IBM Center for
The Business of Government

Using Technology Series

Mitigating Risks in the Application of Cloud Computing in Law Enforcement

Paul Wormeli
IJIS Institute

Using Technology Series 2012

Mitigating Risks in the Application of Cloud Computing in Law Enforcement

Paul Wormeli
Executive Director Emeritus
IJIS Institute

IBM Center for
The Business of Government

Table of Contents

Foreword


Daniel J. Chenok


George E. Cruser

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, *Mitigating Risks in the Application of Cloud Computing in Law Enforcement,* by Paul Wormeli, Executive Director Emeritus, IJIS Institute.

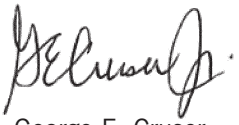
This report comes at an opportune time as the law enforcement community is undergoing a major transformation. Traditionally, communication within law enforcement was often linear and hierarchical. Today, communication happens in real time across jurisdictional boundaries. Because of improved communication and real-time information, the law enforcement community can plan where to place resources *ahead* of time, instead of only reacting to events after they have occurred.

One potential key to this is the advent of cloud computing. Cloud computing can be a cost-effective way to enable improved communication. Cloud computing also provides a potential for cost-savings for law enforcement, since law enforcement organizations don't have to use their tight budgets to build their own information technology infrastructure. According to Steve Ambrosini, executive director of IJIS, there has been a constant search for "emerging and disruptive technology that might positively affect the productivity and efficiency of justice and public safety agencies, and promote better information-sharing in support of their missions." Ambrosini continues, "Cloud computing has been one of the technologies with potential, but executives in justice and public safety have some general skepticism for concepts embedded in this powerful new infrastructure."

Based on a survey of leaders in the law enforcement community about cloud computing, Wormeli gained an increased understanding of their major issues, which include concerns about reliability and availability, performance requirements, cost of migration, and the recovery of data. In response to these concerns, Wormeli explains how the law enforcement community can effectively respond. The report concludes with six recommendations on how law enforcement organizations can successfully implement a move to cloud computing.

We hope that this timely report will be read carefully by law enforcement officials as they weigh the pros and cons of moving to cloud computing. We also hope that the report is useful to other public managers at the federal, state, and local level who are also assessing a move to the cloud.

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com



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

Understanding Cloud Computing

Overview

With the rapid worldwide growth in Internet use, major companies engaged in Internet commerce sought a more economical way to provide computing support. They adopted the concept of massively parallel computing, where hundreds or even thousands of thin "slices" of computers could be linked together to do a common task. They were able to take advantage of software evolutions that allowed many users to share the common infrastructure of large data centers using this technology. This new approach resulted in major performance improvements, greatly reduced costs, and the flexibility of instantaneous shifting of resources to tasks as needed.

As the data centers were built out for the purposes of supporting search engines and online sales, the companies found that they had built a massive capability accompanied by a virtual ease of shifting resources. Having achieved great cost reductions and built large capacities, they realized they could sell excess capacity to other companies and the government, as well as to individual consumers, and make more profits from such transactions—and that, by balancing the load across many users, the same physical resources could serve many customers.

As the major data center operators began to sell this capacity, other companies and government agencies found significant cost savings in this approach. The customer's contract with the data center operators provided the computing power and, in some cases, the software needed by the customer organization to save the cost of local hardware and software. Since the customers of this new service were contracting to use any of the data centers connected to the Internet without having to know the physical location of the data center, this service became known as computing in the cloud—or, simply, cloud computing.

This new capability led to the creation of new forms of service. Companies invented new ways to use cloud computing to sell what became known as Software as a Service (SaaS). In this model, companies ran the software at data centers in the cloud and made remote access over a browser sufficient to perform needed functions. Other forms of cloud computing were introduced which made just the infrastructure available for organizations to buy rather than build their own data center and have to handle the associated maintenance and support functions.

In the commercial world, cloud computing was successfully deployed rather quickly to serve many companies in a variety of configurations. Major software and service companies also rapidly expanded the offering of cloud computing to the public and soon began offering free storage and document management. One benefit of cloud computing that helped drive its success was that by storing data in the cloud, companies and individuals were creating a continuity-of-operations plan in the event their local system crashed.

One of the most powerful forces leading toward increased use of the cloud computing model has been accelerated consumer adoption. Consumers rely on cloud computing for such functions

Why this Topic Matters

Since its inception, the IJIS Institute has been attentive to emerging and disruptive technology that might positively affect the productivity and efficiency of justice and public safety agencies, and promote better information-sharing in support of their missions. Cloud computing has been one of the technologies with potential, but executives in justice and public safety have some general skepticism for the concepts embedded in this powerful new infrastructure approach. Some of the more rational skepticism is well-founded, and stories of implementation problems are always present in the introductory stages of any new technology.

Our intention in further studying this topic was to reach out to law enforcement executives and attempt to uncover the specific concerns they might have about the use of cloud computing, particularly for mission-critical applications such as computer-aided dispatching and records management. We are aware that some states, cities, and counties have begun to take advantage of the cloud computing model for more administrative functions such as e-mail, but the adoption of cloud technologies for mission-critical applications has moved much more slowly.

The premise for the study was that if the concerns could be identified, then the expertise and knowledge of senior technologists in our member companies could be applied in order to:

- Help the justice and public safety community better understand the strengths and limitations of this new technology
- Provide answers to some of the questions that remain impediments to further progress in the use of this technology

The survey we conducted in the course of this study has illuminated some of the concerns, and our technologists have provided advice and counsel on ways to mitigate the risks associated with implementing cloud computing technology.

This project and the survey was overseen by a Committee of twelve leaders in the law enforcement community. The IJIS Institute is grateful to the Committee members who contributed their time and guidance for the purpose of making this as useful as possible to the law enforcement and justice community. We appreciate their input, and sage advice on the methodology and in the assessment of the findings. A full list of the Committee is presented in Appendix II.

Law enforcement entities, including The IJIS Institute, will continue to examine this issue as there are sure to be many new developments, such as reduced costs, improved performance, and new ways to apply cloud computing to the missions of the agencies we serve. We remain committed to exploring the ways such innovative technologies can serve justice and public safety agencies to apply the power of information to serve our communities.

Steve Ambrosini
Executive Director
The IJIS Institute

as backing up data (i.e., music and photos), for e-mail, and for a host of other services, many powered via smartphones. In fact, it is not uncommon for individuals to use several different cloud computing services for personal purposes.

Such applications are, of course, of considerable interest to public safety agencies in general and to other government organizations as well. The perceived vulnerability of the Internet and the potential lack of control in the idea of remotely storing data without knowing its physical and logical location resulted in the fairly rapid evolution of the concept of the private cloud. A

private cloud uses the exact same technology for providing the service, but is generally owned by a particular user or provider with strict and certain constraints regarding access and control; for example, a network containing highly sensitive market or banking data that a few companies or government agencies want to protect from broader disclosure would be a candidate for a private cloud.

A similar concept is sometimes referred to as a community cloud, where a cloud infrastructure is deployed to serve a set of customers who share a particular mission. The community cloud is a particularly attractive service model for law enforcement agencies.

> In March 2011, Avanade commissioned a survey of 573 C-level executives, business unit leaders, and IT decision-makers in 18 countries to learn how technology, particularly cloud computing, is being used in the enterprise. According to the survey, 74 percent of enterprises are using some form of cloud services.[1]

Significantly, the Avanade survey (mostly of larger companies) found a preference for private clouds. "Previously, companies relied on third-party public cloud providers for the majority of their cloud infrastructure. Yet today, nearly half of all companies (43 percent) report they utilize private clouds. Further, another 34 percent say they will begin to do so in the next 12 months."[2]

There is still confusion in the marketplace about what cloud computing truly is. Some maintain that whenever an offsite server runs a software application over the Internet, it is cloud computing; but the definition of cloud computing widely believed to be the most accurate and meaningful indicates that this assumption is not the way the professionals see it. According to the National Institute for Standards and Technology (NIST), whose definition seems to be the most widely accepted, cloud computing has to incorporate the idea of sharing resources among multiple users in a virtual environment where the resources can be quickly reallocated to meet varying workloads and scaled to meet higher demand without reconfiguring a system.[3]

Scalability and flexibility are the key descriptors and virtues of cloud computing that go beyond conventional centralized servers as we know them from client server architectures. NIST describes five essential characteristics of what we have come to call cloud computing (slightly edited below):

1. **On-demand self-service.** A consumer can unilaterally and automatically call up any amount of computing capabilities, such as server time and network storage, as needed, without requiring human interaction with the service provider. No delayed reconfiguration is required to take advantage of this capability.
2. **Broad network access.** The cloud computing services are available over the Internet using nothing more than any device with an IP address working on all devices connected to the network (e.g., mobile phones, tablets, laptops, and workstations).
3. **Resource pooling.** The computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customers generally have no control or knowledge over the exact location of the

1. Avanade Global Survey: Has Cloud Computing Matured? June 2011.
http://www.avanade.com/Documents/Research%20and%20Insights/FY11_Cloud_Exec_Summary.pdf
2. Ibid.
3. NIST's description available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

provided resources, but they may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.

4. **Rapid elasticity.** The computing capabilities can be easily increased or decreased to meet the actual demand for service. To the consumer, the computing capabilities appear to be unlimited and can be appropriated in any quantity at any time.

5. **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

> A "**global cloud-computing market** that will grow at an annual clip of about **30 percent a year**, reaching **$270 billion in 2020.**"[4]
>
> Market Media Watch

Because of this capability, providers can charge for usage of resources by the hour and provide only what is needed to meet the demand. The growth rate in the market for cloud computing is staggering. A Bloomberg report cites a prediction that there is a "global cloud-computing market that will grow at an annual clip of about 30 percent a year, reaching $270 billion in 2020," according to Market Research Media Ltd.

Benefits of Cloud Computing

The first question most law enforcement executives have with respect to cloud computing is the same one any commercial manager would have: What is the value proposition here? Before engaging this new technology, there must be a clear understanding of its value to the agency.

There are clear benefits of cloud computing that have stimulated its growth in the commercial sector and can deliver the same outcomes for law enforcement. The following is a general statement of the potential benefits of using this technology in either commercial or government operations. These benefits would also have potential appeal in law enforcement agencies, although there are some limitations incurred due to current acquisition strategies. An insightful explanation of cloud computing's benefits to government is presented by Thom Rubel of IDC Government Insights in his paper, *Cloud Computing in Government: The Case and Considerations.*[5]

Benefit One: Operations Cost Reduction

In a services model where equipment and software are provided by a third party, so that only PCs equipped with a browser are needed to provide the IT functionality, the agency eliminates:

- The costs of the server and its maintenance
- The investment in software licenses for the operating and supporting software needed on the server and on the PC

4. http://www.marketresearchmedia.com/?p=839
5. Available at http://www.cisco.com/web/strategy/docs/gov/IDC_cloud_computing_wp.pdf

- Maintenance costs for the software
- The cost of staff resources to keep the server and associated software running

Cloud computing is a generally pay-as-you-go model that can be a price per hour for the software and the computing resources used.

Benefit Two: Service Availability

For public cloud providers, a new and much higher standard of availability has been one of the hallmarks of cloud computing. The data centers constructed for the purpose of providing cloud computers have built-in redundancy and environmental controls seldom possible in law enforcement or general government computer centers. The track record for up-time in cloud computing is significantly higher than for enterprise computing accomplished at the local level.

Benefit Three: Scalability

The most notable feature of cloud computing is the ability to scale resources to meet demand. In a scenario of a major event, such as a terrorist attack, when the need for computing resources may skyrocket, the cloud is ready to handle this kind of load variation. Within minutes, additional sources can be prioritized to the most urgent tasks. It is possible to think about a tenfold increase in computing time available in an emergency, while lowering the cost during non-emergency times.

Benefit Four: Increased Security

The cloud computing data centers offer a level of physical security far beyond that of most government data centers, with greatly locked-down operations. These systems are also much more secure against hackers and other interventionists than local systems tend to be. This is not to say that local systems are insecure, as they can be protected well by the right combination of software and other defenses, but they seldom are as well-engineered and protected as cloud computing centers.

Benefit Five: Ensured Continuity of Operations

Support for staying in operation in the course of natural or man-made disasters is made easier by cloud computing resources that are typically located far from the specific operator. If Louisiana parishes had been using cloud computing prior to Hurricane Katrina, it is likely that service could have been available as soon as power was restored.

Benefit Six: Utility Model Pricing

Rather than investing upfront in equipment and software, users are often sold cloud computing on a pay-as-you-go basis, with hourly charges for the use of the computing resources. There are significant cost savings to be realized by buying only the computing power needed during normal times and then being able to acquire more power as necessary. The idea of renting only what is necessary for as long as it is necessary is a model that has precedent in many other fields and is not a totally new phenomenon in IT; however, it is this approach to pricing cloud services that makes for the attractive ongoing cost savings that cloud providers attempt to deliver.

Implications of Cloud Computing for Law Enforcement

Government applications of commercial technology often lag behind the technology's introduction in the commercial world; but in this case, it did not take long for government to realize the potential of cloud computing. In February 2011, former federal government Chief Information Officer Vivek Kundra announced the *Federal Cloud Computing Strategy,* in which he declared that:

> "To harness the benefits of cloud computing, we have instituted a Cloud First policy. This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments."[6]

State chief information officers (CIOs) also saw the potential for saving considerable costs and began to explore applications, particularly following the concept of private data centers. The National Association of State CIOs (NASCIO) reported from its survey of CIOs in 2010 that "50% of states are considering using cloud computing."[7]

One of the key financial impacts that makes cloud computing—predominantly the public cloud—so attractive is the principle of pay-as-you-go for services at the heart of cloud computing offerings. Some organizations have found that their total computing resource costs can be cut in half by this approach. Savings that law enforcement can get enthused about include avoiding costs for the acquisition of servers, software, ongoing maintenance, and personnel for central system support.

> Just to provide a rough idea of the pricing, it is possible to pay a total of two cents per hour for a small server in the cloud. Amazon Glacier provides customers with data storage beginning at $0.01 per gigabyte per month, and charges for only the space that is used.[8]

Budgeting for Cloud Computing

Conversely, the value of this feature to law enforcement fundamentally challenges the way law enforcement agencies budget for services. In almost every instance, cities and counties make annual budgets for information technology, and agencies must stay within those budgets. Acquisition of new systems is normally done through capital funds projects. The idea of only

6. Kundra, Vivek, Federal Cloud Computing strategy, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf
7. 2010 State CIO Survey—Perspectives and Trends from State Government IT Leaders is available at www.nascio.org/publications and www.techamerica.org/2010-state-cio-survey.
8. Amazon Glacier pricing is available at http://aws.amazon.com/glacier/pricing/

paying for what you need has a very significant potential for saving actual dollars, but it requires a model that is much more like dealing with snow removal costs: An agency can budget a nominal amount to be expected as a matter of normal operations, but must be able to increase the funds available in the event of the kind of emergency or other situation that requires the allocation of additional computing resources.

It is this approach of only paying for the computing services you need that most directly distinguishes the true cloud computing model from the existing technology of hosted or shared systems. Law enforcement agencies and other public safety and justice agencies have shared central computing resources using various models for cost-sharing, such as paying a percentage of the budget based on number of users, population, or other metrics. The leap forward in cloud computing, with its measured services, allows the provider to bill each using agency for various services by the hour. This is very different from the current practices of:

- Several agencies using the same computer-aided dispatch (CAD) software and server with a consolidated dispatch center
- A law enforcement agency covering some portion of the cost of a shared server in the city
- A statewide system serving multiple user agencies

Hosted systems do not offer the ability to reallocate or scale resources in accordance with demand as a cloud computing provider can do with the appropriate architecture.

The pay-as-you-go or as-you-need model is attractive, but it is also sometimes tricky to negotiate. Since cloud providers typically unbundle pricing (e.g., for storage, CPU time, access time), it is possible to experience unanticipated, runaway costs if the usage is not properly managed.

A more common practice for early cloud computing adaptors seems to be a fixed monthly cost per user that is paid out of operating budgets rather than with large capital expenditures. An example of a current cloud-based offering following this model is the product offered by Datamaxx that provides full NCIC and Nlets access over a cloud-based network that fully complies with FBI CJIS Security requirements with 24x7 technical support at a cost of $10 per user per month.[9]

Cloud Computing and Administrative Functions

Law enforcement executives are concerned about another important part of the approach to cloud computing: whether the nature of the selected applications is appropriately provided by cloud computing. The initial applications that have been implemented or proposed for government purposes have mostly been associated with what are sometimes called administrative functions. It is fairly common for government agencies to explore and in some cases implement the use of cloud computing for such applications as e-mail and document storage and retrieval. Companies have continued to expand offerings for cloud-based e-mail, word processing, and other office automation functions. These functions are web-based applications requiring only a browser to operate.

Law enforcement has been slow to adopt the use of cloud computing. As part of city or county operations, law enforcement agencies have seen their e-mail and document creation and storage migrate to the web and to a cloud computing model only because the whole of a city or county is making such a change.

9. Datamaxx Contract with the State of South Carolina, reported by Kay Stephenson, CEO of Datamaxx.

Some agencies, sometimes driven by central government approaches, will turn to cloud computing for administrative functions such as personnel management, training, customer relations, and vehicle maintenance, just to name a few. In cases where very high application availability in support of a direct mission is not a requirement, using cloud computing—even public cloud computing—makes economic and policy sense.

There are a host of cloud computing-based applications that are useful to law enforcement and either supplement or enhance on-premise information technology applications. A good example is the robust offering of a cloud computing-based geographic information system from Esri.[10] BAIR Analytics has implemented a regional crime analysis system that provides a cloud-based analytical tool for data visualization that agencies can use at no cost to share incident data across geographical boundaries and with the public.[11] TASER International has added a cloud-based service of creating and maintaining a digital evidence locker originally designed as a place to store and manage (with full chain of evidence management) the video files resulting from officers wearing miniature video cameras.[12] SST offers its ShotSpotter Flex capability as a cloud-based service—in this case, using the Intrado Next Generation 9-1-1 (NG9-1-1) conformant cloud services to provide a subscription-based service of the ShotSpotter capabilities.[13]

Cloud Computing and Mission-Critical Functions

The use of cloud computing for mission-critical IT functions in law enforcement is not well developed. There are only a few agencies at the time of this writing that claim to be using cloud computing for such critical functions as access to state and federal crime databases, CAD, records management systems (RMS), or intelligence systems. Some of the subsystems that support these mission-critical purposes do operate in a web mode, and some of the actual applications have been built to use Internet technology, including browser-based operations, but these applications tend to be run on servers controlled by and on the premises of the police department or communications center. In some cases, the servers running these critical systems are part of the city or county data center, but even this remote placement has caused problems over the years.

Supporting systems, such as geographic information systems (GIS), are available today in the public cloud and can be used in support of mission-critical functions such as CAD and RMS. One of the possible models for the deployment of cloud computing is often called the hybrid mode, where some of the core functionality remains on local servers but the cloud is used for supporting functions and as a backup for data storage and disaster recovery.

There is also a growing acceptance of the concept of using multiple clouds to ensure recoverability of data in the event of a problem with any given cloud services provider. There are now cloud provisioning software packages that can handle the use of multiple clouds for these purposes, and this approach reduces the concern about there being a single point of failure in the cloud.

From the perspective of law enforcement, there are very significant differences and perceived risks between the public, private, community, and hybrid models of cloud computing. Fundamental concerns about the lack of control of applications running under the public cloud

10. http://www.esri.com/technology-topics/cloud-gis/arcgis-and-the-cloud
11. http://bairanalytics.com/raidsonline/
12. http://www.taser.com/products/digital-evidence-management/evidence
13. http://urgentcomm.com/psap/briefs/shotspotter-intrado-cloud-service-20111004/

are lessened by the adoption of the private cloud restrictions, and are even further mitigated by a hybrid model.

If the commercial model holds true in the law enforcement world, then it is reasonable to expect that the largest agencies might be attracted to the construction of their own private cloud, while smaller agencies are more likely to eventually embrace the public cloud model unless coalitions of agencies combine to create their own private or community clouds.

It is important to note that there is often an assumption that cloud computing is something for only large agencies to pursue. Actually, the greatest benefits may come to smaller agencies. The smaller the agency, the greater the percentage of potential benefit. Given the reality that smaller agencies cannot often afford to acquire and maintain their own computer system for law enforcement purposes, the concept of cloud computing—predominantly, the community model—tends to be quite attractive.

In this study, the focus was on the fundamental concept of cloud computing as a whole, and not particularly on one form of service or another, nor distinctly on specific models for implementation. Regardless of the model chosen, there are concerns that law enforcement executives have about computing in the cloud that will have to be faced in order for the IT companies that offer these services to be successful in designing and implementing cloud-based solutions; the intent of this study is to identify these concerns and then to address ways to resolve them in the course of adoption of this technology.

Concerns about Implementing Cloud Computing In Law Enforcement

Based on anecdotal input received by the IJIS Institute from law enforcement practitioners, there is some degree of apprehension on the part of law enforcement (and justice) officials regarding the use of cloud computing, particularly with respect to mission-critical applications. To lend some credibility to this hypothesis, the IJIS Institute asked the practitioner community for its views on this topic. This effort was not intended to be a statistically significant survey of all of law enforcement. Rather, it was done as a way to start obtaining information from law enforcement and public safety officials about their specific cloud computing concerns in the hopes of identifying impediments to widespread acceptance that may have to be resolved.

While the response in numbers was somewhat disappointing, the data presented in Appendix I were subjected to further validation with a set of attendees at a cloud computing workshop held at the 2012 IJIS Institute Summer Industry Briefing, with selected IJIS Institute committee members, and with the project advisory committee listed in the *Acknowledgements* for this report. There was agreement among all participants with the findings and recommendations given in the report. Further, the narrative submitted in open text form in the survey of executives supporting our coming to some fairly clear conclusions about the way law enforcement and communications executives viewed the impediments to the adoption of cloud computing.

> Reviewing the answers to the survey questions and the narrative supplied by 137 respondents, if this group is representative, we would conclude that about 80 percent of law enforcement officials are concerned about whether cloud computing is appropriate for mission-critical applications. This calculation is the average of responses across CAD, RMS, CJIS, intelligence, and other systems. (See the graph in response to question 2 on the survey responses in Appendix 1, page 30.)

More executives in the survey were apprehensive about the use of cloud computing for CAD than for RMS or other mission-critical applications. From this survey, it appears agencies perceive that either state law or FBI policy prohibits them from using cloud computing for these applications. Further, these agencies would not move forward until these issues are resolved.

Overview of Issues

The specific concerns that law enforcement executives have about using cloud computing for mission-critical applications such as CAD and RMS can be summarized as follows:

- **Issue One:** Using the Internet and remote computing resources for mission-critical applications carries a risk that **unauthorized individuals** can degrade or abscond with sensitive law enforcement data; or that access to privileged, sensitive, or classified data, including criminal history information, might then undermine operations, derail productive investigations, subject the public and officers to greater risk, and benefit the interests of criminals and criminal enterprises.

- **Issue Two:** There are concerns about the reliability of the Internet, and about the use of remote computing resources, resulting in a view that cloud computing may not provide the **availability** required for mission-critical applications—particularly CAD systems.
- **Issue Three:** The use of cloud computing services may not be able to match the **performance requirements** for mission-critical systems—particularly CAD—which require sub-second response under all load conditions. Further, the performance available is a function of workloads not under the control of the agency that owns the data and is, therefore, not consistent.
- **Issue Four:** The **cost of migration** to cloud computing, including equipment, software, data migration, and training, is a concern, and funds may not be available for this investment.
- **Issue Five:** There are risks associated with the remote storage of data in installations that may be damaged, destroyed, seized, bankrupt, or otherwise no longer accessible; and the **recovery of data** under such circumstances is a prime concern.
- **Issue Six:** Companies selling services that rely on the public cloud with **unqualified sharing of resources** among users cannot and will not comply with Federal Bureau of Investigation Criminal Justice Information Services (FBI CJIS) rules for the management control of law enforcement systems.

Several respondents declare that their current software provider (particularly for CAD or RMS) does not yet provide a cloud computing solution but, if they were to do so and it met the FBI CJIS security requirements as discussed above, then the agency would be willing to consider moving to cloud computing.

Responding to User Concerns

There is a mounting body of evidence that the use of cloud computing in some form and for some functions is inevitable in law enforcement information technology. The sanguine police executive will do the due diligence to find out what the issues are and to research what the resolution of those issues is in order to gracefully move into this new age. The issues uncovered in the IJIS Institute survey of police executives are suggested as a starting point, and we postulate that the resolution of these issues is required to clear the path toward the innovative use of cloud computing in law enforcement.

Therefore, we discuss the issues previously described and provide specific guidance on how to deal with each issue and resolve it in order to consider some level of implementation of cloud computing in law enforcement agencies.

Issue One: Risk of Unauthorized Individuals

Issue

Using the Internet and remote computing resources for mission-critical applications carries a risk that unauthorized individuals can degrade or abscond with sensitive law enforcement data including criminal history information.

This is a legitimate concern for all potential users of cloud or even remote computing services. The use of distributed resources does indeed increase the risk of penetration of systems and expose the system more than centralized resources do. The range of threats includes the intentional and unintentional exposure of data to inappropriate use.[14]

14. A good summary of the threats along with guidance for threat mitigation is provided in the Cloud Security Alliance "Top Threats to Cloud Computing" Version 1.0 (2010) https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

The origins of this perception—that when computing resources use the Internet there is an increased danger of data loss or abuse—stems from the easy access everyone throughout the world has to the Internet. There is no doubt that there is a threat; however, the extent to which it is a show-stopping feature has to be evaluated on the basis of what can be done to mitigate the risk.

Response to Issue

Commercial public cloud and private cloud providers have made extremely strong provisions against hacking into their data centers. Many of the examples of data being stolen or hacked come from the storage of the data on personal computers that were lost, stolen, or left behind. The commercial world has the same concerns about security as the law enforcement world. In the June 2012 *Information Week 2012 Cloud Security and Risk Survey*—a survey of 268 business technology professionals using, planning to use, or considering public cloud services—*Information Week* reports that 55% of the potential customers shared this exact concern (Davis, 2012).

Cloud computing infrastructure is, in nearly every respect, more secure than its premise-based equivalent. An Aberdeen Group study states:

> "Compared to companies using on premise web security solutions, users of cloud-based web security solutions had 58% fewer malware incidents over the last 12 months, 93% fewer audit deficiencies, 45% less security-related downtime, and 45% fewer incidents of data loss or data exposure."[15]

Since their inception, online service providers have been exposed to the open Internet, and have consequently learned to be far more diligent in application of best practices for security. Note, for example, that misconfiguration incidents are 12 times more common for on-premise systems. Misconfiguration is the online equivalent of leaving a car unlocked with the keys in the ignition. Either security options are not turned on, or default user IDs and passwords are left unchanged (e.g., 'admin' / 'admin').

In the law enforcement world, networks that have the potential of adopting cloud technologies and architectures such that they truly become private clouds have already adopted some of the recommended best practices to control access and authorization, such as:

- Data encryption at rest and in motion
- Redundant data storage and availability
- Two-factor authentication
- Global Federated Identity and Privilege Management (GFIPM) specifications

Adoption of these practices should be in the specifications issued for the procurement of cloud services wherever there is a potential for sensitive data to be included. If this course of action is followed, then it is likely that the cloud services provider can create a defensive, in-depth approach to security that exceeds what most law enforcement agencies could or would do on their own. There is no particular reason why cloud services should be any less secure than centralized enterprise systems if the proper analysis and provisioning of security are implemented.

15. "Web Security in the Cloud: More Secure! Compliant! Less Expensive!" Derek Brink, Aberdeen Group, May 2010, http://goo.gl/XZeDI

Additional Resources

You can learn more about the best practices from such sources as the Cloud Security Alliance (CSA),[16] a relatively new organization that gives cloud providers a place to describe and validate their security protections so customers can determine the level of protection afforded by their cloud offerings. The CSA also posts a set of best practices for cloud computing in such areas as encryption and applications security. The CSA includes a Security, Trust, and Assurance registry, which is a free source of cloud provider self-documentation on its practices.

Another source for solid advice on the protection of data in cloud computing is Safegov.org. According to its website:

"SafeGov.org is a forum for IT providers and leading industry experts dedicated to promoting trusted and responsible cloud computing solutions for the public sector. By fostering a more comprehensive understanding of cloud technologies, including their benefits, capabilities and limitations, SafeGov.org works to empower government users to make well-informed procurement choices from the growing universe of marketplace offerings."

Issue Two: Reliability and Availability

Issue

There are concerns about reliability of the Internet, and about the use of remote computing resources, resulting in a view that cloud computing may not provide the availability required for mission-critical applications—particularly CAD systems.

It is not surprising that the application with the most concerns for potential deployment in the cloud is the CAD system. The likely reason for this concern is the issue of availability. As a system that deals with the life and death of the citizen to whom responders are called, CAD being unavailable has perhaps the most serious consequences of any IT failure in law enforcement.

For on-premise CAD systems, the rule of thumb for years has been to insist on an availability of five nines: 99.999%. Availability is a matter of determining how much the system can be inoperable. The five nines measure means that the system can only be inoperable 5.26 minutes per year. It is generally understood that adding each 9 to the percentage of uptime approximately doubles the cost of the system. To get to the five nines in most CAD environments, agencies require the supplier to provide a system that is fully redundant, with no single point of failure in the combination of hardware, software, and network.

Availability is normally a component of the Service Level Agreement (SLA) that is negotiated with the supplier. Procuring a system directly from a CAD service provider or a system integrator usually implies negotiating an SLA that incorporates the five nines measure for CAD.

Most agencies in law enforcement accept a lower level of availability for the RMS function. Many RFPs do not even specify availability for the RMS or, if they do, it is given to be in the range of 99.9%—three nines instead of five—which is about 8.76 hours per year (10 minutes per month). To achieve this level of availability does not require the same level of redundancy that the five nines for CAD imply.

Most CAD procurements in medium to larger cities and counties require fully redundant systems, with no single point of failure, so that the five nines number can be realized.

16. https://cloudsecurityalliance.org/

Response to Issue

Companies that provide cloud computing services are well aware of the need to offer high availability, and their practices do lead to such high availability, including redundancy, for the data centers normally used in providing these services. With the carefully defined availability commitments in an SLA, the cloud provider will be able to produce the necessary availability. The availability offered by most professional cloud providers is much higher than is normally computed for stand-alone enterprise servers, particularly where a small number of servers and disks constitute the production configuration of the enterprise system.

The weak point in this scenario is generally the connection to the network itself. Having a redundant way to connect, such as access to both wired and wireless service, is the best protection to ensure the availability that is needed.

For CAD systems in particular, a reasonable way to achieve the five nines' level of availability is to provision multiple clouds to achieve the same kind of redundancy that would be achieved in a fully redundant on-premise system. With this capability, the availability requirements can be met in a cloud environment.

Additional Resources

There is more information about the concept of brokering services for cloud computing in a Forbes article by Kevin L. Jackson, titled "Cloud Management Broker: The Next Wave in Cloud Computing."[17]

Issue Three: Ability to Match Performance Requirements

Issue

The use of cloud computing services may not be able to match the performance requirements for mission-critical systems—particularly CAD—which require sub-second response under all load conditions. Further, the performance available is a function of workloads not under the control of the agency that owns the data and is, therefore, not consistent.

Performance and availability are two of the key concerns that law enforcement executives—and commercial executives as well—have about cloud computing. The primary way that organizations approach the need to insist on both availability and performance is to create an SLA that specifies both. In the case of performance, we typically express this requirement as response time. For decades, the RFPs for CAD systems have called for sub-second response times. This requirement is not nearly so ubiquitous in RMS procurements, where something in the order of two seconds is generally deemed sufficient.

Performance in the cloud is dependent on many factors:

- The extent to which the application is distributed between the local workstation and the remote server farm
- The bandwidth consistency provided by the Internet provider
- The capacity of hardware at the user end
- The software application itself

17. http://www.forbes.com/sites/kevinjackson/2012/08/12/cloud-management-broker-the-next-wave-in-cloud-computing/

Response to Issue

The more experienced CAD software companies are well aware of the requirement that the performance of their software in a client/server mode must produce the requisite sub-second response times.

Cloud computing should be able to offer consistent sub-second response time for operation of a CAD system, provided there is high availability and sufficient bandwidth and performance engineering work is performed to ensure expectations are met. There is no doubt that the number of customers using a particular cloud solution will influence response time, but the whole premise of cloud computing is the ability to provision additional resources on demand so the agreed-upon service levels can be met.

The majority of the transactions in CAD systems are incident initiation, status changes, and short messages, and it is crucial for participants in the response to be aware of these state changes as soon as possible; however, the idea that CAD cannot run in the cloud presumes that every transaction must make a round trip to a central server before it is shared with other nearby users. This is not the case for CAD systems built on modern messaging architectures. CAD workstations and servers are peers in networks that ensure reliable asynchronous message delivery. State changes and messages can be exchanged by locally interconnected workstations even when network connectivity is lost.

CAD applications are already optimized to support the distributed operation. Many, if not most, larger dispatch environments support telecommunicators and dispatchers in multiple locations, often interconnected by networks with nominal quality-of-service. Also, critical message transmission between dispatchers and responding units depends on wireless networks, a much more severe bottleneck than access to an optimized cloud-resident server.

The load balancing and elasticity of cloud computing enable cloud providers to offer quality of service guarantees. In general, applications designed to scale to support many users in a cloud environment are far less sensitive to capacity-related performance fluctuations than are premise based apps which are not adapted to massively parallel environments. Most premise-based systems are sensitive to non-transactional workload, such as report processing and backups, because they do not provision multiple servers for non-core functions for economic reasons; whereas cloud service providers maintain high performance virtualized environments that enable dynamic resource allocation.

One of the ways in which performance under cloud computing conditions can be made more consistent is to contract for a dedicated resource set to provide for specific purposes. This approach does offer the economic advantage of pay-as-you-go computing but it does provide for a way to meet constant expectations without a concern for the number of customers sharing a cloud.

A number of researchers have addressed the issue of high performance cloud computing, mainly for scientific computing purposes, and the research has contributed to the knowledge about how to ensure consistent high performance for such mission-critical applications as CAD. Generally, the measures taken for these compute-intensive purposes lead to the use of extreme redundancy and, thus, higher costs.

The concern over performance in the cloud has led to the development of performance monitors directly addressing this issue, and a number of companies provide such monitoring software to test and measure performance and alert system managers to any reduction in performance.

Additional Resources

Paul Burns has posted a useful 9-minute podcast on monitoring cloud performance and availability where he discusses a tool for comparing response time and availability for major public cloud providers. The podcast is posted on his blog at http://www.neovise.com/podcast-cloud-performance-availability-monitoring.

Issue Four: Cost of Migration

Issue

The cost of migration to cloud computing, including equipment, software, data migration, and training, is a concern, and funds may not be available for this investment.

The availability of funding is obviously a serious issue and concern, and there is no doubt that some costs will be incurred as an agency moves to a cloud computing model. Evaluating this course of action clearly and unequivocally requires an evaluation of Return on Investment (ROI) and a business case for making such a move. Costs are obviously dependent on where the agency is in its provision of information technology—agencies without IT will spend more to move to this world than will those with well-established capabilities—however, the costs for moving from an existing system are relatively minor, and may be a lot less than the initial supposition. Initial acquisition costs are far less, as most cloud concepts are based on what amounts to a rental of service, including software, rather than an acquisition. The hardware required will consist of the personal computers used for access and the networking hardware to connect to the Internet. Data conversion is always a problem in moving to a new system but, if the move is to the cloud offering of the current CAD/RMS provider, then there is a good likelihood conversion cost will be either zero or minimalized.

Response to Issue

There is a tendency to lose detail in the excitement about the potential of cost savings in cloud computing (Carr, 2011). In particular, the cost of moving a large amount of data from a dedicated file structure on a single server to the cloud storage capabilities may be significant. Getting quotes for all the elements of a conversion is critical to the analysis of an ROI for making this move. Agencies should generally take a 10-year view of the cost model to determine the actual comparison of costs for cloud computing vs. on-site resources. Further, the combination of ongoing maintenance, support, and personnel costs should be compared in the ROI evaluation over this period, as should the acquisition costs for the alternative methods. Mark Fetherolf, chief technology officer of Interact, estimates that in moving applications to cloud computing, "the life cycle cost savings that are possible for a single agency approach 70%."

The experiences of other agencies at the federal level, as well as the state and local levels, is that, once the full analysis is done, there will emerge a distinctive cost savings and a positive ROI from moving to the cloud.

Additional Resources

CIO Magazine has an article on 8 ways to measure the ROI for Cloud Computing, available at http://www.cio.com/article/595179/8_Ways_to_Measure_Cloud_ROI. A white paper on calculating the ROI from cloud computing is also available at http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx.

Issue Five: Recovery of Data

Issue

There are risks associated with the remote storage of data in installations that may be damaged, destroyed, seized, bankrupt, or otherwise no longer accessible; and, the recovery of data under such circumstances is a prime concern.

This is a very legitimate concern. There is a distinct risk associated with cloud computing of losing data in such instances. The way to deal with this concern is to determine ways to mitigate the risk.

Response to Issue

Protecting against the primary causes of data loss that might be incurred during a natural disaster or even an attack on a data center is the objective of geographically separated, secure, duplicate, redundant computing services. Commercial cloud service providers know very well what has to be done to maintain continuity of operations under just about any known conditions, and the cloud computing designer should take these provisions into account in building and providing the services. Disaster recovery from such events as hurricanes, tornadoes, earthquakes, and other severe weather is a design principle built into cloud services. As noted earlier, many organizations, both commercial and government, seek out cloud computing services simply to provide effective disaster recovery.

Loss of data under conditions where the provider goes out of business, goes bankrupt, has its assets seized, or incurs some other kind of financial trauma leading to the data being unavailable should probably be a greater concern than the basic disaster recovery. Fortunately, there is an effective mitigation of this risk: using multiple cloud services and requiring data recovery methods that are non-proprietary. With these methods, copies of the data can be stored in multiple services, giving as much recovery as desired to the organization.

Managing multiple cloud services is now made easier by a number of new software and process services that amount to cloud computing brokers, with software to automate the splitting of load and duplication of data storage in ways to minimize the potential loss of data from any single source.

Additional Resources

Cloud services providers are fast becoming aware of customer requirements to deal with this issue. Stephanie Overby of *CIO Magazine* has published a helpful article—titled "Hostage Crisis in the Cloud: Can You Rescue Your Data?"—with advice on how to deal with this issue.[18]

Issue Six: Compliance with FBI CJIS Rules

Issue

Companies selling services that rely on the public cloud with unqualified sharing of resources among users cannot and will not comply with FBI CJIS rules for the management control of law enforcement systems.

Response to Issue

This issue embodies a misperception probably introduced by press reports about the failure of

18. http://www.cio.com/article/705806/Hostage_Crisis_in_the_Cloud_Can_You_Rescue_Your_Data_?page=1&taxonomyId=3195

the City of Los Angeles to include the police department in its efforts to move e-mail and other applications to a public cloud provided by Google. The excuse for not including the police department was that Google did not or would not comply with certain of the FBI CJIS security requirements; however, FBI CJIS rules for the management control of local law enforcement systems do not apply to e-mail or document storage mechanisms that do not contain Criminal Justice Information (CJI) provided by the FBI CJIS.[19]

From a review of the statements made after this issue was resolved by terminating the police portion of the city contract, it appears that the cloud provider was not informed in advance that there was a requirement for satisfying FBI CJIS security requirements. It also appears that there was no initial understanding of the need for compliance being connected to the potential interaction between local systems and the FBI CJIS network. The result was that the provider did not consider making services compliant with FBI regulations and was not therefore prepared to do so.

In response to an inquiry arising from the LAPD incident, the FBI provided a clear statement of its policy related to cloud computing as described in *The CJIS Security Policy as it Relates to Cloud Computing* on page 24.

It may be true that the major cloud services companies that have worldwide distribution centers would have difficulty meeting the FBI requirements or would choose not to do so to maximize the efficiency of their cloud offerings over the largest number of customers worldwide. Even the larger cloud service providers, however, have been exploring or offering the availability of government-oriented cloud services that constrain the locations to U.S. sites and may consider adhering to the full conditions that the FBI requires to accredit their participation in providing law enforcement services.

Theoretically speaking, the FBI CJIS rules only apply to systems that contain CJI derived from the FBI CJIS, so it is possible that a standalone CAD or RMS would not have to conform to the CJIS rules; however, the better CAD and RMS systems already have incorporated a seamless interface to provide, for example, a consolidated reply to a single query about a name, vehicle, etc. Even if a system initially is not connected to the FBI CJIS WAN, it would be reasonable to expect further movement toward this more ideal context; and, therefore, it would be prudent to enter into agreements only with providers who are able to meet the CJIS requirements.

There is no reason that smaller companies focused on the law enforcement market cannot provide cloud computing services totally in accord with CJIS rules. In fact, in reporting on the issue, Jeff Gould, chief executive officer of IT consulting firm Peerstone Research, and a founder of SafeGov.org, cited InterAct Public Safety, Datamaxx, and Vertical Computer Services as cloud companies that use secure data centers staffed by people who have undergone the requisite FBI background checks (Vijayan, 2012). Other companies are also offering to provide cloud services. For example, Tiburon advertises a partnership with Intrado to provide application services over their private cloud infrastructure.

Cloud providers recognize the requirements of the law enforcement community and community cloud infrastructure and applications are growing rapidly. Amazon Web Services GovCloud is accessible only within the U.S. and supports FIPS 140-2 compliant endpoints. NIets provides cloud hosting services for a number of secure online law enforcement applications. Intrado, InterAct, and other public safety software and service providers offer secure community cloud

19. Federal Bureau of Investigation, Criminal justice Information Services (CJIS) Security Policy, Version 5.1, July 13, 2010.

The CJIS Security Policy as it Relates to Cloud Computing

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing—or using the Internet to maintain data and applications—is often considered as a business solution. But, when the security of information and transactions must be maintained, as it must be with access to the FBI's Criminal Justice Information Services (CJIS) systems, additional issues arise. Can a law enforcement entity maintain the security mandated by the CJIS Security Policy while taking advantage of modern cloud technology? Because the CJIS Security Policy is a cloud-compatible policy, the answer is yes—but that yes is dependent on the vendor of the cloud technology being able to meet the requirements of the policy.

Who created and implements the CJIS Security Policy?

The CJIS Security Policy is not a policy created by the FBI. Rather, it was created by the law enforcement community as an information-sharing security policy. It was developed by a task force of law enforcement IT and security subject matter experts over a two-year period. It was fully vetted and approved by the CJIS Advisory Policy Board (whose members provide guidance to the FBI and represent local, state, tribal, and federal criminal justice agencies in the United States and Canada) and the Compact Council (which disseminates rules and procedures for noncriminal justice access to criminal history information to help assess suitability of individuals for positions of trust). The CJIS Security Policy documents the minimum security standards the criminal justice and noncriminal justice communities require to securely share their information nationally.

Can an Agency be Compliant with CJIS Security Policy and also Cloud Compute?

As mentioned, the CJIS Security Policy is a cloud-compatible policy; however, the requirements may be tough for some vendors to meet. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personal identity information (PII) will be protected when shared with other law enforcement agencies across the nation. Some of the requirements that may be challenging for a cloud-computing vendor to reach are:

1. Identifying the list of their system/database/security/network administrators who have the capability to access and recompile criminal justice information.
2. Prohibiting the performance of remote maintenance from locations outside the United States.
3. Requiring fingerprint-based background checks on their system/database/security/ network administrators who have the capability to access and recompile criminal justice information.

Admittedly, these requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, these requirements aren't new to vendors serving the criminal justice community and many vendors have successfully met these requirements for years.

The FBI remains committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted.

hosted applications for the public safety industry that meet or exceed FBI CJIS security requirements.

It has been reported that some states are reluctant to work with cloud computing providers, citing the need for FBI certification or state statute provisions on data residing out of state. Agencies seeking to explore the use of cloud computing will need to determine any limitations imposed by their state control terminal agency regarding access to state or federal data.

Implementation Recommendations

While it is likely that cloud computing will evolve to be a very useful new form of providing information technology services to law enforcement, it is also a complicated and in some ways more sophisticated way to make technology available. The end user may experience little difference in the move from on-premise computing to cloud computing, but many important issues suggest a different approach to acquisition and ongoing use of these new technologies. Any agency that is interested in taking advantage of cloud computing should consider the following recommendations.

Recommendation One: Look first to determine if the existing software provider is or will be offering a true cloud computing option. This reasonable course of action should minimize the costs of conversion including data migration.
As companies who have a track record for offering mission-critical software products and services migrate to cloud computing, they will acquire the deep technical and operational knowledge about how to best utilize the cloud environment for their products. This is not an easy task, and it will take their acquisition of technical talent familiar with the cloud business and technical models. Once they make this move, their customers will find that they have to provide the knowledge of cloud computing that will help make the transition successful, and this should minimize the cost of taking this step forward.

Recommendation Two: Investigate the interests of other agencies in forming a community cloud computing environment that will provide service to a significant number of agencies of all size.
Some of the traditional service providers in the law enforcement industry, such as Datamaxx and Interact, have basically followed what amounts to a community cloud computing model, in which they have configured a cloud solution in partnership with other companies in order to deliver a cloud solution reserved for law enforcement agencies. This kind of solution directly ties the service provider to the agency, and provides more accountability for the service than an independent search for a cloud computing provider would. There are not yet many examples of the community cloud approach in law enforcement; however, this model seems more acceptable and it is likely that agencies, and perhaps states, may explore this option.

Recommendation Three: The agency should study and prepare its own requirements for service level agreements (SLA) covering guarantees (with penalties) of availability and performance for each application to be included.
For any agency directly negotiating with a cloud service provider, rather than going through a system integrator or the software provider, a careful construction of a service level agreement requires research and identification of the acceptable range of service on a host of parameters

that should define the service. There are templates[20] available on the Internet to help identify the topics that should be considered in forming an SLA. The SLA should define the objectives as well as the measures of performance and the penalties associated with a failure to meet the provisions defined.

Recommendation Four: Test candidate cloud providers to determine that availability and performance levels guaranteed are being met before and after the implementation of the service.

Companies that offer cloud computing services should be able to provide a full test of the performance of any given service. Availability can be estimated, but evidence of availability is best determined by references from other users. This kind of investigation is no different than an agency would normally pursue in selecting an on-premise turnkey solution for its information technology services and products, and such diligence should be pursued with any cloud computing acquisition with as much or more rigor.

Recommendation Five: Ensure that for mission-critical applications, such as CAD and RMS, the cloud provider is certified to meet *FBI CJIS Security Policy 5.0* requirements.

For any system that may incorporate criminal justice information extracted from the FBI CJIS that is subject to the security regulations and data protection accorded to such data, the provider must be able to guarantee compliance. Any RFP or other acquisition document should spell out compliance with the latest version of the requirements, which are available on the Internet and should be made clear to the service provider.

Contracts must also spell out compliance with these regulations. This conformance is particularly critical for CAD, RMS, NCIC access, intelligence, and any other systems that may have the need or capacity to acquire or store CJIS data. For systems that the agency wishes to acquire that may not meet the FBI standards, it is important to put in place policies to prohibit the acquisition, storage, and secondary dissemination of CJI through such systems.

Recommendation Six: Acknowledge that moving into this new realm is challenging and difficult. Agencies will be more likely to succeed if professional enterprise architects and engineers are used to design and orchestrate the introduction to this powerful new technology.

This is a critically important issue. This new field requires expertise not yet found in typical IT operations. The expertise in enterprise architecture, system design, and software design that will optimize an application in the cloud environment is crucial to long-term success. There are at least three ways to gain access to this expertise.

- First, if the existing software provider is managing the shift to cloud computing, the agency should confirm that the supplier does indeed have the necessary expertise.
- Second, an experienced system integrator or consulting firm that has such expertise may be employed to help review or design implementation and manage the construction of the SLA.
- Finally, larger agencies may want to either hire such expertise or train existing IT staff to fill this role before moving out with more than pilot projects or experiments.

Regardless of how such talent is acquired, the careful implementation design is a very important step in ensuring operational utility of cloud computing applications.

20. "SLAs in Cloud Systems: The Business Model." http://www.ijcst.com/vol31/3/yrabi.pdf

Many of the best practices from the well-known and proven System Development Life Cycle management processes are still very much applicable to implementation projects with cloud computing. Even though the end user may not see the work or the "back room" that runs the enterprise information system, the common rules of good design practice still apply.

Conclusions

Law enforcement executives are cautious when it comes to deploying mission-critical software applications under the banner of cloud computing. Many of their concerns raise legitimate issues which are now being addressed by the cloud and the criminal justice industry. There are risks associated with this new technology; however, there are many significant advantages to this new approach to provisioning information technology, and it is only prudent to explore ways to mitigate the identified risks. This report has attempted to identify the key risks and concerns, and then to discuss ways to resolve these concerns.

Cloud computing is a valuable and reasonable approach to operating law enforcement mission-critical applications.

The risks identified in this study and the research into the cloud computing field, on which much of this analysis is based, lead to the conclusion that cloud computing is a valuable and reasonable approach to operating law enforcement mission-critical applications in a cloud computing environment. While there are security issues that are unique to law enforcement in protecting information shared by the FBI through CJIS, there are companies that have been certified and others that will be certified as they move to offer this service to law enforcement. This requirement is not an obstacle to adoption of cloud computing.

It is likely that law enforcement executives will find more comfort in adopting cloud computing in what has been called the community model, where the use of the computing resource is shared with other law enforcement agencies. In more of a hybrid mode, where the public cloud may be used for supporting purposes (e.g. geographic information systems) the basic functions of CAD and RMS can be moved to the cloud, providing that certain precautions are taken in selecting providers and negotiating service level agreements that ensure the availability and performance of the service.

Appendix I: Survey Results

This survey was done to begin a process through which law enforcement and public safety officials could express their specific concerns about cloud computing in the hopes of identifying the impediments that may have to be resolved before there is widespread acceptance. In that sense, this was more of a call for views and opinions than a scientifically constructed survey sample. Even so, the response to this call for input was somewhat disappointing. In order to give the highest number of individuals a chance to have input, approximately 5,000 invitations were sent using a variety of different mailing lists. A total of 117 people began the survey; however, only 37 respondents fully completed all questions. The respondents identified themselves as mostly either law enforcement (67%) or communications (28%).

In spite of the relatively low response rate, a significant number of extended narrative responses were helpful in assessing the general attitude and acceptance of cloud computing among the respondents. The responses to the ranking questions, when combined with the narrative responses to the essay questions, provide what we believe to be an accurate perception of law enforcement attitudes regarding their readiness to move forward with cloud computing for mission-critical applications. Because of the relatively light response rate, the summary of findings was validated in discussions with a set of attendees at a cloud computing workshop held at the IJIS Institute summer briefing in 2012, with selected IJIS Institute committee members, and with the project advisory committee listed in the beginning of this report. There was agreement among all discussants with the findings and recommendations given in the report.

The components of the survey and the analysis of the responses are summarized below.

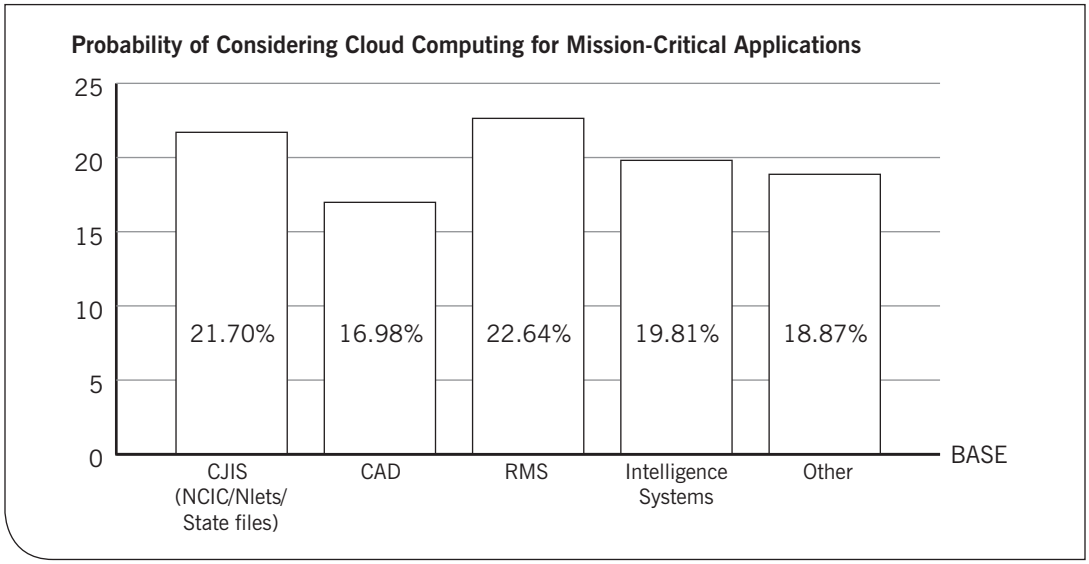
1. **Have you considered adopting, or have you adopted, cloud computing services for your agency for handling any of the following applications? Please answer 'Yes' or 'No' for each item.**

Of those responding:

- 20 percent have adopted or considered the deployment of CAD systems in the cloud
- 31 percent have adopted or considered cloud computing for RMS
- 28 percent have adopted or considered the deployment of intelligence systems in the cloud

2. Which applications do you think could be handled by cloud computing? (Select all that apply)

The general response to this question indicates that 80 percent of the respondents do not think mission-critical applications for law enforcement could be handled by cloud computing. Respondents are less likely to think that CAD systems can be delivered in the cloud rather than RMS. The distributions of the responses to this question are seen below:



3. Please rank the following reasons from 1 to 5 on how important they were in the decision to USE cloud computing in your agency, with '1' being the most important factor and '5' being the least important. If your organization decided NOT to use cloud computing, please skip to the next question.

In analyzing responses to this question it appears that the 37 individuals who fully responded to the survey answered this question as a hypothetical, not on the basis of actually having decided to use cloud computing. In summarizing the responses, the top three reasons for choosing this technology and the percent of respondents choosing this factor as the top priority are as follows:

- The lower cost to deploy a cloud solution vs. conventional systems (41%)
- Security available with cloud solutions (39%)
- Ability to conform to regulatory conditions of access and use (33%)

The least influential reasons for choosing to invest in cloud computing are any dissatisfaction with the current vendor or any issue of vendor lock-in.

4. Please rank the following reasons from 1 to 5 on how important they were in the decision NOT to use cloud computing in your agency (with '1' being the most important).

It appears that 37 respondents also answered this question in terms of their perceptions about why agencies might not want to use cloud computing. This response to this question is one of the clearest in revealing the general attitude that prevents agencies from considering cloud computing in law enforcement. The top reasons and the percentage of respondents that rated each the number one reason for not using cloud computing are as follows:

- Control over access and security of data (50%)
- Difficulty of complying with regulatory controls (39%)
- Potential performance issues with remote access (22%)

"CAD needs to be real time, all the time, regardless of the conditions."

The least significant impediments to cloud adoption are reported to be:

- The shortage of skills in the agency to manage IT implementations
- Dissatisfaction with vendor offerings/pricing
- The ability to cope with changes

In the questions asking respondents to elaborate on their reasons for rejecting cloud computing, the most common answers are somewhat specific to the application. Numerous respondents cite reliability and availability concerns, particularly for CAD systems, commenting that "CAD needs to be real time, all the time, regardless of the conditions." There is common concern about the Internet not being reliable enough to support CAD operations at the availability level (generally expected to be 99.999% of the time) that CAD performance must provide. Some respondents mentioned that CAD is mission-critical, while RMS is less so, and, therefore, might be eligible for cloud computing.

Privacy and security and access control (i.e., authentication and authorization) are major issues for respondents. Several respondents indicate that the potential for unauthorized access in data centers where personnel are not subjected to the kinds of rigorous background checks that law enforcement personnel are subjected to is a widespread concern.

An additional common concern voiced by some respondents is that, "We must own our data and if we decide to change vendors, or the company goes out of business, or the servers are seized, or damaged, etc., we will have a problem. We also want to be able to move to other software and having it in the cloud could make it hard for us to switch and bring our old data into the new system."

Some of the respondents also voice their belief that their current software provider of CAD and RMS applications does not offer a cloud option so they are not able to consider this potential. The implication of these comments is that there is a certain amount of loyalty to the existing software provider and the agency would only move to cloud computing if the current supplier were to offer cloud based solutions.

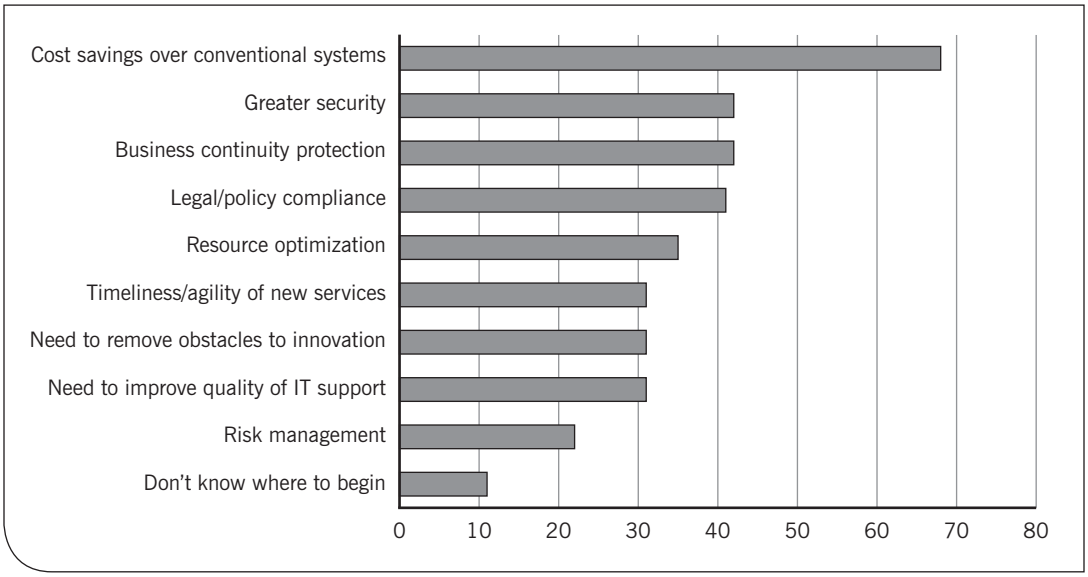
The survey asked respondents to identify technical, legal, and administrative issues that would have to be resolved before they would move forward with cloud computing, and there are a significant number of responses that highlight the following:

- Cost and approach to migration, including hardware, software, data migration
- Matching WAN performance with existing LAN performance, including network connection speed
- Ensuring availability and reliability of cloud resources
- Ensuring conformance with FBI CJIS 5.0 requirements and state law governing control of data

Some agencies believe that their state laws restrict their ability to use the public cloud in particular, given that data might reside in other states or countries.

5. If your organization uses a cloud computing environment, or if you are considering using cloud computing, please rank the following on their importance as factors in your decision, with '1' being the most important factor and '5' being the least important.

This question seeks to elicit understanding of the factors that are most important to the respondents in choosing or considering a cloud computing solutions. The list of factors proposed and the percentage of the 37 respondents weighting the factor as the most important are as follows:



6. Do you think that the FBI CJIS Security Policy 5.0 provides appropriate security levels to support the use of cloud computing for CJIS Services in your agency?

Of the 37 respondents that fully answered all questions in the survey, only 33 percent answer this question in the affirmative, while 55 percent simply do not know the answer, leaving the impression that considerably more education is called for about this issue. Several respondents also wrote that the FBI CJIS Security Policy 5.0 requirements prohibit use of the cloud (a position that the FBI has clearly criticized).

Appendix II: Cloud Computing Study Project Advisory Committee

The IJIS Institute is grateful to the Committee members who contributed their time and guidance for the purpose of making this as useful as possible to the law enforcement and justice community. We appreciate their input, and sage advice on the methodology and in the assessment of the findings.

Committee Member	Title	Organization
Tom M. Clarke, Ph.D	Vice President, Research and Technology	National Center for State Courts
Steve Correll	Executive Director	Nlets, The International Justice & Public Safety Network
Matthew D'Allessandro	Senior Business Development Manager, Integrated Command and Control Division	Motorola Solutions
Ron Hawley	Executive Director	SEARCH
Mike Lyons	Vice President of Operations	Tritech Software Systems
Harlin McEwen	Chairman, Communications and Technology Committee	International Association of Chiefs of Police
Ed Posey	Captain, Commander of the Police Operations Bureau	Gainesville, Florida Police Department
Eddie Reyes	Deputy Chief, Administrative Services Bureau	Alexandria, Virginia Police Department
David Roberts	Senior Program Manager, IACP Technology Center	International Association of Chiefs of Police
Alan Shark	Executive Director and CEO	Public Technology Institute
Kay Stephenson	President and CEO	Datamaxx, Inc.
Christopher Traver	Senior Program Analyst, Bureau of Justice Assistance	U.S. Department of Justice

Acknowledgements

The conduct of this study was a team effort, including key staff at the IJIS Institute—Martha Hill, Ashwini Jarral, Alice Jacobsen, and Chelsea Cooper—all making contributions to the data collection and other research that will determine the extent to which this study is useful to the law enforcement community.

A special thanks goes to those in the law enforcement community who took the time to complete the practitioner survey that was central to this study, and particularly those who made the extra effort to write down the perceptions and opinions that made this survey's results so valuable.

We also thank the companies that contributed ideas and best practices to help explain how the concerns that law enforcement executives raised about the introduction of cloud computing could be resolved.

The insights and advice on the methodology and interpretation of the survey results that were provided by the Cloud Computing Study Project Advisory Committee was invaluable. The Committee members are all knowledgeable participants in the larger law enforcement community and their contributions to the success of this report were invaluable.

We also thank the technologists in industry that helped discuss and respond to the concerns voiced in this report. In particular, Mark Fetherolf, Chief Technology Officer at InterAct Public Safety, provided specific data and references for this report. Kay Stephenson, CEO of Datamaxx, provided insights directly from their customers and developers.

Finally, this study could not have been possible without the direct financial support of the IBM Center for The Business of Government, IBM's focal point for "connecting public management research with practice." Since 1998, the Center has helped public sector executives improve the effectiveness of government with practical ideas and original thinking. The Center also sponsors independent research by top minds in academe and the non-profit sector, and creates opportunities for dialogue on a broad range of public management topics.

References

Anderson, J. (2012, February). The President's Budget: Making Cloud Computing a Priority for the Future. SafeGov. Retrieved from http://safegov.org/2012/2/16/the-president%E2%80%99s-budget-making-cloud-computing-a-priority-for-the-future

Benameur, S. P. (2010, December). Privacy, Security and Trust Issues Arising from Cloud Computing. HP Labs - Bristol, UK. Retrieved from http://salsahpc.indiana.edu/CloudCom2010/slides/PDF/Privacy,%20Security%20and%20Trust%20Issues%20Arising%20from%20Cloud%20Computing.pdf

Black, N. (2010, May). Law Enforcement: Security, Ethics and Cloud Computing. Firmex blog. Retrieved from http://www.firmex.com/blog/law-enforcementand-the-ethics-of-saas/

Bookman, S. (2012, January). State Dept., AG address EU Cloud Data Privacy Concerns. FierceTelecom. Retrieved from http://www.fiercetelecom.com/story/state-dept-ag-address-eu-cloud-data-privacy-concerns/2012-01-18

Boubez, D. T. (n.d.). Cloud Computing and Public Safety Services. InterAct. Retrieved from http://www.interact911.com/wp-content/uploads/overview/cloud-computing-public-safety.pdf

Braue, D. (2011, December). Hackers, Like Security Vendors, are Embracing the Cloud; Can You? CSO. Retrieved from http://www.cso.com.au/article/408956/hackers_like_security_vendors_embracing_cloud_can_/

Carr, D. (2011, April). What the Cloud Really Costs: Do You Know? CIO. Retrieved from http://www.cio.com/article/678418/What_the_Cloud_Really_Costs_Do_You_Know_?page=1&taxonomyId=3008

Chertoff, M. (2012, January). Can We Trust the Cloud to Protect Sensitive Law Enforcement Information? SafeGov. Retrieved from http://www.safegov.org/2012/1/18/can-we-trust-the-cloud-to-protect-sensitive-law-enforcement-information

Cleverley, M. (2012, March). Cloud Computing Offers a Public Safety Edge. *Law Officer.* Retrieved from http://www.lawofficer.com/cloud

Collier, D. (2012, February). Cloud Computing is a Viable Option for Law Enforcement. *Citizens Against Government Waste: The Swine Line.* Retrieved from http://swineline.org/?p=6285

Couillard, D. A. (2009). Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing. *Minnesota Law Review,* 93, p. 2205. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1832982

Davis, M. (2012, August). Don't Trust Cloud Security. *Information Week.* Retrieved from http://www.informationweek.com/global-cio/security/dont-trust-cloud-security/240005687

Fox, A. (2009, April). Cloud Computing, Law enforcement and Business Continuity. *Above the Clouds: A Berkeley View of Cloud Computing.* Retrieved from http://berkeleyclouds.blogspot.com/2009/04/cloud-computing-law-enforcement-and.html

Gantz, S. (2010, August). Major Cloud Computing Privacy Legal Issues Remain Unresolved. *Security Architecture.* Retrieved from http://blog.securityarchitecture.com/2010/08/major-cloud-computing-privacy-legal.html

Gourley, B. (2011, April). Cloud Computing for Law Enforcement. *Cloud Computing Journal.* Retrieved from http://cloudcomputing.sys-con.com/node/1810027

Greenfield, R. (2011, August). The Pros and Cons of the Federal Push Toward the Cloud. *The Atlantic Wire.* Retrieved from http://www.theatlanticwire.com/technology/2011/08/pros-and-cons-federal-push-toward-cloud/41537/

Hanson, W. (2012, February). Oakland County, Michigan, Taking Shared Services National. *Government Technology.* Retrieved from http://www.govtech.com/e-government/Oakland-County-Mich-Taking-Shared-Services-National.html?elq=b7336a32b73b4db7bd2057c45a94c959

Hanson, W. (2012, January). The Cloud Builders: Ann Arbor and Washtenaw County, Michigan. *Digital Communities.* Retrieved from http://www.digitalcommunities.com/articles/Lessons-Learned-Sharing-Technology-in-Michigan.html?elq=2dfa8b085b6740bca3d148927df86e24

Hanson, W. (2012, January). The Cloud Builders: City and County of El Paso, Texas. *Digital Communities.* Retrieved from http://www.digitalcommunities.com/articles/The-Cloud-Builders-El-Paso-City-and-County.html?elq=135209dc2fb14ae480d05a41f98cabbd

Hardy, Q. (2012, February). Taser's Latest Police Weapon: The Tiny Camera and the Cloud. *New York Times.* Retrieved from http://www.nytimes.com/2012/02/21/technology/tasers-latest-police-weapon-the-tiny-camera-and-the-cloud.html?_r=4

Heaton, B. (2012, May). IT Leaders, Security Concerns Slowing Federal Cloud Adoption. *Government Technology.* Retrieved from http://www.govtech.com/policy-management/IT-Leaders-Security-Concerns-Slowing-Federal-Cloud-Adoption.html

Homeland Security NewsWire. (2012, January). New Cloud Computing Based Disaster Management System. *Homeland Security NewsWire.* Retrieved from http://www.homelandsecuritynewswire.com/dr20120106-new-cloud-computing-based-disaster-management-system

Jackson, W. (2011, November). Cloud offers Feds Access to Police Data. *Government Computer News.* Retrieved from http://gcn.com/articles/2011/11/07/interior-pilots-police-data-cloud.aspx

Kerner, S. M. (2012, January). U.S. DOJ: The Cloud Provides No Legal Cover for Criminals. *eSecurity Planet.* Retrieved from http://www.esecurityplanet.com/network-security/u.s.-doj-the-cloud-provides-no-legal-cover-for-criminals.html

King, L. (2011, August). Police Planning Major Switchover to Cloud Computing. *ComputerWorld UK.* Retrieved from http://www.computerworlduk.com/news/public-sector/3295484/police-planning-major-switchover-to-cloud-computing/

Kundra, V. (2011, August). Tight Budget? Look to the 'Cloud'. *New York Times.* Retrieved from http://www.nytimes.com/2011/08/31/opinion/tight-budget-look-to-the-cloud.html?_r=1&src=me&ref=general

Lucus-McEwen, V. (2012, May). How Cloud Computing Can Benefit Disaster Response. *Emergency Management.* Retrieved from http://www.emergencymgmt.com/disaster/How-Cloud-Computing-Can-Benefit-Disaster-Response.html

Maltais, M. (2012, April). Google Drive: Watch out, Cloud Computing in U.S. like 'Wild West'. *Los Angeles Times.* Retrieved from http://articles.latimes.com/2012/apr/25/business/la-fi-tn-cloud-storage-legal-20120425

McCann, B. (2011, December). As Law Enforcement Moves to Cloud, Security Concerns Loom Large. *CivSource.* Retrieved from http://civsourceonline.com/2011/12/29/as-law-enforcement-moves-to-cloud-security-concerns-loom-large/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Civsource+%28CivSource%29

NASCIO. (2011). Capitals in the CloudsThe Case for Cloud Computing in State Government Part 11: Challenges and Opportunities to Get Your Data Right. Lexington: *NASCIO Online.* Retrieved from http://www.nascio.org/publications/documents/NASCIO_CloudComputing_PartII.pdf

Nestler, G. (2012, May). Cloud Computing Applications for Public Safety. *FireFighter Nation.* Retrieved from http://www.firefighternation.com/article/technology/cloud-computing-applications-public-safety

Niemann, B. (2011, October). Build The NIEM Information Exchange Clearinghouse In The Cloud. *AOL Government.* Retrieved from http://gov.aol.com/2011/10/31/build-the-niem-information-exchange-clearinghouse-in-the-cloud/

Olesker, A. (2011, April). Cloud Computing For Law Enforcement. *CTO Vision.* Retrieved from http://ctovision.com/2011/04/cloud-computing-for-law-enforcement/

Pardeep Kumar, V. K. (2011, May). Effective Ways of Secure, Private and Trusted Cloud Computing. *IJCSI International Journal of Computer Science Issues,* 8(3 .) Retrieved from http://arxiv.org/ftp/arxiv/papers/1111/1111.3165.pdf

Raths, D. (2012, January). Shared and Regional Services Are on the Rise. *Public CIO.* Retrieved from http://www.govtech.com/pcio/Shared-and-Regional-Services-Are-on-the-Rise.html?elq=f45df97b92d946d9ab11d15c97e0503c

Rice, J. (2012, March). Transforming Public Safety with Cloud Computing. Miscrosoft Worldwide Public Safety Symposium. Retrieved from http://mspublicsafetysymposium.com/media/7681/rice_0315_1610.pdf

Sarno, D. (2011, December). L.A. Won't Put LAPD on Google's Cloud-Based E-mail System. *Los Angeles Times.* Retrieved from http://articles.latimes.com/2011/dec/14/business/la-fi-google-e-mail-20111215

Tuutti, C. (2012, March). Cloud Conversation Shifting to New Concerns. *Federal Computer Week.* Retrieved from http://fcw.com/articles/2012/03/19/gsa-dave-mcclure-smart-cloud-computing.aspx?s=fcwdaily_200312

United States Government Accountability Office. (2011). Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives. Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. Retrieved from http://www.gao.gov/new.items/d12130t.pdf

Vijayan, J. (2012, February). FBI declares cloud vendors must meet CJIS security rules. *ComputerWorld.* Retrieved from http://www.computerworld.com/s/article/9224048/FBI_declares_cloud_vendors_must_meet_CJIS_security_rules

Walden, I. (2011). Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. Queen Mary School of Law Legal Studies. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067

Walker, M. B. (2012, January). NIST Issues Security, Privacy Guidance for Public Cloud. FierceGovernmentIT. Retrieved from http://www.fiercegovernmentit.com/story/nist-issues-security-privacy-guidance-public-cloud/2012-01-25?utm_medium=nl&utm_source=internal

Walker, M. B. (2012, February). NIST security controls update addresses privacy, mobile, cloud. *FierceGovernmentIT.* Retrieved from http://www.fiercegovernmentit.com/story/nist-security-controls-update-addresses-privacy-mobile-cloud/2012-02-29?utm_medium=nl&utm_source=internal

Williams, M. (2012, February). 5 Issues to Consider Before Deploying Cloud-Based E-mail for Law Enforcement. *Public CIO.* Retrieved from http://www.govtech.com/pcio/5-Issues-to-Consider-Before-Deploying-Cloud-Based-E-mail-for-Law-Enforcement-.html?elq=856f56cf097e43a1a9c78c5f7b0603bd

Williams, M. (2012, January). Utah Signs On With Google. *Government Technology.* Retrieved from http://www.govtech.com/policy-management/Utah-Signs-On-With-Google.html?elq=1845ca6b3e254dcf9bf2c4918c9d14ec

Yasin, R. (2011, November). Why agencies Need 'Cloud-Smart' Apps. *Government Computer News.* Retrieved from http://gcn.com/articles/2011/11/30/cloud-smart-applications.aspx?s=gcndaily_011211

Yasin, R. (2012, March). How Cloud can Improve Intel Community's Analyses. *Government Computer News.* Retrieved from http://gcn.com/articles/2012/03/13/intelligence-community-cloud-big-data-analysis.aspx?s=cloud_200312&admgarea=TC_CLOUD

Yasin, R. (2012, January). Montana Law Enforcement Shares Data via the Cloud. *Government Computer News.* Retrieved from http://gcn.com/articles/2012/01/19/montana-public-safety-secure-data-sharing.aspx?s=cloud_240112&admgarea=TC_CLOUD

Yasin, R. (2012, February). Moving Storage to the Cloud? Don't Forget about Security. *Government Computer News.* Retrieved from http://gcn.com/articles/2012/02/09/data-replication-amazon-cloud.aspx?s=gcndaily_100212

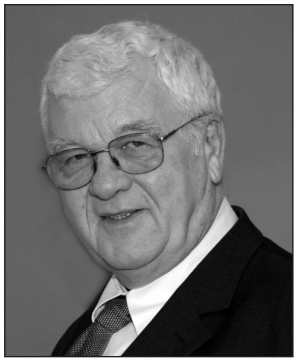
Yasin, R. (2012, November). NIST Releases 'Bible of Cloud Implementation'. *Government Computer News.* Retrieved from http://gcn.com/articles/2011/11/04/nist-cloud-tech-roadmap-impact.aspx?s=gcndaily_071111

Yasin, R. (2012, January). NIST Sets Security Approach for Cloud Computing. *Federal Computer Week.* Retrieved from http://fcw.com/articles/2012/01/26/nist-cloud-security-guidelines.aspx?s=cloud_310112&admgarea=TC_CLOUD

Yasin, R. (2012, January). NOAA, Pittsburgh Complete Switch to Google Apps. *Government Computer News.* Retrieved from http://gcn.com/articles/2012/01/04/noaa-city-of-pittsburgh-migrate-to-google-apps.aspx

Yasin, R. (2012, January). States Test Regional Cloud Hubs. *Government Computer News.* Retrieved from http://gcn.com/articles/2012/01/20/idc-report-regional-cloud-hubs.aspx?s=cloud_240112&admgarea=TC_CLOUD

About the Author



Paul Wormeli is Executive Director Emeritus of the Integrated Justice Information Systems Institute, a non-profit corporation formed to help state and local governments develop ways to share information among the disciplines engaged in homeland security, justice, and public safety. He has had a long career in the field of law enforcement and justice technology. He has been active in the development of software products, has managed system implementation for dozens of agencies throughout the world, and has managed national programs in support of law enforcement and criminal justice agencies.

Mr. Wormeli was the first National Project Director of Project SEARCH, and was subsequently appointed by the President as Deputy Administrator of the Law Enforcement Assistance Administration in the U.S. Department of Justice. Mr. Wormeli helped design the first mobile computing equipment sold in this county to law enforcement agencies. Mr. Wormeli managed the staff work and wrote much of the report for the Information Systems section in the report of the National Commission on Standards and Goals for Criminal Justice, which dealt with criminal justice information system standards. He was the project manager for the development of the first crime analysis handbook published by the National Institute of Justice. He has been an advisor to the White House on security and privacy, participated in the drafting of federal law on this topic, and was responsible for the development of numerous state plans to implement the federal and state laws on information system security and privacy. During his tenure at the Justice Department, he served on the President's Committee on Drug Enforcement. Mr. Wormeli is an author and lecturer on law enforcement and justice technology.

Mr. Wormeli was also the first Chairman of the Integrated Justice Information Systems Industry Working Group (IWG), a consortium of over 100 companies which was formed in 1999 at the request of the U.S. Department of Justice to help facilitate the implementation of integrated justice information systems throughout the nation. After the IJIS Institute was created as a non-profit follow-on to the IWG, he became the first full-time executive director of the IJIS Institute and served in this capacity until January, 2011, while the membership grew to

nearly 200 companies. In this capacity, he was the first Chairman of the NIEM Communications and Outreach Committee and was the first Chairman of the Executive Steering Committee of the Justice Training and Technical Assistance Committee, a consortium of service providers created by the U.S. Department of Justice to help to facilitate the implementation of new ways to share information. He has served on the technical advisory committee for the Harvard School of Government Innovator's Network program for law enforcement and justice, and on the NASCIO Information System Architecture Working Group. He is an associate member of IACP, the Police Executive Research Forum, and a corporate member of the Association of Public Safety Communications Officers.

In 2009, Mr. Wormeli was appointed to a three-year term on the Committee on Law and Justice (CLAJ) of the National Academy of Sciences. The CLAJ, established in 1975, was created to provide a more scientific understanding of issues pertaining to crime and justice, and its activities today include identifying new areas of research and participating in resolving scientific controversies.

In 2011, Mr. Wormeli was named by Government Technology magazine as one of the Top 25 Doers, Dreamers & Drivers in Public Sector Innovation in the U.S., one of "an eclectic group of individuals … who share a willingness to challenge convention and find new answers to long-standing issues."

At the 2011 Annual Conference of National Association for Justice Information Systems (NAJIS) Wormeli was presented the Kelly Bacon award for "Outstanding Service to the Justice Information Technology Community." The award, which is made periodically but not every year, recognizes individuals who, like Bacon (NAJIS's first president), have made long, sustained contributions to NAJIS and its mission to foster overall improvement of justice information systems nationwide.

Mr. Wormeli has been a founder of three companies in the law enforcement information systems field, providing computer-aided dispatch and police records management software applications to law enforcement agencies. Software developed and implemented by his companies has been used by hundreds of agencies throughout the U.S. and Australia.

Mr. Wormeli writes a blog called "The IJIS Factor" at http://www.ijis.org/EDblog/ which has been named by FedTech as one of the 50 "Must Read" blogs on federal information technology. He is a co-author of *CIO Leadership for Public Safety Communications: Emerging Trends and Practices,* Alan Shark, Ed., published by Public Technology Institute, August, 2012.

Mr. Wormeli holds a Bachelor of Science degree in Electronics Engineering from the University of New Mexico, and a Master of Engineering Administration degree from the George Washington University. He undertook courses in the honors program for industry as a part of the doctoral program in Engineering Economic Systems at Stanford University. He received a certificate in Cross-Boundary Transformation from the John F. Kennedy School of Government Executive Education program at Harvard University.

Key Contact Information

To Contact the Author:

Paul Wormeli
Executive Director Emeritus
IJIS Institute
44983 Knoll Square
Ashburn, VA 20147
(703) 726-3693
e-mail: paul.wormeli@ijis.org
website: www.ijis.org
blog: http://www.ijis.org/EDblog/

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

Recovery Act Transparency: Learning from States' Experience by Francisca M. Rojas
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

Collaboration Across Boundaries: Insights and Tips from Federal Senior Executives by Rosemary O'Leary and Catherine Gerard
Designing Open Projects: Lessons From Internet Pioneers by David Witzel

Conserving Energy and the Environment

Best Practices for Leading Sustainability Efforts by Jonathan M. Estes

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
Using Geographic Information Systems to Increase Citizen Engagement by Sukumar Ganapati

Improving Performance

The Costs of Budget Uncertainty: Analyzing the Impact of Late Appropriations by Philip G. Joyce
Five Methods for Measuring Unobserved Events: A Case Study of Federal Law Enforcement by John Whitley
Forging Governmental Change: Lessons from Transformations Led by Robert Gates of DOD and Francis Collins of NIH by W. Henry Lambright

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

Challenge.gov: Using Competitions and Awards to Spur Innovation by Kevin C. Desouza
Working the Network: A Manager's Guide for Using Twitter in Government by Ines Mergel

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:
Daniel J. Chenok
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

Stay connected with the IBM Center on:

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