2011

Interoperability and information sharing

Sean P. Varano
Roger Williams University, svarano@rwu.edu

Thomas J. Dover
Federal Bureau of Investigation

Recommended Citation

Varano, S. P., & Dover, T. 2011. "Interoperability and information sharing." In *The future of law enforcement: A consideration of potential allies and adversaries,* edited by J. A. Scherer & J. P. Jarvis, 125-140. Quantico, VA: Federal Bureau of Investigations.

Interoperability and Information Sharing

Sean P. Varano[38] and Thomas J. Dover[39]

Communication and information sharing are two of the most pressing issues facing the public safety community today. In previous chapters of this volume, authors have made note of the changing public safety landscape as it relates to the need for enhanced information and intelligence sharing among a broad cross-section of organizations. Public safety organizations, particularly law enforcement agencies, have been quick to adopt emerging technologies that have allowed for greater communication and information sharing capacities. While substantial improvements have been made over the decades that enhanced communication and information sharing, many challenges remain in the move to seamlessly integrated communication capacities. The key challenge in the upcoming decades relates to the *technical* and *cultural* changes necessary to achieve integrated communication systems. There is no shortage of resources given to increasing the communications capacity of the public safety community, yet serious challenges remain in the degree of interoperability within and across public safety domains. Interoperability has in many ways become *the* defining issue in the arenas of communications and information sharing. This chapter will provide an overview of critical historical events that placed questions of interoperability and information sharing on the national agenda. The chapter will also provide an overview of national models for information sharing.

Background

The September 11th, 2001 terrorism attacks as well Hurricanes Katrina and Rita in 2005 put the challenges associated with the interoperability of communication systems across the public safety landscape in the public spotlight. On the morning of September 11th, 2001 law enforcement, fire, medical, military and private security personnel from the New York City region, as well as, countless numbers of private citizens responded to the unfolding tragedy in the World Trade Center towers in lower Manhattan. The sheer volume of personnel responding

[38] *Dr. Sean Varano is currently an Assistant Professor in the School of Justice Studies at Roger Williams University.*
[39] *Mr. Thomas Dover is currently a Crime Analyst and Instructor in the Behavioral Science Unit, Federal Bureau of Investigation*.

to the WTC theatre to provide assistance to those in need serves as one of the defining moments in American history. What quickly became apparent on that fateful morning was that the public safety apparatus in and around New York City was woefully underprepared for the tragedy that was unfolding right before their eyes.

The after-action reports that resulted from this tragedy revealed what was otherwise widely known among many sectors of the public safety community, namely, that serious problems existed within the local and regional communication systems that resulted in a systemic communications failure around the WTC theatre. The radio system used by the Fire Department of New York (FDNY), for example, was inadequate in terms of technical capacity to reach all of the locations throughout the WTC theatre (911 Report, 322). Their radio system was not capable of reaching the upper floors of several of the WTC towers due to the sheer size of the buildings and the density of the concrete and other building materials. The myriad of public and private agencies responding to the attacks also used a variety of different communications technologies that were not easily adaptable (McKinsey Report, 2008). In the end, a critical part of the overall WTC tragedy was that the response could have been more effective had proper training and equipment standards been established.

On that same fateful day, those responding to the crash site at the Pentagon experienced much of the same shock and horror as their counterparts in New York. Damage and chaos created a similar sense of panic and need for an immediate regional response across multiple emergency response systems. The response in Washington, DC metropolitan area, however, unfolded differently than those in New York. The DC metro area had a long history of planned exercises in response to anticipated natural and manmade disasters. As part of these exercises, a wide range of federal, state, and local first responders had extensive and well established protocols for responding to such events. Of notable importance, these agencies had protocols in place for dealing with the well-known problems associated with interoperability (Arlington County, 2002). While the Pentagon was plagued by challenges in responding to the unprecedented attack, there were far fewer problems associated with the overall communications capacity and interoperability across agencies. Compared to their counterparts in New York, there was an overall sense that the communication among the responders, particularly in terms of the interoperability and coverage of their systems, to this event was largely effective.

The systemic problems caused by a lack of interoperability within and across public safety sectors emerged as a critical area needing attention by federal, state, and local policymakers in the aftermath of the 9/11 attacks. In an effort to prevent similar problems in the future, the Department of Homeland Security (DHS) had implemented national efforts to enhance interoperability limitations by 2004. The broader policymaking community became acutely aware of what had been known for decades among many first responders; interoperability problems were not unique to New York but instead plagued most regions of the country. As Bitto (2007, p. 460) observed, "[n]ot only is the interoperability problem not novel, but it [ ] seems that each time a major emergency exposes the lack of interoperability, a new blue ribbon commission is convened to study the issue." Several notable interoperability achievements were announced by DHS by September 2004 that were argued to substantially enhance emergency responses by first responders. The following are some of the most notable accomplishments outlined in this report along with brief descriptions (Department of Homeland Security, 2004):

- **Created central office within Homeland Security for interoperability**: The Department of Homeland Security's Office of Interoperability and Compatibility was created as part of the Science and Technology directorate. This office was charged with coordinating federal government activities relating to research and development as well as technical assistance and training as it relates to interoperability.
- **Developed statement of Technical Requirements**: DHS established the first national Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability[i]. The intent of the standards is to aid the country's estimated 50,000 public safety agencies in defining future interoperability requirements for both voice and data communications.
- **Assisted states in acquiring the necessary funding to improve interoperability**: The federal government provided over $280 million in federal funding from 2001-2004 to specifically address the challenges of interoperability across the broad range of public safety agencies.
- **Established Federal Interagency Coordinating Committee**: This council was designed to coordinate all federal efforts geared toward addressing issues of interoperability. More

specifically, the intent was to coordinate efforts directed at grants, technical assistance programs for state and local activities, and federal efforts at regulating airwaves.

These are a few of the federal, state, and local efforts specifically designed to address the problems associated with interoperability. There was a sense by some by early 2005 that the nation had made substantial progress in its efforts to create a more integrated communications system that facilitated interoperability (Department of Homeland Security, 2005). By early 2005, there was a general sense that substantial progress had been made.

While communities across the nation made some notable improvements in the area of interoperability and enhanced communication, Hurricanes Katrina and Rita in August 2005 clearly demonstrated substantial improvements were still necessary. The sheer magnitude of the physical destruction in addition to the large geography posed significant challenges. An after action report revealed that

> Hurricane Katrina destroyed an unprecedented portion of the core communication infrastructure throughout the Gulf Coast region. [T]he storm debilitated 911 emergency call centers, disrupting local emergency services… More than 50,000 utility poles were toppled in Mississippi alone….The complete devastation of the communication infrastructure left emergency responders and citizens without a reliable network across which they could coordinate. (The White House, 2006, 55).

The after action went on to later identify basic standards for operability and interoperability as one of the core recommendations coming out of Katrina (Ibid, 97). Hurricanes Katrina and Rita, however, demonstrated full well that nationally, the United States had still fallen very short of reaching the necessary communications capacity to effectively respond to large scale disasters. As Tom Kean, co-chair of the 9/11 Commission Report noted, "On Sept. 11, people died because police officers couldn't talk to firemen…Katrina was a re-enactment of the same problem. It is really hard to believe this has not been fixed" (Careless, 2006).

The question remains as to why interoperability, a highly technical issue that seemingly could be fixed through the application of proven technologies, remains such a critical challenge. Some have argued that the problem of interoperability is less a *technical* but more *cultural* in nature. As McKay (2010) points out, "[Members of agency A] doesn't talk to agency B because

they two aren't really familiar with each other – or maybe they just don't want to talk. Even when there's a new, multimillion-dollar system, agency personnel revert to previous behavior." New technology, even when implemented well, sometimes amounts to little more than a "$100 million doorstop" (Ibid.). As those across the vast public safety community try to break down the cultural barriers that often thwart effective communication and interoperable systems, many technical challenges remain. The following section outlines key initiatives that have been implemented to enhance information sharing and communication among a diverse set of stakeholders. Particular emphases are given to national programs that are intended to foster collaborative working relationships between public safety entities that not only create frameworks for information sharing and access, but also break down the cultural barriers that impede coordination.

Current Practices Fostering Interoperability

There have been a number of measures employed by local, state, and federal agencies to promote inter-agency communication and flow of information. These efforts include increasing the ability of police, fire, and rescue communication systems to span the gap between jurisdictions, merging resources to provide regional based specializations, and integrating of information collection and dissemination practices. The common goal of all of these efforts has been to provide correct and accurate data to those persons who can contextualize the information and operationalize investigative leads, actionable intelligence, or functional recommendations. Moreover, they are intended to build effective working relationships among agencies that may have limited histories sharing information or developing local, state, or regional data sharing strategies. The goal of these programs is to break down the traditional "silo" approaches whereby individual agencies or public safety sectors (e.g., police, fire, private security) operate either independently, or worse yet, with a sense of antagonism. The following section then outlines some of the efforts by local, state, and federal agencies to integrate their information gathering and dissemination capabilities. Several of these strategies were incorporated in a post 9/11 environment where the flow of information has trumped jurisdictional disputes and necessitated inter-jurisdictional cooperation.

Critical Incident Reviews

There are at least two distinct types of critical incident reviews (CIR). The first is the process whereby agencies responding to a particular incident or set of incidents implement a post-hoc review process with the intent of evaluating the overall quality of the response. The primary purpose of the review process is to identify breakdowns in the response and develop protocols for eliminating problems in the future. The second type of CIR relates to information sharing related to a particular case or investigation. This second CIR model has been developed under the auspices of the federally funded *Project Safe Neighborhoods* in places like Rochester, NY (*see* Klofas, Hipple, McDevitt, Bynum, McGarrell, and Decker, 2006).

The first CIR model is part of evaluating agency preparedness, evaluating the ongoing operational aspects of response and containment, and evaluating post event activities. Arguably, CIRs should be standard operating procedure in any critical incident response. This is especially true due to the potential for civil liability issues, and potential for wide spread, knee-jerk policy responses. CIRs provide agencies with an opportunity to effectively evaluate and critique the incident response. It also assures the public that the agencies involved are doing everything they can to understand the dynamics of the incident, how it led to successes and failures, and how to enhance responses in the future. They represent an important feedback loop that is essential to continued response improvement.

CIRs assess the contribution of each component involved in responding to the incident in terms of that component's role and effectiveness. These components will of course differ depending on the incident, but may generally include initial emergency response, command and control, information collection, information dissemination, collateral containment, media services, and post event follow-up. The purpose of a critical incident review is to understand what did and did not work, and provide reasonable and measured recommendations for further training, resources, and policy. Aspects of data sharing and communication barriers, including problems associated with interoperability, often lie at the core of these efforts. CIRs provide a real life contextual understanding of the significance of the challenges individuals and agencies directly involved in incidents experienced. These events provide a capacity to move the discussion out of the hypothetical into the practical, from the probable into the actual.

In providing an effective evaluation, it is imperative that the politics of the situation be kept at a minimum. Finger-pointing and inter-jurisdictional bickering serves no purpose. Thus,

an important consideration of any CIR is identifying the review team. This manuscript will not make any recommendations as to how to assemble a review team other than to suggest that the team should be as objective as possible, incorporate both self-assessment, and third party assessment, and operate autonomously without political pressure from any of the involved agencies. Most importantly, the team should be comprised of individuals with leadership responsibilities who are capable of creating an environment of leadership and positive self-reflection.

The second CIR model involves ongoing information sharing among a broad group of stakeholders related to a particular event or a series of events. There is a long and well-established parochial tradition in the public safety community whereby organizations and individuals within organizations are generally not inclined to share information or draw in a cross-section of stakeholders to assist in individual investigations that might fall outside of their individual jurisdiction (Dawes, Birkland, Tayi, & Schneider, 2004). In fact, it is not uncommon to find that there is little information sharing between individual units within larger police departments that investigate shared problems. For example, an outside observer might be amazed to learn in larger, more complex police departments, it is rare for a homicide detective to collaborate with a narcotics detective when working homicide cases involving drug dealers. Moreover, it is equally as likely that agencies operating in close proximity share very little intelligence as it relates to particular investigations even when they share a common "client" base.

Incident specific CIRs are being used increasingly more by police departments around the nation as coordinated strategies for solving specific cases. They represent one of the more innovative strategies for sharing information on specific crimes, usually homicide or similarly serious crimes, in local criminal justice communities. The purpose of the reviews is to assist localities solve individual crimes and enhance local or regional responses to crime in general (Klofas et. al, 2006). While this type of CIR is not new per se, a more formalized and deliberative strategy for information sharing has emerged in communities across the nation participating in the federally funded Project Safe Neighborhoods initiative (*see* www.psn.gov).

In the most straightforward example, CIRs involve on-going meetings with a group of key stakeholders organized around information sharing. The identified stakeholders often come from a wide range of organizations, but in the typical example, the inclusion of particular

representatives is tied directly to their capacity to provide direct assistance in the investigation. Participants often involve representatives from federal law enforcement agencies, state agencies (e.g., state police, Department of Corrections, and Parole), and other county or local agencies (e.g., Probation and other local police departments). Those organizing CIRs are also encouraged to consider selecting participants from different specializations within individual agencies. Individuals, for example, may be selected from different investigative units (e.g., Vice, homicide, and narcotics), from different levels of an organization (e.g., patrol), and those with highly specialized expertise (e.g., ballistic experts).

While this description of stakeholders represents a model fostering communication and information sharing within an organization or small network of agencies, the basic model is one of scale and scope. Thus, it can be extended to a variety of problems and situations. The review process itself takes on many different forms. In the end, the primary purpose is for the stakeholders to bring as much tangible intelligence to the table about individuals involved in events, specifics of locations, and to generally draw a connection between what appears to be disparate facts.

> "It is in that combination of professionals with different training and experience that the potential of incident review is found. [ ] The goal of the incident review is for a group of experts to combine two different sets of knowledge and skills…so that the result is an understanding of the crime problem that supports the development of a strategic plan to help prevent those types of crimes" (Klofas et al., 2006, 4).

The most effective solutions to interoperability and information sharing have, and will continue to, come from well informed and crafted CIRs of both types outlined above.

Memorandums of Understanding

A Memorandum of Understanding (MOU) is a formalized inter-jurisdictional agreement to share resources. Generally, speaking if multiple agencies identify the need to pool funds for regional equipment needs, for example air support, an MOU is drawn up identifying the personnel and budgetary obligations of the contributing agencies. MOUs have also been used quit effectively in inter-agency agreements to share data. They can be one of the most straight

forward and simplistic strategies for starting a formal partnership between two or more agencies. Most importantly, MOUs establish the protocols for the relationship and establishes a clear understanding of the mutual expectations.

MOU's can be an effective starting point for developing shared information and communication systems. At the state or regional level, MOUs may serve as a starting point for drawing consensus around a strategic vision for communication systems that help guide the technology investment decisions among stakeholder agencies moving forward. Developing MOUs in the absence of tactical emergencies and/or impending funding creates a better opportunity create agreements that are both mutually beneficial but also more likely to achieve their intended goals. This type of pre-crisis and pre-funding planning is generally more deliberative and creates a better framework if and when resource investments are made. Access to resources sometimes emerges quickly, possibly caused by a failed system or new grant opportunity. These situations often require quick action to develop requirements documents, identify vendors, and select technology. Those responsible for performing these functions may lack specific expertise in these areas. Absent a plan that articulates shared values and established standards, it is likely that new systems will fail to meet the desired level of interoperability.

Joint Terrorism Task Forces

The first Joint Terrorism Task Force (JTTF) was established in New York City in 1980. Currently there are 100 cities nationwide that maintain a JTTF. Sixty-five of these JTTFs were established as a direct response to the national terrorism threat following 9/11. A JTTF is a small cell "… of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies."[ii] The JTTFs were created to address short comings in information flow between local state and federal agencies, and to give regional support to domestic intelligence gathering requirements.

One of the advantages of the JTTF approach is the use of local, and state law enforcement entities to provide regional snapshots of domestic terrorist activity that can be further synchronized at a national level. JTTFs utilize local, state, and federal law enforcement personnel that, in all likelihood, already have a working relationship based on other regional crime issues. In addition, JTTFs provide a structure that can be effectively applied to collect

intelligence and combat other forms of complex criminal activity (often identified as peripheral to terrorist activity) to include organized crime, narcotics, and murder. The JTTF model creates an infrastructure for coordinated, collective action and information sharing.

JTTFs represent an excellent opportunity to develop shared agreements about information sharing protocols, demonstrate the need and value of information sharing that helps break down institutional barriers against information sharing, and pilot what works within the context of the current system. JTTF are generally more proactive and less reactive, and thus, are better positioned to pilot technologies and to build the business case that justifies their need. The individual cases or threats addressed by the JTTF then create the real-life opportunities to model shared information and communication systems. Just as importantly, there is often the possibility that resources might be available to pilot emerging technologies on a smaller scale.

Fusion Centers

As a means to synthesize and analyze data coming from JTTFs and other regional sources, several states have established fusion centers. These fusion centers act as command and control centers to handle and disseminate information and intelligence on a state or multi-state level. Fusion Centers are staffed by agency representatives from a variety of regional law enforcement and emergency service agencies.

The FBI participates in the information-sharing environment (IEO) fostered by state fusion centers by assigning Field Intelligence Group (FIG) analysts and agents to leading regional fusion centers as provided by the Intelligence Reform and Terrorism Prevention Act of 2004. To assess the need for FBI involvement in a state fusion center,

> The field office SAC assesses the maturity of the fusion center by asking the following questions:
>
> 1. Does it have a facility and connectivity to local systems?
> 2. Will multiple agencies commit full-time personnel?
> 3. Is the fusion center attempting to meet the Global Justice Guidelines?
> 4. Does the fusion center cover a significant region or metropolitan area?

> If the fusion center meets the aforementioned criteria, then the FBI participation is mandatory. If the fusion centers are not mature enough to warrant full-time FBI personnel assignment, the SAC is directed to establish an effective and robust connectivity allowing for effective two-way exchange of intelligence.[iii]

The primary role of FBI personnel in a JTTF and/or fusion center environment is to:

> 1. Establish a gateway/connectivity between the FBI and the federal, state, local, and tribal partners across all investigative programs.
>
> 2. Provide an effective two-way flow of information through the intelligence cycle (e.g., requirements, taskings, intelligence, and feedback) between the fusion center and the FBI.
>
> 3. Participate as an investigative/analytic partner in uncovering, understanding, reporting, and responding to threats.
>
> 4. Ensure the timely two-way flow of terrorism-related threat information between the fusion center and the local JTTF and FIG.
>
> All terrorism information and intelligence generated from the fusion center/FIG relationship will continue to be directed to the JTTFs. The JTTFs remain the recognized and designated environment for which federal to local operational partnerships take place to detect, investigate, and disrupt terrorist threats or pursue perpetrators.[iv]

In many ways, Fusion Centers represent the perfect laboratories to model and pilot data and radio communication technologies. Fusion Centers are specifically mandated to draw data from disparate data sources and to rationalize their meaning. To accomplish this, there is a need for enhanced technologies to facilitate this, but also for building the individual and organizational relationships that make it happen. These relationships often do not develop naturally. Moreover, it is not uncommon for antagonism to exist that discourages such

coordination. Historical turf battles or personality disputes within and between agencies are powerful impediments against information sharing and shared technology visions.

Information Sharing in Action: FBI's ViCAP Program

In the early 1980's the FBI realized that "linkage blindness"[v] was an underlying impediment to the successful resolution of serial murder cases in general. It was further determined that a means to collect, collate, and disseminate case data on homicides and rapes that appeared to be serial in nature would potentially increase case solvability by linking agencies and providing cross-jurisdictional leads. Thus, the FBI's Violent Criminal Apprehension Program (ViCAP) was created as a central repository for murder, rape, missing person, and unidentified human remains cases from across the United States.

In its earliest form, ViCAP existed as a standalone system operating out of the basement of the FBI Academy in Quantico, Virginia. Cases were submitted in a hard copy format to data entry clerks who would hand enter cases, and if appropriate, search the database for similar types of cases based on *modus operandi*. Soon it became apparent that local agencies could expedite the entry of cases into ViCAP by entering their own cases into a local agency stand-alone copy of ViCAP and then sending them, first by floppy disk and then, as technology allowed, via email, to the ViCAP Unit. These cases were then uploaded into the national database. At the time, the national database existed on servers within the ViCAP Unit and the national database was searchable only by ViCAP analysts.

Web-based technology has made sharing the ViCAP national database with local, state and federal agencies technologically feasible. Therefore, ViCAP changed from an internal FBI database to a truly interoperable database that can be shared with all submitting agencies. By early fall, 2008, the ViCAP system became a web-based database operating through the Law Enforcement Online (LEO) website.

The ViCAP national database is an example of how the collection, storage, and dissemination of data can be facilitated in an online environment. This move toward information sharing will result in a reduction of data entry by ViCAP analysts, and an increase in case submissions and inter-jurisdictional case-awareness by local, state, and federal agencies. Furthermore, this interoperability allows investigators and analysts from local, state, and federal

agencies to perform their own analysis using national data, and thereby identify other agencies that may be stakeholders in a particular series.

Like other models presented above, ViCAP represents an opportunity to develop the business case and technological capacity to share information among agencies. In many ways, ViCAP represents an integrated intelligence system that draws data elements from a variety of sources, identifies common characteristics, and creates linkages between events that otherwise appear distinct. The general inability of the public and private sectors to do this lies at the heart of the 9/11 Commission Report that detailed how those tragic events occurred even after multiple indicators were observed across the broad array of intelligence and law enforcement agencies. It was evident that agencies had long histories of organizational competition, and that few effective practices were in place. ViCAP and similar programs continue to represent promising strategies for modeling new approaches.

Other Data Sharing Strategies

An integral part of any interoperability paradigm is the idea that data must be shared with those who can contextualize it, analyze it, and then create investigative leads, actionable intelligence, and operational recommendations from it. Regardless of the data to be collected, the data requirements for intelligence gathering must be understood and established across those agencies participating in the effort. Similar formats, collection strategies and requirements for reliability, validity, timeliness, and accuracy should all be well established to facilitate ease of integration and analysis.

Often one of the greatest impediments to interoperability of data is the variation in underlying database structures utilized by different record management systems from different agencies. This issue alone is often one of the key justifications for a complete lack of information sharing. While it is not reasonable to expect all agencies to change their internal records system and data management to the same regional or national interoperability scheme, it is important to recognize that compatibility is important. Many agencies have invested hundreds of thousands, if not millions of dollars in a functional records management system that meets their needs. However, the ability to export this data or portions of this data, into a standard format that can be shared with other agencies is important to the concept of interoperability. Furthermore, this data extraction should be automated and pulled directly from the agencies

native records management system, so as not to necessitate duplication of entry (which can easily result in errors and wasted man hours). A history of investment in one type of technology or a given "system" may discourage movement to a different system even if the alternative is superior. Key policymakers might perceive that movement to new technologies after historical investment in others is a sign of failed leadership or squandered resources.

Future Practices in Interoperability

Interoperability and information sharing will continue to be key features of enhanced homeland security efforts in the coming decades. Communities will continue to be pushed to enhance interoperability and move toward seamless communication and information sharing. The federal government has helped to propel the interoperability concern to the forefront of public safety planning. The Department of Homeland Security, for example, has funded Interoperability Coordinator positions for many states across the nation in an effort to establish a single point of contact for voice-and-data based interoperability concerns. While many states are still in the infancy stage in terms of their progress toward large-scale interoperability, the groundwork continues to be laid.

One of the more interesting examples of cutting edge efforts directed at seamless information sharing and community is the Law Enforcement Online (www.leo.gov) system funded by the Federal Bureau of Investigations. As a digital networking site, LEO is an elastic system that permits approved users to create and manage secured digital discussion boards and intelligence sharing sites. Among other functionality, LEO also functions as a portal of sorts whereby authorized users can access to access a variety of national data sources such as a JTTF site, Function Center data, or other national databases. Authorized users, for example, may not only be granted access to the ViCAP system but can allow users investigating cases thought to be linked to form integrated discussion groups. There are numerous examples of threads dedicated to ongoing major case investigations where personnel who are currently working on the case can post information, maps, diagrams, photos or anything else that needs to be shared with the community of stake-holders in the investigation. This represents a true paradigm shift in how multi-jurisdictional investigations are managed. Moreover, it represents a first of its kind virtual public safety community.

It will be imperative for public and private sector public safety entities to continue progress that has begun in recent years. Experience suggests, however, that the most substantial hurdles that will have to be overcome are less about technical capacities than about the cultural impediments that can threaten even the most well-funded effort.

References

Arlington County (2002). *After-action report on the response to the September 11 terrorist attack on the Pentagon*. Arlington, VA: Titan Systems Corporation.

Bitto, J. (2007). Sending out an S.O.S.: Public safety communications interoperability as a collective action problem. *Federal Communications Law Journal, 59*(3), 457-492.

Careless, J. (2006, October). Interoperability progress, five years after 9/11. *Law and Order Magazine*.

Dawes, S. S., Birkland, T., Tayi, G. K., & Schneider, C. A. (2004). *Information, technology, and coordination: Lessons from the World Trade Center Response*. Albany, NY: University at Albany, SUNY.

Department of Homeland Security (2005). *Fact sheet: Key priorities update March 1, 2004-March 1, 2005*. Washington, DC: Department of Homeland Security.

McKay, J. (2010, December 15). Interoperability is a cultural problem. *Emergency Management.*

---

[i] *See* http://www.safecomprogram.gov/NR/rdonlyres/127FFF18-100D-4405-AA40-076B79F17B1B/0/interopbooklet.pdf.

[ii] http://www.fbi.gov/page2/dec04/jttf120114.htm

[iii] Michael C. Mines, Deputy Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation, *Statement Before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*, September 27, 2007. http://www.fbi.gov/congress/congress07/mines092707.htm

[iv] … http://www.fbi.gov/congress/congress07/mines092707.htm

[v] A term used to describe the tendency for agencies to be unaware of similar murders occurring in other jurisdictions.