountability and access to justice information that is considered sensitive or protected by privacy laws in some settings (e.g., state criminal history records in many state repositories and the FBI system), while viewed as public record in others (e.g., criminal history record information in the courts). Increasingly, the public also expects that this access be automated and online.

The diversity of justice information consumers carries an attendant consideration: different types of users have different requirements. A judge making a sentencing decision has more time for his/her task—and a less expedited need for response to inquiry—than an officer on the scene requiring instant access to succinct information.

The purposes also vary. For example, it is one thing if the primary objective is to validate the identity or status of an individual (e.g., a law enforcement officer communicating with the Department of Motor Vehicles to check on a driver’s license),

⁹ *The Emergence of the Problem*, Logan, 1990; Bowman, Simon, and Sidenstat, 1992; Shichor, 1995. <http://www.geocities.com/CapitolHill/Lobby/6465/emerg.html>.

but another when an exhaustive search for information is required (e.g., a probation officer conducting a presentence investigation of a convicted offender).

Different sources also mean differences in expectations about who can use what information. Privacy and data quality issues, which are demanding enough when dealing with a single information system, grow exponentially when dealing with different disciplines. It is one thing to share the records of a criminal sentencing hearing held in open court; it is quite another when dealing with health records or an ongoing criminal investigation. Incomplete or inaccurate data may be an annoyance if the task is to identify leads for subsequent investigations; they are a different issue entirely if they prohibit one from getting a job, traveling on an airplane, or lead to incarceration. Working documents in one setting can become dispositive evidence in another.

What this means is that the information system design cannot begin with a clear definition of the boundaries of the enterprise. Nor can we assume that all of those who participate share a common set of objectives or an understanding of the process. On the contrary, the information system design must assume diversity, even conflicts, in the operating procedures and objectives of the participating organizations.

The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, tribal, federal, and even international boundaries.

The context for information sharing in the justice community is not singular. The scale will depend upon the objectives and the geographical setting. It is one thing if the objective is to move cases quickly from investigation to arrest through adjudication in a rural county where all of the participants know each other and have ongoing contact on a personal level. It is quite another thing if the objective is to share information about warrants between law enforcement and the judiciary in a large state on a real-time basis. And it is different still if the context moves to a national level, and the objective is to share information among many local, state, tribal, and federal law enforcement and health agencies about a reported health epidemic.

The resources required to develop an infrastructure for justice information sharing will come from many independent sources, the largest body of which will be local. It is safe to assume the funds will be spent to meet the immediate needs of the entities within the funding source's jurisdiction and not as a result of priorities that are provided by a state or national plan. An approach to infrastructure design that cannot be adapted to the different scales without losing their internal integrity will quickly be marginalized. A successful approach must have the capacity to meet the needs of a prosecutor, sheriff, and judge addressing a jail-crowding problem or DHS reaching out to local and state law enforcement for intelligence information. There is not a

national entity – nor even a statewide entity – that has the resources or authority to impose a solution devoid of value to local participants.

Information sharing must occur among data sources that differ widely in software, hardware, structure, and design.

The history of efforts to develop integrated information systems among local criminal justice agencies around a single hardware and software platform is large and filled with many disappointments. When the focus shifts to the state and national level, the success rate becomes even smaller and is largely populated by single-purpose efforts. The explanation for this phenomenon is relatively simple: technology investment decisions are made by funding sources with their own tax base, budget cycle, and spending priorities. The result is that information system development among local, state, tribal, or federal justice community entities rarely occurs in concert.

The reality is that no infrastructure development strategy can assume that all participants will be at the same point in the technology cycle. To paraphrase: new technologies are important, but legacy systems will always be with us.

The independent nature of local and state justice systems—particularly issues of funding—has contributed to the development of many “silo” or “stovepipe” information systems at the local level. Variations in local priorities, budget cycles, and needs have led to wide disparities in systems and capabilities within and across jurisdictions and branches of government. In many cases, federal funding, exacerbates this problem. Since 1970, with the creation of the Law Enforcement Assistance Administration (LEAA), federal grants have been used to assist local, state, and tribal governments in improving justice information systems. Since that time, numerous programs have been authorized by Congress, and the original LEAA initiative has transitioned into various programs providing needed assistance to local, state, and tribal governments to develop systems necessary for the efficient and effective operation of law enforcement, public safety, and justice agencies.

Eliminating these silos may be a long-term objective, but in the meantime, they contain information that is needed by fellow members of the justice community. There are still numerous information systems with large databases written in Common Business-Oriented Language (COBOL) that are important sources of information for the justice community. An infrastructure strategy that assumes their elimination is no strategy at all.

Public sector technology investment must reflect and incorporate the lessons and developments of the private sector.

It often surprises the justice community to learn how much of the technology needed to share information is common to the private sector as well. When you think

about it, only parts of the data and the transaction definitions are unique to the justice world. The several other technical layers in a transaction that provides a service are driven by open standards defined by private industry and implemented in their tool sets and products. We will never have the market clout to change these underlying technology standards, so we must learn how to incorporate and leverage them.

The Global process and the projects sponsored by it must take these powerful trends in the private sector into account. We can have some influence on such decisions, even in the private sector, by more fully participating in the open standards bodies that decide what will be proposed to the market for implementation; continuing collaboration with industry partners such as the Integrated Justice Information Sharing (IJIS) Institute¹⁰ will be necessary to succeed. Often, such participation and collaboration will educate us on how to develop and/or reuse the standards without needing to invent something new and unique for our business problems. And, as Global puts together an agenda for progress, we can also learn what **not** to do from some of these initiatives that have failed. These discoveries and lessons learned from the private sector will save us money and speed the day when we can all share critical data in ways that increase public safety.

It is only in the area of governance that the justice community may have some rare needs and problems that require unique solutions.

The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is transformed.

The operational requirements of members of the justice community are in constant change. The events of September 11 have elevated intelligence information to a leading priority for law enforcement; the rise of domestic violence cases has expanded the judiciary's need to reach out to the family services community; the increased mobility of the population has complicated probation's efforts to monitor offenders; and the spread of AIDS has put a premium on health management by corrections administrators. An infrastructure design that cannot adapt to an evolving definition of the boundaries and critical components of the justice community will, before long, become irrelevant.

The technology itself will change as well. The history of technology is written in the names of companies (does anyone remember Osborne?), hardware (Virtual Address Extension [VAX], portable computers, desktops, and laptops), and software titles (COBOL, C Object-Oriented Programming Language [C++]) that have been popular and then receded or even disappeared from view. Our approach to

¹⁰ For more information on the IJIS Institute, go to www.ijis.org.

infrastructure must be strategic, based on a conceptual framework that makes the most of current technology, but is able to evolve with the field.

The Recommended Solution: Service-Oriented Architecture (SOA)

The list of six requirements paints a formidable landscape for an infrastructure that will support justice information sharing on a local, state, tribal, and national level. It is our contention that the technologies are now maturing for meeting the technical requirements and that a conceptual framework is available to exploit these technologies for the justice community. These technologies consist of the standards, specifications, and protocols that have been developed to support the Internet, specifically the Web. The conceptual framework that has emerged to apply these technologies to information sharing is Service-Oriented Architecture (SOA). It is not important for policymakers to understand the details of these technologies. It is important, however, that they understand the implications for their information technology investment decisions and the outcomes they should reasonably expect from adopting these recommendations.

What Is SOA?

SOA is an approach to the design and development of an information system. *The assumption is that a system should be designed and developed around the basic components of the operational procedures or, in the language of the software literature, the business practices of an agency. These components are then combined into a loosely related larger structure that, in turn, can be combined into an even larger entity.* It assumes, in other words, that the design of a system begins with a concept of the business practices of an enterprise (e.g., case-flow management, investigations, or trial preparation), which identifies the critical components (e.g., personal identification, sentencing document, or arrest report), which defines the parameters of stand-alone pieces of software (i.e., services). The effect is to permit the evolutionary development of a system. Software can be written to serve specific purposes (e.g., define the identity of an individual) and shared on an approved basis with other programs (e.g., borrow the identity definition software of the postal service in a judicial case management system). Lessons learned from development of the components can be used to revise the business practices that, in turn, can guide the development of additional components. It then follows that a system can begin small—organized around specific operations—and evolve into a larger, more comprehensive system as the parts are linked together. *This approach to design, development, and implementation is possible because of the technology developed for the Web.*

We have all become familiar with the ability of the Internet-based technologies to support exchanges of messages and searches for information across a seemingly

infinite number of participants. The focus is upon the message and its utility to the user rather than on the underlying data source. The technology allows a search across a crazy quilt of hardware and software systems for information that is relevant to the user. SOA exploits those attributes in architectural design, whether the problem involves a single, small agency working on a dedicated network or a far-flung operation involving numerous agencies, databases, and operational requirements.¹¹

Before going further, the significance of SOA is easier to understand if it is contrasted with traditional architectural designs—monolithic, centralized systems based on one big server and departmental systems based on a closed local area network with attached homogeneous systems.

The monolithic framework required every participant to be part of a single comprehensive information system, symbolized by the “dumb” terminal used to access it. All of the applications and data were housed in a single centralized place in order to maximize uniformity and control. The monolithic system could not be designed or changed in any way without taking into account all of the functions it performed. That made it so difficult and expensive to meet evolving business needs that many users just gave up.

The departmental systems relieved some of that rigidity and unresponsiveness to business needs. Users with access to personal computers (PCs) and small servers were free to develop their own independent applications and data stores. Sharing of information was still constrained by the type of local area network and agreement on the use of common applications. Exchanges between applications still required custom development in each case. The problem of overall coordination remained, but it was reproduced on the level of the department. Meanwhile, coordination among departments declined, and many organizations lost overall control of their information as costs rose.

Neither the monolithic nor the departmental computing architectures did much to further the difficult business of sharing justice information among disciplines. The costs were too high unless a small and well-defined business requirement was shared, using a strong, centralized governance structure such as the FBI CJIS Advisory Policy Board that coordinates the National Crime Information Center (NCIC), Integrated Automated Fingerprint Identification System (IAFIS), etc. The first breakthrough in the resolution of this problem was the rise of inexpensive wide area networks and the standardization of local area networks. These developments suddenly allowed different agencies to economically share compatible information across compatible architectures. For the first time, experts began to talk about the network as being more important than the server or the application.

¹¹ SOA and “Web services” are often used interchangeably, but strictly speaking, Web services is just one—if the most viable—way to realize the benefits of SOA.

The second breakthrough was the advent of open standards for sharing information across networks without regard for the underlying technologies or applications. This is what an SOA enables. At one stroke, the need for centralized coordination of technology or application disappeared, and economic means of communicating became possible because many vendors support the open standards around which SOA is built. We are free to specify business goals for sharing data while leaving it to individual agencies to incrementally support and implement the underlying mechanisms. A sheriff's office may use a mainframe with an application written in the 1970s, and a police department may use a PC server with an application written last week, but they can share criminal history data as long as they agree on a set of open standards for exchanging the information.

SOA exploits Web open standards and technology to free the developer and the business from the traditional constraints of the monolithic and departmental models. Conceptually, an SOA is a distributed software model in which small pieces of application are published, consumed, and combined with other applications over a network. The developer begins with software that defines the basic building blocks (or "services") of our business processes—e.g., the investigation, rap sheet, warrant, indictment, or presentence report. These software components are then made available (published) to other developers either within the agency or to a larger audience.

Conceptually, an SOA is a distributed software model in which small pieces of application are published, consumed, and combined with other applications over a network.

SOA and Justice System Requirements

If we return to the six criteria for an infrastructure that will support information sharing among the justice community, the advantages of SOA become obvious.

The architecture must recognize innumerable independent agencies and funding bodies from local, state, tribal, and federal governments. The independence and number of entities that need to share justice information is almost overwhelming. Certainly, it is beyond the ability of existing conceptual frameworks, computer models, or financial resources to create a comprehensive network using traditional technology. SOA, however, is ideally suited to the task. A quote from SOA literature makes this fit clear: "Designing for SOA involves thinking of the parts of a given system as a set of relatively autonomous services, each of which is (potentially) independently managed and implemented, which are linked together with a set of agreements and protocols into a federated structure."¹² "Autonomous," "independent," "agreements," and "federated" capture the environment for justice information sharing.

¹² *Demystifying Service-Oriented Architecture*, Daniel Sholler, META Practice, June 9, 2004.

Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions. The decentralized, loosely coupled characteristics of an SOA approach means that law enforcement, prosecutors, defense counsel, courts, corrections, probation, and parole can share information without sharing a common set of objectives or funding sources. The only agreement has to be a mutual understanding of what information will be shared with whom. The focus is on the messages, not on the structure of the database, the application, or the network. This decentralization allows for sharing of information outside of the immediate justice community and expands it to Global's vision, including corollary organizations and the public.

It also allows for local control over who may access data and for what purposes. SOA does not require an agency to send its records to a central warehouse over which they have no control. It is ironic that SOA both simplifies the issues of privacy and data quality by allowing greater control by individual agencies over how and under what circumstances their information will be used and complicates the search for solutions because of the greater variety of circumstances that have to be addressed.

The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, federal, and even international boundaries. SOA begins with the business processes of a justice agency, regardless of size, which are then linked together through agreements and protocols. Sharing services will reduce the development costs for small agencies without sacrificing the ability to access information from the extended system.

Information sharing must occur among data sources that differ widely in software, hardware, structure, and design. SOA makes no assumptions about hardware or software within participating agencies. By using Internet-based technologies, the focus can be on the interrelationships of systems and services, not internal platforms.

Public sector technology investment must reflect and incorporate the lessons and developments of the private sector. SOA is rapidly being adopted as the architecture of choice for the private sector. As one observer has noted: "By 2005, a new set of meta-architectural principles, currently referred to as 'service-oriented architecture,' will be broadly diffused throughout the IT environment in the form of service-oriented business architecture, service-oriented security architecture, service-oriented management architecture, etc."¹³

The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is

¹³ Ibid.

transformed. SOA assumes a system will evolve through the development and sharing of individual components rather than through the implementation of a single comprehensive design. As the priorities and requirements of the justice system change, the information system can evolve and adapt without having to reinvent itself. Indeed, the SOA approach is elegant ***precisely*** because it is logical and evolutionary, **not** radically divergent. SOA simply reflects and responds to what exists today.

The SOA Agenda for the Justice Community

The advantages of SOA over alternative approaches are so obvious that they sound too good to be true. And, in fact, there is a catch. It is true that SOA is rapidly being adopted by industry as the architecture of choice in system development. It is also true that many justice agencies are beginning to experiment with SOA to address information sharing issues.¹⁴ At the same time, *it is important to realize that SOA is a work in progress in both the private and public sectors.* Whether the promise of SOA is fully realized for justice purposes will depend upon the justice community taking an active part in the evolving world of technology.

The issues that need to be addressed can be grouped into six categories: services, standards, interagency agreements, registries, security, and privacy and data quality.

Services

The drivers behind information sharing are the justice community members' business processes. The SOA approach assumes that the members of the justice enterprise share some common business processes, which can be shared when common definitions for producing and consuming information are created using open Web standards. Defining these common business practices is a key step in gaining value from an SOA. If we implement unique definitions of business practices at each agency, an SOA will just create a "Tower of Babel" by exposing many inconsistent and incompatible services to each other. Fortunately, law enforcement, court, corrections, and probation associations have already taken steps in the direction of defining common business processes within their associations. We can build on this work.

The justice community is just beginning to develop these common definitions. Software components that expose the capability to produce information on demand are called "services." To effectively share services across all levels of government and across the various justice communities, we must create common definitions for those business practices, the data that is being shared, and the transactions that implement the exchanges. In particular, the transactions that ultimately constitute successful

¹⁴ Two examples are the Wisconsin Criminal Justice Information Systems and the Washington state courts.

sharing must talk the same “language” across multiple layers of technology, even if the technology is based on the same open standards. The Joint Task Force on Rap Sheet Standardization’s rap sheet is an early example of an effort to completely define an open Web transaction based on SOA standards.

In part, we are talking about how we divide up the business “pie” into services of consistent size and definition. When we talk about a criminal history, a driver’s history, an arrest warrant, or a felony disposition, we should be talking about services with equivalent kinds of information. This step in the service definition process relies on a community effort to characterize “reference documents” for typical justice data exchanges. Reference documents may form the business basis for defining common transactions that share common services.

Reference documents describe parts of business processes that justice practitioners must agree upon. Much of the actual information (person identification, addresses, and payment information) has already been standardized by private industry using open Web standards. It would be foolish of us to separately define incompatible services without looking to the work that is already completed. The value is to add to that body of work’s shared definitions for sets of information unique to the justice community.

Standards

SOA assumes the existence of accepted and open technical standards that define how different systems will interact and that are independent of any vendor. Both the Web and an SOA for sharing information are possible because major technology vendors reached consensus on technical standards to broaden their markets. Similarly, the justice community can broaden its information sharing market by agreeing on the definition or reuse of common technical standards upon which to base their services.

We often think of justice data as having uniquely difficult requirements for sharing, but private industry trusts billions of dollars in value to their exchanges: they are driving key work on open standards to ensure secure and reliable exchanges of data. It is unlikely that the justice community can successfully convince vendors to implement a new and different set of technical solutions to these important business requirements. Translating the business requirements into justice-relevant terms, however, is within our province. This means the justice community must be prepared to take an active part in defining our business issues and the policy constraints that the technical solutions must address by participating in whatever public or private forums are available (such as the World Wide Web Consortium [W3C]¹⁵) where such standards are being developed.

¹⁵ For more information about the W3C, go to www.w3c.org.

While the Global Justice Extensible Markup Language (XML) Data Model¹⁶ (Global JXDM)—national justice data model—and the Global Justice XML Data Dictionary (Global JXDD)—national justice data dictionary—represent fundamental first steps toward a complete set of technical standards for transactions implementing common services, there are several layers of additional standards necessary to ensure successful interoperability. To deliver on the promise of business value, progress to these next steps should be made without delay.¹⁷

Consortiums such as the Web Services Interoperability Organization¹⁸ (WS-I) are providing valuable services that can be leveraged by the justice community. WS-I develops profiles of standards that are shown to be interoperable and effective for industry. It is likely that these same profiles can be adopted and customized for the justice community.

Interagency Agreements

The third category of issues concerns how agencies reach consensus on their interactions with each other, usually represented by interagency agreements. If an agency is to share services and information, it must establish the conditions for gaining access to registries and databases maintained by others and, conversely, how others will have access to their registries and databases. It is similar to the procedures agencies currently use when engaging an outside contractor. The contract model is appropriate when there is a one-on-one relationship, for example, a prosecutor's office reaching agreement with the local court on the rules for electronic filing of cases. The problem becomes more complex as you add participants, for example, participation in NLETS or the FBI's Law Enforcement Online (LEO). And it reaches epic proportions as agencies move across disciplinary boundaries and participation is among the many.

Registries

At the heart of SOA is the assumption that software components (services) will be shared. This requires not only standard definitions but also a means for locating and accessing the relevant components. The solution to these issues has focused on the concept of a system of federated registries and repositories. These are sites where either the reusable software could be located or the instructions for accessing the software can be found.

¹⁶ For more information about the Global JXDM, go to www.it.ojp.gov.

¹⁷ Mention should be made of two additional efforts to address these issues: the National Association of State Chief Information Officers' Enterprise Architecture Maturity Model (<https://www.nascio.org/publications/index.cfm>) and SEARCH's Justice Information Exchange Model (<http://www.search.org/programs/technology/jiem.asp>).

¹⁸ For more information on WS-I, go to www.ws-i.org.

The numerous complex issues surrounding the creation and operation of public registries will have to be addressed for the justice community. These issues are still open questions for the private sector.

Security

Concerns about trust, confidentiality, security, privacy, accuracy, and reliability have always been major information sharing issues among justice agencies. Our solutions in the past have tended to depend on limiting the number of participants and dealing only with people we know. Previous Global recommendations, homeland security, public safety requirements, and SOA challenge those assumptions. New solutions must be found as the number of participants increases and the probability of dealing with strangers is high.

Privacy and Data Quality

Issues of privacy and data quality are integral to any information system, whatever the technology. Paper-based systems are as dependent upon accurate records for their effectiveness as those that use electronic signals. By the same token, an individual's right to privacy is no less violated if privileged information is accessed by opening a cardboard file than it is if read on a computer screen. It would be naïve, however, to pretend that a system which shares digital information does not increase the threat to the right to privacy of individuals or heighten the risk of decisions that threaten the safety of individuals because of bad information. It will be essential that the implications of SOA for privacy and data quality be addressed. In the final analysis, it is not the technical issues that are the most difficult to resolve. It is these basic policy concerns that, if unresolved, pose the greatest threat to realizing the Global vision.

The Next Steps

Three conclusions should be clear from the previous discussion: (1) SOA should be embraced by the justice community as the most appropriate framework for the design principles for information sharing; (2) SOA is a reality, but the promise is much greater than what is available now; and (3) if that promise is to be realized, the justice community must take an active part in the evolving process of defining the content and technology on which SOA depends.

The Action Agenda: Local, State, and Tribal Agencies

SOA has emerged as a broad conceptual framework to capture and rationalize the small, incremental steps taken by practitioners addressing real-world problems. This close interaction between broad theory and narrow experimentation is a major reason SOA holds such promise. The promise, however, will only be realized if this

pattern continues in the justice community. *This means a two-part agenda for the local, state, tribal, and federal operating agencies: (1) they need to initiate projects and demonstrations that address real-world issues, and (2) they must be willing to share their results with the larger community.*

For most local, state, and tribal justice agencies, the first task will be to develop an understanding of SOA and the technology on which it rests and to begin experimenting with its application. The very attributes of SOA make this a much less formidable task than with other technical innovations. Because of its orientation around business practices, the first experiments can be conducted on a relatively small scale where the price of failure is relatively low. SOA lends itself to incremental development, even of large-scale applications. The result is a shift in the cost model of strategic information technology development from front-loaded expenditures and “cliff-based” deployments to one of manageable, incremental investment. This shift reduces risk and frees up resources for other strategic investments.

A business consulting and advisory services firm¹⁹ recently completed a study of early adopters of Web services and SOAs. They found that a major imperative was to reduce technical complexity and to increase business flexibility, which was realized by the move to SOA. The experience of early adopters resulted in reduced maintenance, leveraging of existing investments, improving operational visibility, and creating new business value.²⁰

The second part of the practitioners’ agenda is as important as the first: they must be willing to share the results of their experiences with others—failures as well as successes. This is no small task as it means moving out of the comfort level of a known world into a world of strangers. Without that shared experience, however, SOA solutions will be based on abstractions and broad theories rather than on the bumps and bruises that come from wrestling with real-world problems.

The Action Agenda: Federal Agencies

SOA will also require significant changes in the role many federal agencies play in justice information sharing. Traditional approaches to developing the required infrastructure will need to be adjusted and new strategies developed that recognize and take advantage of the resources and experimentation going on at the local, state, and tribal levels.

First, federal agencies, like their local, state, and tribal counterparts, should embrace SOA as the approach of choice in the development and implementation of

¹⁹ The Stencil Group <http://www.stencilgroup.com>.

²⁰ Mirroring Global Intelligence Working Group’s shift in focus in defining “infrastructure,” as previously outlined in this report.

their information systems. This move is already taking place in several agencies, and we applaud their effort.

Second, federal agencies should form active partnerships with standard-setting bodies in the public and private sectors. The need for technical standards and proven, effective techniques is too great for any one source to capture the universe. This is especially true for the justice community, since there is no single entity that can claim credibility among the many disciplines represented. Unilateral efforts by federal operating agencies to set standards are likely to result in anachronisms as technology investments at the local level and developments in the private sector overtake and surpass the requirements embedded in a typical three-year procurement process.

Third, it will be important for federal grant-making agencies to encourage SOA experimentation at the local, state, and tribal levels. Although SOA reduces the cost of experimentation, there are still risks for operating agencies. We need to encourage local, state, and tribal jurisdictions to test new practices and procedures built around SOA. For many agencies, federal funding reduces the risk involved in that testing process.

Fourth, federal funding will be critical to Global's role in extending SOA into the justice community. In the following paragraphs, we lay out an ambitious agenda for Global in furthering the evolution of an architecture that will support justice information sharing. That role will require resources to ensure the kind of broad participation required from local, state, tribal, and federal agencies and branches of government.

The Action Agenda: Global

If SOA is to be used successfully as the framework for justice information sharing architecture, Global must play a proactive leadership role in several areas.

First, Global has formally, actively embraced SOA as the recommended framework for a national infrastructure to support justice information sharing and will integrate its requirements into all of its activities. This means incorporating SOA into the activities of all of the Working Groups. SOA raises issues for security, privacy and information quality, and intelligence that will be given explicit attention and treated as part of a broad initiative.

Second, Global will take steps to encourage the creation of a mechanism for drawing together the experiences and lessons from the field. SOA reinforces the basic strategic approach Global takes toward standards development; i.e., it assumes a bottom-up approach to national information system development rather than top-down. It embraces the fact that the largest funding source comes from local and state governments and works to exploit the variety of resulting approaches and solutions rather than try to force all solutions into a single mold. At the same time, a simple list

of experiences will only marginally advance the objective of a national infrastructure. What is needed is a process for synthesizing the disparate conclusions into a systematic set of recommendations that are creditable in the justice community as a whole. The XML Standards Task Force (XSTF) has been extraordinarily effective in developing standards for data definitions using XML and holds promise as one approach for such a process.

Third, Global will reach out to existing national systems to incorporate their efforts into the design of an overall strategy. The pipes for moving this information across the country already exist in NLETS, the American Association of Motor Vehicle Administrators network (AAMVAnet), Regional Information Sharing Systems® (RISS), etc. The objective of the national strategy is to use these pipes and existing networks to their best advantage, not to supplant them.

Fourth, the six issues identified in this report—services, standards, interagency agreements, registries, security, and privacy and data quality—will be a major part of the agenda for the next set of activities of Global. Four of the six issues are new to the Global agenda but are integral to extending SOA into the justice community. They will be addressed by the Global Infrastructure/Standards Working Group. Security is already being addressed by the Global Security Working Group; its agenda will now include a reexamination of the issues within the context of SOA. The Privacy and Information Quality Working Group will also move quickly to address the implications of SOA for its agenda, as these critical policy issues must be addressed early in the process for success.

Fifth, Global will develop a multitiered strategy for the public sector to influence standards. It will include encouraging the creation of a public process (as it did with XML); taking part in industry groups developing standards that are relevant to justice (e.g., World Wide Web Consortium [W3C]); and developing partnership processes with industry and other public entities. No single strategy will be sufficient, nor will it be possible for the public sector to control all of the standards development processes.

Conclusion

This report lays out an aggressive role for Global and for the justice community. It argues that the members of Global, acting both collectively and individually, should exploit the unique composition of its membership to ensure that a justice perspective is part of the evolving practice of SOA. The majority of financial drivers behind justice information systems' development are at the local and state level. SOA's focus on the development of discrete components that are in turn published and shared with the larger community turns this decentralized environment into a strength instead of a weakness. However, it is only a strength if there is a sense of the whole, that is, a sense of where the components fit into the justice enterprise

and a consensus on which components are to be treated as local experiments and which ones as standards. SOA assumes a dynamic relationship between a bottom-up process that is driving applications and a top-down process that is driving standards and best practices.

Global is uniquely situated to provide the leadership required. There is no other entity at the national level that can command agreement by local and state governments, agencies, or branches of government. There are national entities that are in a position to structure the debate within specific subject areas, but no other body exists for the justice community. National standards and practices that are to serve the justice community require a group that holds enough stature in all of the several disciplines to give immediate credence to its products. Global brings that credibility to the process.