



IBM Center for
The Business of Government

Collaborating Across
Boundaries Series

Designing Collaborative Networks

Lessons Learned from Public Safety



Jane Fedorowicz
Bentley University

Steve Sawyer
Syracuse University

Designing Collaborative Networks: Lessons Learned from Public Safety

Jane Fedorowicz

Departments of Accountancy and Information and Process Management
Bentley University

Steve Sawyer

School of Information Studies
Syracuse University



Table of Contents

Foreword	4
Executive Summary	6
Introduction	8
The Challenge of Improving Interagency Collaboration	11
Research Observations About Public Safety Networks	14
Factors Influencing the Design of Public Safety Networks	14
Findings about Implementing Public Safety Networks	15
Recommendations for Implementing Collaborative Networks	20
Appendix: Examples of Collaboration from Other Policy Arenas	23
References	26
Acknowledgements	31
About the Authors	32
Key Contact Information	34

Foreword

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, *Designing Collaborative Networks: Lessons Learned from Public Safety*, by Jane Fedorowicz, Bentley University, and Steve Sawyer, Syracuse University.

This report offers practical advice to public managers and political leaders who are addressing complex public challenges through multi-organizational networks. The use of collaborative networks of organizations has matured in the past decade. However, the developers of collaborative networks face political, organizational, and technological challenges in a world accustomed to the traditional, hierarchical approach to problem-solving and accountability.

Professors Fedorowicz and Sawyer draw on a six-year project which collected data on 266 collaborative networks of public safety organizations, such as law enforcement and first responders to emergencies. They found a great deal of diversity in these public safety networks. They also found, however, common patterns of issues. For example, most of the design issues surrounding public safety networks center on data security and access concerns of the various participants. The authors also found common principles for designing successful collaborative networks, and they believe that these design principles can be applied in policy arenas other than public safety.

One principle they present is the importance of leveraging the use of technology as a way to advance the work of a collaborative network. For example, to address the issue of data security and access, they recommend that those involved in designing a collaborative network “ensure that data custodianship remains with the data’s owners ... the collaboration should be seen as providing a portal to data, not a warehouse for its storage.”

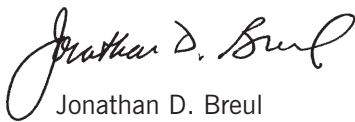


Jonathan D. Breul

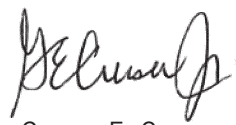


George E. Cruser

Much of their advice and recommendations come from the experience of people on the ground who have faced and solved knotty problems. As a result, we hope this report serves as a useful guide to federal managers as they develop collaborative networks to address challenges that reach across federal agency—and sometimes state, local, non-profit, and private sector—boundaries.



Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
jonathan.d.breul@us.ibm.com



George E. Cruser
Vice President, U.S. Federal Team
IBM Global Business Services
george.e.cruser@us.ibm.com

Executive Summary

Government agencies face increasing internal and external pressure to share information and to communicate across agency boundaries. Multiple-organization collaborative initiatives are far more complex and difficult than technology-based projects developed for use by a single agency. Collaboration requires a shared technology infrastructure that knits together legacy information systems of each partnering organization. Even more challenging is the need to design new approaches to organizing, funding, governing, sharing data, security, and operations.

For those involved in cross-boundary and cross-agency collaborations, this report recommends ways for designers, implementers, managers, and users to get the most from these efforts. The underlying goal is to answer the question: How does an agency effectively contribute to a partnership in the face of existing technological, organizational, or political boundaries?

The basis for the findings and recommendations presented here is the Public Safety Networks Study (<http://www.publicsafetynetworksstudy.org>), a multi-year, multi-university research collaboration. Public safety networks link police and other responder agencies that access shared data and a common communications infrastructure across functional or geographic borders, and may link agencies from multiple levels of government. Public safety networks provide value beyond the specifics of their domain, as they exhibit many characteristics common to cross-agency collaborations in other domains and focused on other needs. That is, public safety networks, like most cross-agency collaborations, need to set up a new kind of cooperative governing structure and obtain capital funding outside of normal channels. Like participants in all collaborations, public safety networks must worry about how to obtain, verify, share, and protect data that come from a variety of sources out of their control. And they need to do all this outside their normal operating structure and procedures while still addressing participating member agencies' goals and the broader goals of society.

Based on the study findings described in this report, five implementation recommendations are presented. These recommendations represent distilled insight framed as prescriptive guidance for policy-makers, collaboration leaders, systems developers, and participating agencies as they work collectively toward cross-boundary information-sharing.

- **Recommendation One:** Involve all stakeholders in the design of a collaborative network.
- **Recommendation Two:** Create networks that stakeholders will value, participate in, and use.
- **Recommendation Three:** Pursue every opportunity to fund a collaborative network.
- **Recommendation Four:** Develop a diverse set of performance goals.
- **Recommendation Five:** Leverage technology to advance a collaborative network. There are six actions required to implement this recommendation:
 - Design the collaboration's information technology elements to be flexible and modular.
 - Ensure that data custodianship remains with the data's owners.

- Ensure standard security and access approaches are used to frame both technology design decisions and related governance processes.
- Plan to build on and incorporate legacy technologies.
- Design collaboration and information-sharing processes and technologies to support routine use, as this will help increase system usage.
- Emphasize system reliability and stability when designing technology, so that usage will increase.

Introduction

Working across agency boundaries to share information is both critical to improving government services and—for a number of good reasons—impressively difficult. This report identifies guidance to assist both decision-makers and information system developers who are making the kinds of organizational and technological choices that will advance cross-agency, cross-boundary, and government-spanning information-sharing.

The specific focus of this report is to draw insights from a comparative analysis of collaborative networks used to share information for public safety—generically labeled here as public safety networks (PSNs)—and leverage the findings of this study to develop a more general set of recommendations for sustaining collaborative networks. Patterns of organizational behavior and commonly noted observations on information-sharing systems in public safety are shared here as implementation guidance for decision-makers and systems builders who pursue cross-agency, cross-level public sector collaborations. That is, the specific insights on successful cross-boundary information-sharing and collaboration in the public-safety context should be useful as general guidance well beyond the specific focus of the study.

What is a Public Safety Network?

A public safety network is an initiative connecting policing with other public safety, emergency management, homeland security, or criminal justice agencies. A PSN is both a technological effort (often a complex combination of information and communication technologies, databases, security protocols, and information-sharing portals and algorithms) and an interorganizational collaboration attentive to the needs of technology design, funding, security, and information-sharing policies and procedures.

From a technological perspective, a PSN links police and other first-responder agencies seeking to access shared data and draw on a common communications infrastructure across functional or geographic borders. A PSN most often links agencies from multiple government levels. A PSN may also involve non-governmental or private-sector partners such as hospitals or utilities. Because they coordinate in ways that supersede normal operating and reporting procedures, new organizing and governance structures often evolve as part of the PSN design processes and operations. Because PSNs incorporate a technological infrastructure to link together existing data stores, communications devices, and new technologies, they also provide the shared space needed to link the range of participants they anticipate supporting.

Wide variation within these definitional boundaries is possible, so that any one PSN can take on a very different look and feel in practice. Public safety networks vary in terms of their reporting structures, funding structures, the services they provide, their technological arrangements and elements (often called technology architecture), and their membership. What PSNs share, however, is at the core of organization-spanning collaborative networks. All PSNs:

- Involve multiple agencies
- Combine services to span existing agency boundaries
- Access multiple sources of information from host agencies
- Share governance of the technology architecture
- Set policies for membership and use

There are many initiatives throughout the United States that could carry a PSN designation. The box on page 10 provides examples of several current PSNs that participated in the larger study of PSNs forming the basis of the analysis presented in this report. The larger study is described in the *Public Safety Networks Study Project* box below.

The Public Safety Networks Study Project

Data Collection Method and Analysis

The implementation guidance reported here is drawn from a multi-year study of public safety networks within the United States. The Public Safety Networks Study project is itself a collaboration across multiple universities¹ which has been funded in part by the National Science Foundation,² Bentley University,³ and the IBM Center for The Business of Government.⁴

This report is the product of six years of data collection and analysis. Much of the understanding of the intricacies of cross-agency interaction results from conducting detailed case studies of several PSNs. Each case study is based on extensive interviews with representative sponsors, designers, management, and users of a PSN, conducted over multiple visits, conference calls, and e-mail. Important documents such as system documentation, meeting minutes, legal documents, and procedure manuals also were combed for relevant information.

In addition to the case studies, the project team assembled a data set describing 266 PSNs at the state and local levels to garner an understanding of the number and distribution of existing collaborations. Another data set containing secondary data at both state and local levels (such as census data, political science research findings, and published grades or rankings) permitted the comparison of PSN existence and location based on approximately 230 state and county demographic factors.

A third data collection effort resulted in observations about some of the most telling patterns that differentiate among PSNs. The project team conducted an extensive telephone survey in which senior personnel from 80 PSNs were interviewed for approximately 45 minutes each in response to over 90 questions about the PSN's origin, purpose, membership, usage, development, technology, governance, performance measures, and goals. This analysis identified many patterns (and some surprising lack of patterns) among the 80 that formed the basis for the design observations and principles presented in this report.

1. The principal investigators for the research were employed by Syracuse University, Bentley University, and Penn State University.
 2. This work is supported by National Science Foundation grants NSF-0852688 and NSF-0534877. Further details are found at www.publicsafetynetworksstudy.org.
 3. See www.bentleyinvision.org.
 4. Fedorowicz, Jane, Janis L. Gogan and Christine B. Williams, *The E-Government Collaboration Challenge: Lessons from Five Case Studies*, IBM Center for The Business of Government, Washington, D.C., 2006.

Examples of Public Safety Networks

The Public Safety Networks Study has conducted several detailed case studies of existing PSNs. The case studies include the following organizations:

- One of the oldest is the **Automated Regional Justice Information System (ARJIS)**. ARJIS began in the late 1970s to serve San Diego County in California. Over time, it has expanded its coverage area to include several neighboring counties. ARJIS focuses on supporting routine emergencies, policing, and crime analysis. Its website is <http://www.arjis.org/>.
- **Clermont County, Ohio**, supports routine emergencies, policing, computer-aided dispatch, and incident management through the Division of Public Safety Services (DPSS). This PSN began in 1987, and has expanded its service area to include some neighboring counties. Its website is <http://comm.clermontcountyohio.gov/>.
- **The Commonwealth of Pennsylvania** started working on the Pennsylvania Justice Network (JNET) in 1997. The system provides support to law enforcement, courts, and probation throughout the state. Its website is <http://www.pajnet.state.pa.us/>.
- **The Capital Area Wireless Information Net (CapWIN)** is a collaboration covering the states of Maryland and Virginia and the District of Columbia. Members come from federal, state, county, and local levels, in support of routine emergencies, policing, computer-aided dispatch, and incident management. This PSN began to offer services in 2003. Its website is www.capwin.org. (It is described in more detail in the box on page 16).
- **Winnebago County, in Illinois**, began development of the Winnebago Integrated Court and Case Management System in 2004. Its users come from law enforcement, the courts, corrections, and probation areas. The system went live in 2010. The website is <http://fce.wincoil.us/fullcourtweb/start.do>.
- **The National Law Enforcement Telecommunications System (NLETS)** is a national PSN whose members are the 50 states. From its headquarters in Arizona, it provides centralized crime and incident data reporting to other PSNs and law enforcement agencies. It began as a teletype service in 1966. NLETS's website is <http://www.nlets.org>.

While the PSNs studied for this report all support police activities of some kind, the findings generalize well to other types of public-sector collaborations. Recognizing that cross-agency collaborations have different mandates, challenges, and goals, there are also many commonalities among collaborative networks that—were it possible to more clearly identify and understand them—could serve as the basis for providing guidance to others seeking to establish or extend cross-boundary, information-sharing initiatives. For example, the PSNs examined for this report cross functional, geographic, and government-level boundaries. These PSNs obtained initial capital funding and continually worried about maintaining operational funding. They needed to set up a governance structure and procedures for multiple agencies whose structures are different from the typical member agencies' structures (or participants' experiences). The PSNs examined for this report all worried about how to obtain, verify, share, and control data. These characteristics are common to other governmental organizations facing the need to share data and communicate outside normal reporting lines.

The Challenge of Improving Interagency Collaboration

How does an agency effectively contribute to a partnership in the face of technological, organizational, and political boundaries? Improving interagency collaboration and information-sharing is critical to advancing the work of most government agencies (if not most contemporary organizations). Federal, state, and local agencies collect huge volumes of data and information, much of which would benefit many other agencies if only they were able to share it effectively. President Obama and many state governments have called for organizations to become more collaborative in order to enhance information-sharing and improve communication.

Specific examples of this broad-scale need illustrate the challenge of successfully implementing a large-scale collaborative data exchange. For example, there is a long and expanding design schedule allowed for the evolving Nationwide Health Information Network. In another example, large expenditures of federal funds to implement broadband communication networks permit local emergency response agencies in many parts of the country to replace their array of old radio systems that previously could not talk to one another. The goal for the new radio systems is for public safety personnel to be able to work side by side with those from outside their home agency.

Cooperative efforts to encourage information-sharing and communication among agencies can greatly improve government's ability to operate and better achieve collective goals of serving and supporting the public. These increased benefits also bring about increased challenges and new risks. We already know that large-scale technology infrastructures are not easy to implement when they are designed to support a single agency—just ask the Internal Revenue Service or the Department of Defense. Collaborative initiatives break new ground in many ways, starting with the challenges of designing, implementing, and operating cross-boundary entities that do not reside in a single agency. Beyond the typical technological design issues to be resolved, decisions need to be made and support found for funding, governing, operating, and using the shared mechanisms that form the basis of the collaborative network. Moreover, success in cross-boundary collaborative networks is multifaceted: reliability, efficiency, effectiveness, responsiveness, participation, and other measures, all matter—even if these may sometimes be at odds with one another (as it is hard to be frugal while delivering services to all who seek them).

PSNs are not the only government arena in which cross-boundary collaboration is needed. The Appendix presents examples of collaboration in other policy arenas. The examples summarized in the Appendix all involve the challenges of crossing boundaries, finding the flexibility needed to meet varying and changing goals, and working within the restrictions of existing organizational and technological infrastructures.

The broad-scale need for greater guidance to support cross-boundary information-sharing is tempered by the need to ensure that guidance is grounded in the specific needs of the situation. While there may be some set of common-to-all-situations guidance regarding how to best design and implement cross-boundary information-sharing systems, these will need to be framed by the

particulars of an initiative. Still, there are clear similarities (such as the need for flexibility and a call for meeting the needs of a broad base of users) in the kinds of advice presented in this report. To that end, this report provides a set of implementation recommendations that will aid designers, implementers, managers, and users of PSNs in linking technological and organizational implementation decisions that lead to more successful initiatives. For example, successful public-safety collaborations depend upon:

- **Increasing public safety, homeland security, and operational effectiveness** (e.g., reducing the number of air accidents, improving homeland security responsiveness, or moving more quickly from arrest to conviction)
- **Meeting financial commitments** (e.g., lowering the cost of an arrest or reducing the resources needed to complete an investigation)
- **Upgrading technological features** (e.g., ease of system use, compatibility with current technologies, or operational reliability)
- **Improving access to public safety data** (e.g., by making it faster and easier to get to data sources, creating new data sources, or making existing sources available to more authorized people)
- **Supporting public-sector employees who work across geographic or functional lines** (e.g., by providing shared services or leveraging common technological platforms)

When these competing perspectives are considered, it becomes clear that building a technological infrastructure for cross-agency collaboration in public safety is only one of many interconnected challenges. Principles of collaborative design need to allow for close and careful alignment with the political environment, the goals and capabilities of participating organizations, and the objectives of the collaboration. The design and operation of a PSN, or any cross-boundary information-sharing system, will be many-faceted and encompass technological design in addition to organizational operations and their governance.

As with any new initiative, the development and implementation of a PSN unfolds within some structure charged with decision-making and allocation of resources. For PSNs—and, more broadly, any public-sector cross-boundary collaboration—there needs to be a *host organization*, one assembled to oversee the technological infrastructure. In developing this host organization, there has to be some means of allowing for shared governance so that the various institutions involved have their say and represent their needs. This shared governance must extend to the data and technology infrastructure accessed by its participants and users. To add to the challenge of governance, each goal, performance objective, or operational constraint emanating from the initiative or one of its contributing partners will have corresponding organizational and technological implications. So, even when a concern is predominantly related to politics or operations, there is likely also an impact on how the technology will be implemented or used.

Technological choices (decisions about the technology architecture) may similarly encourage or limit usage. Also, technological decisions will have both political and operational implications. For example, an in-car computer may be welcomed by a police officer. But it may be seen as a nuisance to firefighters as their cabs are already chock-full of other instrumentation. Likewise, a government mandate may stipulate that open-source software will result from any new initiative, yet the vendor may refuse to give up the intellectual property rights without a large payment. Federal funding may restrict the ability of an organization to charge for a system's use, but without charging, the organization cannot afford to exist. A system may integrate many sources of complementary data, but some data owners (the data's custodians) may restrict access to their own government level, or insist on controlling security and access by others to their database. Another agency may demand payment for its data, even though supplying it

would achieve a public good. Simply put, technological, organizational, and political design issues are tightly intertwined.

These and other examples of a decision or constraint on one piece of a collaborative network having repercussions for others demonstrate why careful documentation of patterns of practice is invaluable to others facing equally complex design pressures. Collectively, these examples form the basis of a set of observations that lead to prescriptive design guidance for those in similar situations.

Research Observations About Public Safety Networks

Factors Influencing the Design of Public Safety Networks

Public safety networks are a specific example of government's movement toward using information and communication technologies to help organizations improve operational effectiveness, reduce operational costs, streamline services, improve productivity and policy-making, and flatten bureaucracy. Less common are joint efforts using information technologies that cross traditional agency boundaries to accomplish shared agency goals. Three areas of government that have been particularly prominent in the pursuit of increased information-sharing and cross-boundary collaboration are homeland security, health care, and public safety (the focus of this report).

Public safety agencies generally, and police agencies in particular, have been at the forefront of efforts to leverage information and communications technology (ICT) and to better share information across agency boundaries. Public safety agencies need to collaborate, as incidents often require the services of more than one agency. Even routine events like automobile collisions on the interstate typically require response from multiple services including police, ambulance, fire, hazardous materials, and transportation.

Moreover, information and communications technologies are considered central to modern policing and are ubiquitous in police agencies. However, the legacy IT infrastructures and long-standing practices within police agencies often inhibit their ability to capitalize on the benefits of using modern networked technologies to collaborate. The legacy ICT environment among police agencies is one of non-integrated, diverse, non-interoperable systems. This patchwork infrastructure is attributable to three factors.

Factor One: The federated structure of policing in the United States. Policing in the United States is structured in a manner that runs counter to the goal of a coordinated, integrated ICT infrastructure. There are more than 19,000 police agencies in the United States (many of which include fewer than 50 people).⁵ Each agency has its own organizational norms, rules, policies, funding mechanisms, and ICT infrastructures. Fewer than 1,000 have a dedicated chief information officer. As a result, there has been little coordination at a national level of information and communication technology development activities in policing. Even national information systems such as the National Criminal Information Center (created in 1968) suffered from poor data quality for decades as a result, in part, of the need to have voluntary compliance with data standards.

Factor Two: Chronic lack of resources. Most police and public safety agencies are chronically under-resourced and so cannot devote scarce resources to information and communication technology development and support. Often, poor systems development practices compound

5. Bureau of Justice Statistics, 2007.

the structural barriers to information-sharing and technology integration. In the United States, only the largest urban agencies have the fiscal resources to fund a large ICT development and support its operation. Historically, police agencies have been early adopters of ICT. But they tend to develop and deploy this new ICT in an ad hoc and isolated fashion. The result of this long-standing practice is that the systems developed by individual agencies are often incompatible with other agencies' systems, and occasionally incompatible with the agency's internal systems. As a result, agencies seeking to integrate their ICT infrastructures for the purpose of interorganizational information-sharing and collaboration find themselves facing significant technological hurdles.

Factor Three: Legacy of data-sharing issues. A third factor that inhibits police agencies' ability to share information and collaborate is an entrenched myopia regarding ownership and access to agency data among administrators and policy-makers. Individual agencies have been highly protective of their data, so integration has been problematic.

Plainly, the public safety domain has great need for and significant challenges to collaborating with its partners in meeting the demands of a wide variety of public safety incidents. The next section describes how such collaborations play out. The study on which the findings are based is of actual PSNs and is briefly described in the box on page 9.

Findings about Implementing Public Safety Networks

The objective of this report is to provide actionable implementation guidance, based on analysis of PSN-provided data, to support organizational decision-makers, information-systems developers, and policy-makers on how best to design, develop, and deploy cross-boundary, collaboration-enhancing systems. Basing the guidance recommended here on a large number of existing PSNs increases the likelihood that using the recommended design, development, and deployment of PSNs and similar efforts in other domains will be successful.

To frame the findings, it is useful to understand some general observations or patterns that led to the ensuing recommendations. The nine findings reported below are drawn from two sources:

- The 80 experts interviewed in the nationwide survey of PSNs
- Analysis of six detailed case studies of exemplar PSNs

The PSNs vary quite a bit in fundamental ways, so the findings reported here are notable for their wide applicability—transcending very different organizational arrangements, technologies, and missions.

Finding One: There are two basic types of PSNs, court-oriented or routine-policing oriented

Slightly more than half of the PSNs in the study are oriented toward supporting courts. These PSNs tend to focus on information and data-sharing strategies and processes that allow various participants in court proceedings to more easily access and share digital records. Court-oriented PSNs have strong policies regarding data access, information-sharing, and data usage. The underlying PSN technology tends to be focused on supporting data integration, data sharing, and data security. Many of the court-oriented PSNs have legacy technologies (such as main-frame computers and complex proprietary software systems). Connections to policing operations are often focused on investigation reports (not incidents). Court-oriented PSNs provide little in the way of operational support or services to other public-safety agencies.

Police-oriented PSNs typically focus their attention on supporting a diverse portfolio of operationally oriented applications and processes. This portfolio approach makes these systems appear

CapWIN

CapWIN (the Capital Wireless Information Net) is a regional coalition of public safety and transportation agencies across Maryland, Virginia, and the District of Columbia. The federal government is also a member. The mission of CapWIN is to enable and promote interoperable data communications, operational data access, and incident and situational awareness across jurisdictions and disciplines. CapWIN's infrastructure provides coordinated incident management for routine, emergency, and planned events.

Formation of the CapWIN Public Safety Network (PSN) was precipitated by a 1998 incident in which a man threatened to jump from the Woodrow Wilson Bridge, which crosses the Potomac River. The Wilson Bridge is owned and maintained by the District of Columbia, but one end is in Maryland and the other end is in Virginia. This incident caused massive gridlock in the District, Virginia, and Maryland as responders from multiple jurisdictions could not communicate with each other to share information and coordinate their activities. Subsequently, the 9/11 attacks increased support for CapWIN because of the need to more effectively communicate across jurisdictions.

CapWIN services include:

- CapWIN Comm-Link, which provides direct, real-time data communications to all CapWIN participants regardless of discipline (police, fire, transit, or emergency) or jurisdiction. Providing robust and secure messaging tools, CapWIN participants can now communicate instantly one-to-one or in public or private groups supporting specific incidents or activities taking place in CapWIN.
- CapWIN Global View+GIS, which provides users with a comprehensive picture of live incidents and events taking place in their jurisdictions and across the region. It includes data from transportation, transit, public safety, and emergency management agencies. CapWIN GlobalView+GIS also provides first responders in the field and command centers with immediate access to incident data from across jurisdictions and disciplines

As of 2012, CapWIN supports approximately 7,000 users in 150 participating agencies from all levels of government across the greater metropolitan Washington area. CapWIN includes 114 participating agencies in law enforcement; five are fire-related, nine are transportation agencies, and eight provide emergency services. Its users exchange more than 15,000 messages each day.

CapWIN introduced a sliding scale annual membership fee in 2007, to augment the grants and earmarks it relied on for its initial funding. Operationally, CapWIN's offices are in Greenbelt, Maryland, and it serves under a board of directors comprised of representatives from its member agencies.

For more information about CapWIN, visit <http://www.capwin.org>.

more like portals than end-to-end process-supporting systems. Many of the police-oriented PSNs showcase their ability to support multiple access devices, providing for mobile use (indicating their attention to reaching out to support the patrolwoman in her car or the officer at the scene of an incident). Many of these PSNs also support emergency management functionality and many have dispatch functionality embedded into the core operational structures. The box on this page describes CapWIN, a police-oriented PSN.

Based on this finding, there is no clear pattern of how to best organize for either of these two groups. That is, the type of PSN does not seem to dictate how it is organized. Likewise, performance levels vary across both groups of PSNs, suggesting that the type of PSN does not seem to dictate performance. Taken together, this suggests that the form, performance, and mission of a PSN are tied to its particular situation, the players involved, and the needs of that geographic jurisdiction.

Finding Two: PSNs exist for many reasons

The presence of a PSN is not strongly correlated with location within the United States; crime rate; spending on police, courts, or technology; political party or voter tendencies (e.g., the partisan leanings of the electorate); number of public-safety agencies within the coverage area; presence of state or national borders, or many other demographic characteristics.

There is, however, a wealth of anecdotal evidence suggesting that some PSNs arose in response to high-profile incidents. For example, CapWIN's origin is said to stem from the day in 1998 when a bridge-jumper poised over the Potomac River brought traffic to a standstill and exposed the communication shortcomings that existed among Maryland, D.C., and Virginia public safety agencies. Other PSN creation stories arise from preexisting informal collaborations, personal friendships, and innovations among local agencies. In sum, the reasons why PSNs come to exist vary widely.

Finding Three: A PSN's technology architecture accumulates

The data make clear that a PSN's technology elements reflect some—often unique—combination of preexisting systems with new functionality, new applications, new technologies, or new devices/systems to provide for sharing data, communications, security, and other user needs. The resulting IT architecture is made up of multiple software and hardware vendors' products, proprietary and sometimes open-source software, third-party telecommunications carriers, and data from many sources. New technologies and applications are added. But, older legacy systems are rarely retired. This accretion and the resulting variety of IT components are the central drivers of what appears to be a trajectory of increasing technological complexity over time. This means that a PSN's technological structure will demand constant attention to minimize its complexity as it grows and evolves over time.

Finding Four: Security choices drive PSN design

Data security and access security concerns drive many design decisions and are often a first consideration. The need to address security mandates often constrains design choices, impacts the ways in which the PSN services can be used, demands extensive governance attention, and increases the PSN's technological complexity. Security constraints drives access, limit PSN membership, and curtail data availability for particular users. Security restrictions increase with the number of boundaries to be crossed.

Finding Five: Data control and data ownership are major organizational and technological issues

A combination of laws, regulations, mandates, technology standards, political concerns, budget control requirements, and critical security and privacy issues make data access, sharing, and control one of the most complicated issues for PSNs. Data-sharing requirements must be coordinated centrally by the PSN, making this a central technology and governance issue. And data-sharing constraints often require PSNs to develop numerous information-sharing agreements to govern use and to give constant attention to data management. Disparate, independent, and varied data sources complicate efforts to ensure data quality, so this becomes a constant concern—one with direct implications for usage and reliability. The disparate, independent, and varied data sources require middleware or data bridges, increasing the complexity of the technology architecture and its governance. Likewise, disparate, independent, and varied data sources limit the ability of PSN staff to create common data definitions and standardized data formats.

Finding Six: PSNs designed for routine use get used in non-routine situations

What becomes clear from the PSN data and other studies of system use is that users rely extensively on experience and routine to learn about a system. Most PSNs are a complex, and sometimes not well integrated, set of services in support of many business processes. Users become familiar with the PSN through routine use, leveraging their knowledge to create work-arounds and to master the PSN (as many have overlapping functionality). It is clear that training is helpful for getting started, but experience with using the PSN is what people need to get value. There are also additional problems that emerge with non-standardized uses of PSNs in emergencies: variations in the uses of a common PSN across various stakeholder groups reduce operational utility in large-scale emergencies or events.

Finding Seven: PSNs constantly struggle for funding

Securing funding is a constant concern for PSNs, demanding substantial time and attention from PSN leaders. Only half of the PSNs in the study have some sort of steady operational funding; the rest rely on annual subscriptions, grants, set-asides and charge-backs. This situation leads PSN staff to seek out opportunistic funding and to make most operational and technology decisions with one, if not both, eyes on their budget. Given current and projected federal and state budgets, chronic underfunding will persist, likely with substantial year-to-year changes. The chronic funding concerns typically lead PSN leadership to skimp on maintenance even while most PSNs' heterogeneous architecture drives up operational costs.

Finding Eight: PSNs are complex efforts

There are three reasons why PSNs are complex.

- **PSNs have many stakeholders, and each stakeholder group has particular—and sometimes important and unique—demands on it.** Meeting the needs of the various participants requires PSNs to develop a set of governance processes that give stakeholders a voice in decision-making and increase the organizational complexity. Likewise, the varied and legitimate needs of PSN stakeholders drive the technology architecture to become complex and diverse. Given PSNs' boundary-spanning mission and the fact that they often lack a clear chain of command, governance becomes a negotiated effort that spans political, operational, and technological decision-making. Such negotiation and compromise will be reflected in design decisions.
- **PSNs must respond to an array of mandates, laws, and procedures.** These may require new functionality to accommodate changes in law, funding mechanisms, operating procedures, and technology requirements (i.e., driven by technology vendor decisions regarding software). Certainly mandates can lead to improvements in the PSN, though they also create constraints on what is possible. Sometimes, new laws or new mandates conflict with one another—such as the desire to expand mobile access and the importance of data security and information-sharing controls. Most PSNs take an active stance in favor of mandates and seek to participate in regulations or standards-setting activities. Seasoned PSN leaders are often very focused on technology standards, security, and data management/control discussions.
- **PSNs must meet multiple, legitimate, and often conflicting measures of performance.** More than 15 distinct types of performance measures were identified in the study and 11 of them were important to more than half of the PSNs. Five performance measures (usage, interagency collaboration metrics, productivity, reliability, and data quality) were important to more than 90 percent of the PSNs. Moreover, the results make clear that individual stakeholders evaluate the PSN by their particular measures, and that use is driven by the behavior of users in pursuit of performance goals. These competing goals place great demands on PSN governance processes, often limiting organizational effectiveness and

efficiency as design tradeoffs result from a need to address competing goals. Design tradeoffs typically increase a PSN's technological complexity.

Finding Nine: PSN governance spans multiple organizational boundaries

Most PSNs' organizational structure and governance dictate that they have several funding streams, multiple reporting relationships, multiple stakeholders who participate actively in committees and often in decision-making roles, and typically have connections to local, county, state and sometimes federal agencies. The PSN governance effort typically covers many technology aspects (data, devices, applications, core technologies, standards, etc.), membership, budgeting, and community outreach. While governance structures often adapt as the PSN technology evolves, operational situations often demand that PSN leadership respond more quickly than typical consensus-based governance approaches allow. This also makes strategic leadership difficult as the governance structures move to respond to new technology opportunities.

Summary: Findings highlight the complexity and diversity across PSNs

Taken together, these nine findings make it clear that PSNs are both complex and highly variable organizational arrangements that have equally complex and varied technological arrangements (or architectures). This means there is no one kind of PSN and no single, best way to be one. PSNs will often look very different from one another. Despite this variability, PSNs exhibit a set of clear patterns that can be used to help understand PSNs, even as the details of how these patterns play out in specific PSNs vary greatly.

Recommendations for Implementing Collaborative Networks

Studying a phenomenon in great detail should lead to extrapolations about what can and should happen in the future. The five recommendations presented here can guide decision-makers and designers involved in cross-agency information-sharing beyond the public safety area. There are many cross-agency collaborative initiatives underway in many areas of government such as health care, transportation, financial oversight, and homeland security that share many of the characteristics of a PSN; these design prescriptions can also apply to them.

It is also important to stress that the guidelines presented below encompass both the technology and its organizational setting. This approach highlights the closely intertwined nature of collaborative design decisions and suggests that each will have both organizational and technological impacts. Even though each recommendation may initially appear to stress either a technological or organizational imperative, its implications will, on closer study, be seen to encompass both sides of this coin.

Recommendation One: Involve all stakeholders in the design of a collaborative network

This recommendation focuses on two specific aspects of interorganizational information-sharing collaborations. First, these efforts interweave both organizational and technological elements. That is, the collaborative organization and its governance are symbiotically related to the technologies deployed to support this effort.

Second, there is not a one-size-fits-all approach to interorganizational collaborations; the best practices of one may be deal-killers for another. It is therefore important to involve all stakeholder groups. This is more than asking users what services they want (though user involvement is critical, and too often treated as a secondary aspect of many interorganizational collaborations). Stakeholder involvement is critical to ascertaining and accommodating the political, organizational, and budgetary processes and constraints that will shape the collaboration. Stakeholder involvement should also include technologists from multiple agencies, and perhaps vendors who will be tasked to support the collaboration's technology operations, maintain the systems, and advance the services.

An important implication of this recommendation is that organizations must focus explicitly on activities that allow potential collaborators to interact and build trust with one another. It is rare (if not unusual) for two agencies to begin cooperating in any meaningful way without prior professional contact or relationships in a variety of activities that developed a sense of shared expectations and common understanding. The leadership of many PSNs talked about the value of building trust over time by repeatedly engaging in cooperative activity with the same partners. Proactively, this suggests there is value in cultivating relationships across agency borders to further the collaborative network's reach, value, and support.

Recommendation Two: Create collaborative networks that stakeholders will value, participate in, and use

Governance structures and processes should be inclusive, consensus-oriented (or at least participative), and clearly articulated. Systems designers' work should allow users access, provide them services, enhance data quality, encourage routine usage, and maximize reliability.

Efficiency is, of course, critical, but the emphasis on effectiveness suggests that focusing on achieving the technological goals of efficient data processing while maximizing capacity, processing speed, and data storage assets often may not meet the needs of those stakeholders who rely on the information-sharing and cross-boundary collaboration as part of their daily operations.

One implication of this recommendation is the importance of communicating to participants both the lessons learned from successful collaborations and the problems that arise during a collaboration. A focus on communicating lessons learned signals a willingness to listen and to learn, and a realization that interagency collaboration and information-sharing can be hard work. There will be successes—that should be known by all and celebrated—and mistakes—whose lessons can help to ensure that the next effort will be better. The evidence from studying PSNs is that those groups who were able to leverage critical events to generate funding, participation, and stakeholder support tended to be the more successful efforts.

Recommendation Three: Pursue every opportunity to fund a collaborative network

Central to this recommendation is the premise that funding will shape both the technologies and the ways in which the collaboration is governed. The collaboration's governance structure and processes must be designed so that funding considerations are front and center. Moreover, substantial organizational resources should be dedicated to pursuing funding and tuned to reach out to the particular sources that support or enable information-sharing and cross-boundary collaborations. Likewise, the collaboration's information technology design should be developed in ways that foresee resource needs, costs, benefits and other measures important to stakeholders.

Recommendation Four: Develop a diverse set of performance goals

Relative to governance, this recommendation focuses attention on ensuring that each stakeholder group has the means to make their needs clear, to connect their needs to resources, and to put in place assessment and evaluation mechanisms to ensure the collaborative enterprise stays focused on goals. In relation to designing the enabling technology aspects, this recommendation encourages systems designers to attend to the current needs of users, eschewing what users might say they want for those things that will enhance actual performance. Such a focus demands careful attention to users, to their operational needs, and to designs that are use-oriented (and not feature-heavy).

Recommendation Five: Leverage technology to advance a collaborative network

A set of core decisions should be made regarding technology arrangements (architecture). The effects of these technology decisions will be seen in both the operational and strategic aspects of the collaboration. Specific implementation actions include:

- **Design the collaboration's information technology elements to be flexible and modular.** Doing so makes it easier to respond to new laws and mandates, to respond to stakeholder needs, to accommodate new and old technologies within the same system, and to more easily relate to performance measures.

- **Ensure that data custodianship remains with the data's owners.** Acknowledging that data control should reside with data owners will require technology designers to think about different arrangements than if the collaboration itself were to become the custodian. Given the legal, political, and resources pressures on data and data owners, the collaboration should be seen as providing a portal to data, not a warehouse for its storage.
- **Ensure standard security and access approaches are used to frame both technology design decisions and related governance processes.**
- **Plan to build on and incorporate legacy technologies.** Because computing infrastructure technologies are rarely replaced, design decisions must plan to expand on and integrate legacy systems. This suggests that designers should seek to use commodity technologies, common standards, and open-source (or open-standards) products as these are the easiest to build from and work with.
- **Design collaboration and information-sharing processes and technologies to support routine use, as this will help increase system usage.** Then, when adding emergency and special-event functionality into existing systems or functions, it will leverage the value and comfort of routine use. Doing so allows users to bring their knowledge and experience of routine use when dealing with exceptional circumstances, reduces training costs, and increases the value of these features.
- **Emphasize system reliability and stability when designing technology, so that usage will increase.** We know that the more stable and reliable a system is, the more it will be used. A relatively simple but stable system is far more useful than a more complex or interactive system that is less reliable.

Appendix: Examples of Collaboration from Other Policy Arenas

The Promise of Collaborative Voluntary Partnerships: Lessons from the Federal Aviation Administration⁶

Mills (2010) provides design guidance on how government and industry should work together to identify aviation-related safety hazards by using voluntary regulatory partnership programs. In his IBM Center for The Business of Government report, he divides his advice into three areas. The first area, administrative lessons, suggests the following:

- Regulatory agencies should have a dedicated organizational entity focused on voluntary programs.
- Regulatory agencies must dedicate adequate personnel at the local level.
- Regulatory agencies and companies should collaborate on processes that remedy safety hazards.
- Regulatory agencies should use collaborative tools, such as third-party agreements, to implement voluntary partnership programs.

The second area pertains to regulatory lessons:

- Voluntary programs should be truly voluntary.
- Voluntary programs should be non-punitive.
- Confidentiality of voluntarily submitted data is critical.
- VRPPs should complement, not replace, traditional enforcement tools.

Finally, he offers lessons on data analysis and IT:

- Regulatory agencies and companies need effective and robust data analysis capabilities at both the local and national levels.
- Regulatory agencies should use a uniform reporting platform.
- Regulatory agencies should develop a national-level database.

Beyond the Pavement: Urban Design Policy, Procedures and Design Principles for Road and Traffic Authorities⁷

Chesterman (2010) suggests areas to assist in the development and design of road and traffic authority projects. His advice contains both general guidance and specific suggestions about

6. Mills, R.W. (2010) *The Promise of Collaborative Voluntary Relationships: Lessons from the Federal Aviation Administration*. IBM Center for The Business of Government. Retrieved from <http://www.businessofgovernment.org/sites/default/files/The%20Promise%20of%20Collaborative%20Voluntary%20Partnerships.pdf>.

7. Chesterman, D. (2010) "Beyond the Pavement: RTA Urban Design Policy, Procedures and Design Principles." Rev. of *Beyond the Pavement: RTA Urban Design Policy, Procedures and Design Principles*. Radar Books September–October 46.

transportation infrastructure. In discussing the contribution roads make to urban structure and revitalization, he identifies roads as the framework of urban areas. They must fit in with the built fabric, so designers must understand the disruptive effects that roads can have on certain environments. Roads connect modes and communities, so they should not divide areas nor be difficult to cross. They must fit with the landform, and should be conceived as part of the landscape. As a result, they need to respond to the natural pattern by reflecting the landscape and ecology. Road design should incorporate heritage and cultural contexts by protecting structures, environments, landscapes, by revitalizing bridges, etc. The designer's goal should be to create an "experience in movement" and use the design of views, bridges, barriers, retaining walls, lighting, signage, utilities, noise barriers, and plantings to break driving monotony. The designer should create self-explaining roads, and design roads so safety is intuitive to the driver. Finally, in order to achieve integrated and minimal maintenance design, good infrastructure design must be low maintenance.

Design Principles Guide New Chicago-Area Schools⁸

Yednak (2002) proposes that communities build school facilities that change with educational needs and with the neighborhood. He suggests that efforts be made to make the school the hallmark of the town, which means that it should be designed to be used by the community as well as the students. He stresses that the building's space should be flexible. He promotes a cookie-cutter design, so that many similar buildings can be designed at a cost savings.

Universal Instructional Design Principles for Mobile Learning⁹

Elias (2011) provides guidance for offering high-quality and accessible mobile learning using handheld computers and mobile telephones. In order to support equitable use, the device should deliver content in the simplest possible formats. He is also a proponent of flexible use, so advises designers to package content in small bits, consider unconventional assignment options, and leave it to learners to illustrate and animate courses. He also advocates keeping the system simple and intuitive—by keeping learner interfaces simple, keeping code simple, and using open sites and software. He suggests employing perceptible information, including acceptable levels of tolerance for error, and requiring low physical and technical effort on the part of the adopter. The system should create a community of learners and support, by encouraging multiple methods of communication and by grouping learners according to technological access and/or preferences. The system should generate a positive instructional climate, and be able to push regular reminders, requests, quizzes, and questions. Finally, the system should pull in learner-generated content.

Environmental Collaboration: Lessons Learned about Cross-Boundary Collaborations¹⁰

Friedman and Foster (2011) produced a report for the IBM Center for The Business of Government containing lessons on how to start and sustain collaborations addressing environmental issues that cross international boundaries in North America. They offer six design guidelines for these cross-boundary efforts:

- Set up a legal structure that allows for equal participation on both sides of the border

8. Yednak, C. (2002) "Design Principles Guide New Chicago-Area Schools." *Chicago Tribune* August 27, 2002.

9. Elias, T. (2011) "Universal Instructional Design Principles for Mobile Learning." *International Review of Research in Open and Distance Learning* 12.2: 144–56.

10. Friedman, K.B. & Foster, K.A. (2011) *Environmental Collaboration: Lessons Learned About Cross-Boundary Collaborations*. IBM Center for the Business of Government. Retrieved from <http://www.businessofgovernment.org/sites/default/files/Environmental%20Collaboration.pdf>

- Legally codify your mission
- Be flexible and willing to adapt
- Commit expectations, needs, priorities, and goals to writing
- Dedicate staff to the endeavor
- Recruit leaders who have a broad network and social capital in the subject's area and who are willing to bring other relevant people on board

References

Design and Implementation Guidance Background and Examples

Agre, P. (2000). "Infrastructure and Institutional Change in the Networked University." *Information, Communication and Society*, 3(4): 494–507.

Baldwin, C. and B. Clark. (1999). *Design Rules: The Power of Modularity*. Cambridge, MA: MIT Press.

Bar, F. (2001). "The Construction of Marketplace Architecture." In *Tracking a Transformation: E-commerce and the Terms of Competition in Industries*. The BRIE-IGCC Economy Project Task Force on the Internet, Eds. Washington, D.C.: Brookings Institution Press. 27–49.

Chesterman, D. (2010). "Beyond the Pavement: RTA Urban Design Policy, Procedures and Design Principles." Rev. of *Beyond the Pavement: RTA Urban Design Policy, Procedures and Design Principles*. Radar Books, September–October. 46.

Denyer, D., D. Tranfield, and J. van Aken. (2008). "Developing Design Propositions through Research Synthesis." *Organization Studies*, 29; 393–413.

Elias, T. (2011). "Universal Instructional Design Principles for Mobile Learning." *International Review of Research in Open and Distance Learning*, 12.2: 144–56.

Fedorowicz, J. and Dias, M. (2010). "A Decade of Design in Digital Government Research." *Government Information Quarterly*. Volume 27, Issue 1, 1–8. January.

Friedman, K.B., and K.A. Foster. (2011). *Environmental Collaboration: Lessons Learned About Cross-Boundary Collaborations*. IBM Center for The Business of Government. Retrieved from <http://www.businessofgovernment.org/sites/default/files/Environmental%20Collaboration.pdf>

Galbraith, J. (1977). *Organization Design*. Reading, MA: Addison-Wesley Publishing Company.

Markus, M., A. Majchrzak, and L. Gasser. (2002) "A Design Theory for Systems That Support Emergent Knowledge Processes." *MIS Quarterly*, 179–213.

Mills, R.W. (2010). *The Promise of Collaborative Voluntary Relationships: Lessons from the Federal Aviation Administration*. IBM Center for The Business of Government. Retrieved from <http://www.businessofgovernment.org/sites/default/files/The%20Promise%20of%20Collaborative%20Voluntary%20Partnerships.pdf>.

Moggridge, W. (2007). *Designing Interactions*. MIT Press; Cambridge, MA.

Nelson, H., and E. Stolterman. (2003). *The Design Way: Intentional Change in an Unpredictable World; Foundations and Fundamentals of Design Competence*. Englewood Cliffs, NJ: Educational Technology Publications.

Norman, D.A. (1988). *The Design of Everyday Things*. New York: Doubleday.

Peterson, R. (2010). "Information Design—Principles and Guidelines." *Journal of Visual Literacy*. 29 (2). 167–182.

Pries-Heje, J. and R. Baskerville. (2008). "The Design Theory Nexus." *MIS Quarterly*, 32(4): 731–755.

Yednak, C. (2002). "Design Principles Guide New Chicago-Area Schools." *Chicago Tribune*, August 27, 2002.

PSN Project Team Publications

Fedorowicz, J., U.J. Gelinias, J.L. Gogan, M. Howard, M.L. Markus, C. Usoff, and R. Vidgen. (2010). "Modeling Physical Barriers to Interorganizational System Implementation Success," *International Journal of Information Technology and Management*. Volume 9, No. 4, 365–388.

Fedorowicz, J., U.J. Gelinias, J.L. Gogan, and C.B. Williams. (2008). "Strategic Alignment of Participant Motivations in E-Government Collaborations: The Internet Payment Platform Pilot." *Government Information Quarterly*, (26)1, 51–59.

Fedorowicz, J., and J.L. Gogan. (2010). "Reinvention of Interorganizational Systems: A Case Analysis of the Diffusion of a Bioterror Surveillance System." *Information Systems Frontiers*. Volume 12, Issue 1, 81–95. March.

Fedorowicz, J., J.L. Gogan, and C. Culnan. (2010). "Barriers to Interorganizational Information-Sharing in e-Government: A Stakeholder Analysis." *The Information Society*. Volume 26, Issue 5, 315–329.

Fedorowicz, J., J.L. Gogan, and C.B. Williams. (2006). *The e-Government Collaboration Challenge: Lessons from Five Case Studies*. IBM Center for The Business of Government, Washington, D.C. Retrieved from <http://www.businessofgovernment.org/sites/default/files/E-Government.pdf>.

Fedorowicz, J., J.L. Gogan, and C.B. Williams. (2007). "A Collaborative Network for First Responders: Lessons from the CapWIN Case." *Government Information Quarterly*. Volume 24, Issue 4. October. 785–807.

Gantman, S. (2011). "IT Outsourcing in the Public Sector: A Literature Analysis." *Journal of Global Information Technology Management*. Volume 14, No. 2. April.

Ghosh, A. and J. Fedorowicz. (2008). "The Role of Trust in Supply Chain Governance." *Business Process Management Journal*. 14 (4), 453–470.

Gogan, J.L., C.B. Williams, and J. Fedorowicz. (2007) "RFID and Interorganizational Collaboration: Political and Administrative Challenges." *Electronic Government: An International Journal*. Volume 4, Issue 4, 423–435.

Markus, M.L. (2005). "The Technology Shaping Effects of e-Collaboration Technologies: Bugs and Features." *International Journal of e-Collaboration*. 1 (1), 1–23.

Markus, M.L., and U.J. Gelinis, Jr. (2006). "Comparing the Standards Lens with Other Perspectives in IS Innovations: The Case of CPFR." *International Journal of IT Standards and Standardization Research*. 4 (1), 24–42.

Sawyer, S, C. Hinnant, and T. Rizzuto. (2008). "Planning for Platforms: Pennsylvania's Transition to Enterprise Computing as a Study in Strategic Alignment." *Government Information Quarterly* 25, 645–668.

Sawyer, S., A. Tapia, L. Pesheck, and J. Davenport. (2004). "Mobility and the First Responder." *Communications of the ACM*. 47 (3), 62–65.

Tyworth, M. (2010). Review Essay: "Policing and Technology." *The Information Society*. Volume 27, No. 1.

Wigand, R.T., C.W. Steinfield, and M.L Markus. (2005). "IT Standards Choices and Industry Structure Outcomes: The Case of the United States Home Mortgage Industry." *Journal of Management Information Systems*. 22 (2), 165–191.

Williams, C.B., J. Fedorowicz, S. Sawyer, M. Dias, D. Jacobson, M. Tyworth, and S. Vilvovsky. (2009). "The Formation of Interorganizational Information-Sharing Networks in Public Safety: Cartographic Insights on Rational Choice and Institutional Explanations." *Information Polity*. Volume 14, Nos. 1–2, 13–29.

Williams, C.B., J.L. Gogan, and J. Fedorowicz. (2005). "Public Safety and Cross-Boundary Data Sharing: Lessons from the CapWIN Project." *IEEE Computer*. 38 (12), 28.

Other Useful Criminal Justice and Public Safety Publications

Bergmann, S. and J. Bliss. (2004). "Foundations of Cross-Boundary Cooperation: Resource Management at the Public–Private Interface." *Society and Natural Resources*. 17(5), 377–393.

Brown, M.M., and Brudney, J.L. (2003). "Learning Organizations in the P Sector? A Study of Police Agencies Employing Information and Technology to Advance Knowledge." *Public Administration Review*. 63 (1), 30–43.

Bureau of Justice Statistics. (2007). Census of State and Local Law Enforcement Agencies, 2004. Retrieved from <http://www.ojp.usdoj.gov/bjs/abstract/cslea04.htm>.

Chan, J.B.L. (2001). "The Technological Game: How Information Technology is Transforming Police Practice." *Journal of Criminology and Criminal Justice*. 1(2), 139–159.

Dawes, S.S. (1996). "Interagency Information-Sharing: Expected Benefits, Manageable Risks." *Journal of Policy Analysis and Management*. 15 (3), 377–394.

Dunworth, T. (2005). "Information Technology and the Criminal Justice System: A Historical Review." In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (1–28). Thousand Oaks, CA: Sage Publications, Inc.

Gil-Garcia, J.R., I. Chengalur-Smith, and P. Duchessi, (2007). "Collaborative e-Government: Impediments and Benefits of Information-Sharing Projects in the Public Sector." *European Journal of Information Systems*. 16 (2), 121–133.

Gil-Garcia, J.R., C.A. Schneider, and T.A. Pardo. (2004). "Effective Strategies in Justice Information Integration: A Brief Current Practices Review." Center for Technology in Government: http://www.ctg.albany.edu/publications/reports/effective_strategies.

Hoey, A. (1998). "Techno-Cops: Information Technology and Law Enforcement." *International Journal of Law and Information Technology*. 6 (1), 69–90.

Kamensky, J. (2007). "Forum Introduction: Toward Greater Collaboration in Government." IBM Center for The Business of Government. <http://www.businessofgovernment.org/pdfs/forum07.pdf>.

Laudon, K.C. (1986). "Data Quality and Due Process in Large Interorganizational Record Systems." *Communications of the ACM*. 29 (1), 4–11.

Manning, P.K. (2003). *Policing Contingencies*. Chicago: University of Chicago Press.

Manoj, B.S., and A.H. Baker. (2007). "Communication Challenges in Emergency Response." *Communications of the ACM*. 50 (3), 51–53.

National Association of State Chief Information Officers. (2003). "Concept for Operations for Integrated Justice Information-Sharing Systems." <https://www.nascio.org/hotIssues/EA/ConOps2003.pdf>.

National Association of State Chief Information Officers (NASCIO). (2005). "A Blueprint for Better Government: The Information-Sharing Imperative."

National Commission on Terrorist Attacks Upon the United States. (2004). *How to Do It? A Different Way of Organizing the Government. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States: Official Government Edition* 399–428.

Nunn, S. (1993). "Computers in the Cop Car: Impact of the Mobile Digital Terminal Technology on Motor Vehicle Theft Clearance and Recovery Rates in a Texas City." *Evaluation Review*. 17 (2), 182–203.

Nunn, S., and K. Quinet. (2002). "Evaluating the Effects of Information Technology on Problem-Oriented Policing: If It Doesn't Fit, Must We Quit?" *Evaluation Review*. 26 (1), 81–108.

Reaves, B.A. (2010). "Local Police Departments, 2007." Washington, D.C.: United States Department of Justice, Bureau of Justice Statistics.

Richman, D.C. (2000). "The Changing Boundaries Between Federal and Local Law Enforcement." In C. M. Friel (Ed.), *Boundary Changes in Criminal Justice Organizations—Criminal Justice 2000* (Volume 2, 81–111). Rockville, MD: National Institute of Justice.

Tyworth, M. (2009). "Reflections of Identity: How Information Systems Mirror the Organization as Social Actor." Unpublished dissertation, The Pennsylvania State University, University Park, PA.

United States Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. (2011). *Law Enforcement Management and Administrative Statistics (LEMAS)*. 2007: Inter-University Consortium for Political and Social Research (ICPSR), distributor.

Waugh, W.L. Jr., and G. Streib, (2006). "Collaboration and Leadership for Effective Emergency Management." *Public Administration Review*, 66 (s1), 131–140.

Williams, S.R., and C. Aasheim. (2005). "Information Technology in the Practice of Law Enforcement." *Journal of Cases on Information Technology*, 7 (1), 71–91.

Acknowledgements

We thank Christine B. Williams, M. Lynne Markus, Michael Tyworth, Martin Dias, Arthur Tomasino, Sonia Gantman, Dax Jacobson, and Robert Schrier for their participation in the data collection and its analysis. We are indebted to the many organizations and individuals who participated in the in-depth case studies and surveys.

The work done on this report is supported in part by the IBM Center for The Business of Government. We thank Mark Abramson and John Kamensky for their guidance and insights on earlier drafts of this report. The findings, recommendations and opinions contained in this report are those of the authors and do not necessarily reflect the views of IBM.

This research underlying this work is supported in part by National Science Foundation grants NSF-0852688 and NSF-0534877. Any opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the National Science Foundation.

About the Authors

Jane Fedorowicz, the Rae D. Anderson Professor of Accounting and Information Systems, holds a joint appointment in the Accountancy and Information & Process Management departments at Bentley University, where she teaches courses on enterprise system configuration, business processes, and internal controls. She is principal investigator of a National Science Foundation project team studying design issues for police and government agency collaboration using public safety networks. She also served as principal investigator for the Bentley Invision Project, an international research team housed at Bentley examining interorganizational information-sharing and the coordination infrastructures supporting these relationships in supply chains, government, and health care. Her interdisciplinary research supports a sociotechnical perspective on organizational collaboration in both the public and private sectors. The Association for Information Systems recognized her contributions to the Information Systems field by naming her an AIS Fellow in 2006.



Dr. Fedorowicz has published over 125 articles in refereed journals and conference proceedings, and coauthored a textbook entitled “Business Processes and Information Technology.” She has served in a governance capacity for a number of professional associations, including the Association for Information Systems (AIS), the American Accounting Association (AAA) and the Institute for Operations Research and the Management Sciences (INFORMS).

Dr. Fedorowicz earned MS and PhD degrees in Systems Sciences from The Tepper School at Carnegie Mellon University in Pittsburgh, Pennsylvania.

Steve Sawyer is a Professor in the School of Information Studies at Syracuse University and currently serves as Associate Dean for Research and Doctoral Programs. He does social informatics research, with a particular focus on the ways in which people work together and use information and communication technologies. His research has been supported by Credit Suisse, Corning, IBM, Sonoco, Xerox, the Lattanze Foundation, Lockheed Martin, Lucent Technologies, the Commonwealth of Pennsylvania, the National Center for Real Estate Research, and the National Science Foundation.



Prior to rejoining Syracuse University (where he first worked as a faculty member from 1994–1999), he helped start Penn State's College of Information Sciences and Technology and served on the faculty from 1999–2008. At Syracuse he was named Professor of the Year in 1997 and served as the Director of its Ph.D. program. At Penn State, Steve was named the first IST Faculty Member of the Year in 2001. In 2002, he won Penn State's inaugural George McMurtry Award for Teaching.

Since 1995, Steve has published nearly 100 works, including two books, and papers in a range of journals such as *Communications of the ACM*, *European Journal of Information Systems*, *Information Technology & People*, *The IBM Systems Journal*, *The Information Society*, *The Information Systems Journal*, and *Computer Personnel*. Sawyer is a senior editor with the *Journal of Information Technology*, and an associate editor at *The Information Society* and the *Journal of the American Society for Information Science and Technology*. Steve is a member of the American Society of Information Science and Technology, the Academy of Management, Association of Computing Machinery (ACM), Association for Information Systems (AIS) and the International Federation of Information Processing's (IFIP) working groups on information systems in organization and society (IFIP WG8.2) and on computers and work (IFIP WG9.1), which he chairs.

Sawyer earned his Doctorate in Business Administration from Boston University in 1995. He also has master's degrees in both Ocean Engineering and Information Systems.

Key Contact Information

Jane Fedorowicz

Rae D. Anderson Professor of Accounting and Information Systems
Departments of Accountancy and Information & Process Management
Bentley University
175 Forest Street
Waltham, MA 02452
+1-781-891-3153
(fax) +1-781-891-2896

e-mail: jfedorowicz@bentley.edu

web pages: <https://faculty.bentley.edu/details.asp?uname=jfedorowicz>
www.BentleyInvision.org
www.PublicSafetyNetworksStudy.org

Steve Sawyer

Professor
School of Information Studies
Syracuse University
344 Hinds Hall
Syracuse, NY 13244
ssawyer@syr.edu
315-443-6147
(fax) 315-443-5806

e-mail: ssawyer@syr.edu

web pages: <http://sawyer.syr.edu>
<http://www.PublicSafetyNetworksStudy.org>
<http://sociotech.net>



Reports from **IBM Center for The Business of Government**

For a full listing of IBM Center publications, visit the Center's website at www.businessofgovernment.org.

Recent reports available on the website include:

Assessing the Recovery Act

Key Actions That Contribute to Successful Program Implementation: Lessons from the Recovery Act by Richard Callahan, Sandra O. Archibald, Kay A. Sterner, and H. Brinton Milward

Managing Recovery: An Insider's View by G. Edward DeSeve

Virginia's Implementation of the American Recovery and Reinvestment Act: Forging a New Intergovernmental Partnership by Anne Khademian and Sang Choi

Collaborating Across Boundaries

Environmental Collaboration: Lessons Learned About Cross-Boundary Collaborations by Kathryn Bryk Friedman and Kathryn A. Foster

Conserving Energy and the Environment

Implementing Sustainability in Federal Agencies: An Early Assessment of President Obama's Executive Order 13514 by Daniel J. Fiorino

Breaking New Ground: Promoting Environmental and Energy Programs in Local Government by James H. Svara, Anna Read, and Evelina Moulder

Fostering Transparency and Democracy

Assessing Public Participation in an Open Government Era: A Review of Federal Agency Plans by Carolyn J. Lukensmeyer, Joe Goldman, and David Stern

Use of Dashboards in Government by Sukumar Ganapati

Improving Performance

Improving Government Contracting: Lessons from Bid Protests of Department of Defense Source Selections by Steven M. Maser

A Guide to Data-Driven Performance Reviews by Harry Hatry and Elizabeth Davies

A Leader's Guide to Transformation: Developing a Playbook for Successful Change Initiatives by Robert A. F. Reisner

Managing Finances

Strategies to Cut Costs and Improve Performance by Charles L. Prow, Debra Cammer Hines, and Daniel B. Prieto

Strengthening Cybersecurity

A Best Practices Guide for Mitigating Risk in the Use of Social Media by Alan Oxley

A Best Practices Guide to Information Security by Clay Posey, Tom L. Roberts, and James F. Courtney

Transforming the Workforce

Engaging a Multi-Generational Workforce: Practical Advice for Government Managers by Susan Hannam and Bonni Yordi

Implementing Telework: Lessons Learned from Four Federal Agencies by Scott P. Overmyer

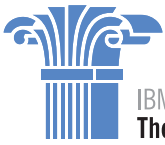
Using Technology

Working the Network: A Manager's Guide for Using Twitter in Government by Ines Mergel

Reverse Auctioning: Saving Money and Increasing Transparency by David C. Wyld

Using Online Tools to Engage—and be Engaged by—The Public by Matt Leighninger

An Open Government Implementation Model: Moving to Increased Public Engagement by Gwanhoo Lee and Young Hoon Kwak



IBM Center for
The Business of Government

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit: ibm.com

For more information:

Jonathan D. Breul

Executive Director

IBM Center for The Business of Government

600 14th Street NW

Second Floor

Washington, DC 20005

202-551-9342

website: www.businessofgovernment.org

e-mail: businessofgovernment@us.ibm.com

Cover photo: © Mary Altaffer/Pool/Reuters/Corbis

Stay connected with the
IBM Center on:



or, send us your name and
e-mail to receive our newsletters.