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

Global Justice Information Sharing Initiative

Public Safety Primer on Cloud Technology

The world is increasingly digital and connected.

This trend provides tremendous opportunities and challenges for public safety. For example, body-worn and surveillance cameras, cell-phone multimedia, and social media generate a great deal of data. Today, the general public expects agencies to have the capability to quickly receive and leverage such data during major disasters, critical incidents, and criminal investigations. As such, many public safety entities have turned to cloud technology ("the cloud") to store and manage the data, increase capabilities, and reduce costs over time.

Global Justice Information Sharing Initiative October 2016

Introduction

The purpose of this resource is to educate the public safety community and provide answers to straightforward common questions public safety agencies may have regarding cloud technology, the services the cloud can provide, and guidance for considering contracts with cloud vendors. In addition, this resource provides a glossary of definitions for terms used throughout the document, as well as a list of recommended resources for further reading. It is intended to provide introductory guidance to agencies, not to be an exhaustive "how-to" guide.

This guidance is the result of a collaborative effort through the Global Justice Information Sharing Initiative (Global), which is supported by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Global acknowledges that this document does not address all subject areas of this complex topic; rather, it provides a strong understanding of cloud technology to help guide government leaders. Global is committed to educating law enforcement and public safety agencies on such matters.

The cloud is much like having extra computing power or a large hard drive in another place where data may be stored and/or processed.

Frequently Asked Questions

What is the Cloud?

The Federal Bureau of Investigation's (FBI's) Criminal Justice Information Services (CJIS)[1] defines the cloud as a model that provides on-demand access to a shared pool of computing resources. It is much like having extra computing power or a large hard drive in another place where data may be stored and/or processed. Through the cloud, data, images, video files, and more can be securely stored, processed, and analyzed in a fully managed remote environment.

Similar to an agency's server room where employees save files they create using software, the cloud is a storage space accessible through various means, such as computer or network software, a Web interface, etc.

While the cloud may be used simply as a place to store data, it also may be the location where software applications reside and process information. In either case, agencies retain all control and responsibility to manage such data in compliance with policy standards, such as 28 CFR Part 23.[2]

It is important to note that the cloud is more than one thing—it is many things. As shown in the following bulleted list, public safety agencies can "set the dial" to determine how much support it provides for a solution as opposed to the cloud provider.

- **Infrastructure as a Service (IaaS)—**This is the most basic use of the cloud. It provides access to servers in the cloud data center but requires an agency to provide the same kind of management as their own servers. It provides the most control but requires the most support by an agency. This model is similar to leasing a car and paying for the use of the car but still being responsible for tune-ups, tires, oil changes, etc.
- **Platform as a Service (PaaS)—**In this model, the cloud provider manages the platform and an agency only has to manage its own solutions. It requires less server management by an agency but also provides less control. This model is similar to renting a car and paying for use of the car but not being responsible for tune-ups, tires, oil changes, etc.
- **Software as a Service (SaaS)—**In this model, the cloud provider delivers both the platform and the solution running on it. Many people already use SaaS solutions for banking or online shopping, where the software and platform are both hosted in the cloud. This model is similar to hiring a taxi and the service of getting to a destination but not being involved in any way with the car's maintenance.

How is the cloud being used?

Cloud services are already commonplace, such as in online banking, Internet shopping, and social media. Many public safety agencies are starting to use cloud-based solutions for mission-critical functions, as well as for daily operations (e.g., e-mail). For example, many agencies may already be using the cloud for body-worn camera systems, data backup, and access to state and federal databases.

How might the cloud help public safety agencies?

Because of the rapid growth of generated data (e.g., digital evidence), agency heads have found themselves needing to consider the capabilities of the cloud environment to efficiently manage data in a cost-effective way. Cloud services can include scalable storage, analytical capabilities, and improved collaboration.

A. Storage

The fastest-growing type of data is digital. A greater variety and number of digital devices are available to more users, capturing information at a higher quality, creating ever-larger files, with longer retention periods. As an example, digital cameras create files that are six times larger today than just a few years ago. Cloud solutions can provide scalable, on-demand, and potentially infinite storage, beyond the capabilities and budgets of most agencies.

B. Analysis

In addition to storage, cloud solutions also can provide enhanced and on-demand analytic capabilities for agencies of any size. These may include crime mapping, coordination of emergency operations, link analysis, statistical assessment, auditing, resource deployment, etc. Such abilities can improve responsiveness, transparency, and public confidence.

C. Collaboration

The cloud environment can improve collaboration by enabling the sharing of work, the organization of assets, and the sharing of results across multiple platforms (e.g., social media, news outlets). Internally, cloud collaboration can mean sharing among agencies, disciplines, levels of government, and citizens (who may contribute to or request information, such as through a public records or Freedom of Information Act [FOIA] request).

D. Cost

Agencies with a significant IT budget and team may choose to manage more of their own on-premises technology infrastructure, but the rapid growth of digital evidence is leading agencies of all sizes to leverage the cloud in some way. Examples include “fail-to-cloud” data center back-up strategies, along with pay-as-you-go cloud resources that enable agencies to respond to unanticipated demand spikes without having to invest budgets and time in deploying additional IT hardware.

Using the cloud can change agency funding models from capital expense outlays to operation annuals. While the cloud may not always result in large upfront savings, it can result in more cumulative cost efficiency over time.

E. Emerging capabilities

The following are new and rapidly developing capabilities that leverage the power of the cloud and its on-demand service model, which can make these services available to more than just large departments.

- Automated video redaction
- Predictive analytics
- Facial detection
- Object and behavior recognition

Is agency information in the cloud secure?

Yes, provided that the public safety agency employs security best practices for use of the cloud similar to those implemented for an agency's local system—access control and a secure platform. Security is a critical factor for public safety agencies. The FBI, through its CJIS Security Policy,[3] has provided guidelines for departments that choose to use the cloud. Public safety agencies should require that any selected cloud solution be configured, deployed, and managed to meet the agency's security, privacy, and other requirements.[4] Agencies have found that the strict security policies implemented by some cloud providers have exceeded the policies in place for their own data centers.

A. Security Standards and Compliance

Many agencies are seeing value in ensuring that their cloud providers comply with the requirements established by governing bodies and standards-development organizations, in addition to the agencies' security policies. Public safety agencies should articulate this requirement within a service level agreement (SLA). These standards/requirements include, but are not limited to:

- *Guiding Principles on Cloud Computing in Law Enforcement*, International Association of Chiefs of Police (IACP)[5]
- *Criminal Justice Information Services (CJIS) Security Policy*, Federal Bureau of Investigation[6]
- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—Criminal Intelligence Systems Operating Policies.[7]
- Federal Risk and Authorization Management Program (FedRamp)[8]

  FedRamp is a governmentwide program that streamlines federal agencies' ability to make use of cloud vendor platforms and offerings and introduces an innovative policy approach to developing trusted relationships between federal agencies and cloud vendors. FedRamp is mandatory for federal agency cloud deployments and service models at the low and moderate risk impact levels. It uses a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves federal government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP requirements and controls address the unique elements of cloud computing to ensure that all federal data is secure in cloud environments. For a list of FedRamp-compliant cloud vendors, refer to www.fedramp.gov/marketplace/compliant-systems/. Public safety agencies can contact any FedRamp-compliant provider to find out the cloud vendor's security package specifications.[9]
- Health Insurance Portability and Accountability Act (HIPAA), U.S. Department of Health and Human Services (HHS)[10]
- *Tax Information Security Guidelines for Federal, State, and Local Agencies, Safeguards for Protecting Federal Tax Returns and Return Information*, Internal Revenue Service (IRS) Publication 1075 (IRS 1075)[11]

It is important to note that a digital record can be subject to multiple standards, so a cloud provider's commitment to compliance is absolutely critical. For example, a body-worn video recorded by an officer could become part of a criminal case file (CJIS compliance), recorded in a setting where medical care is being provided (HIPAA compliance), and include statements on employment, income, and aid (IRS 1075 compliance).

Is agency information in the cloud secure? (continued)

B. Secured Access

Public safety agencies are responsible for establishing appropriate access controls, (e.g., credentialed role-based levels of access), for the agency's software and/or Web interface that interacts with cloud data.

C. Breach Notification

An agency should ensure that breach notification is included in the SLA with both the cloud platform provider and, if applicable, any cloud application provider, to articulate the procedure for notification in the event of unauthorized access to the agency's data.

D. Audits

Generally, different types of audits are associated with agency data. These can include:

- Governing authority audits (e.g., FBI CJIS audits)
- Application and Web interface provider audits (e.g., agency contracted audits per the SLA)
- Agency-level audits (e.g., personnel access/usage, policy compliance, accountability)

- The public safety data that is processed and stored by various applications operating in the cloud may contain financial data, as well as personally identifiable information (PII). This data and PII should be protected against unauthorized access, disclosure, modification, theft, or destruction. The vendor should ensure that the facilities housing the network infrastructure are physically secure.
- The vendor shall ensure that its equipment, software, interfaces, processes, procedures, (e.g., auditing and accountability controls), and personnel are in compliance with CJIS security requirements, as well as with other industry standards (e.g., International Organization for Standardization [ISO]) and regulations regarding security.
- By design, availability and SLAs are often absent in cloud contracts. However, public safety agencies should raise the issue during negotiations, require concrete SLA commitments from the vendor, and ensure that there are remedies for downtime. Note: Cloud vendors typically offer service credits for interruptions.
- **Important issue—**It is crucial that the cloud service provider maintain the integrity of public safety data through physical or logical separation between the cloud storage and services provided to public safety agencies versus those provided to other customers. Law enforcement data may not be stored, shared, processed, or modified in any way that compromises the integrity of the data.[12]

Can agencies retain control over their information?

Yes, agencies can maintain complete authority over their own data. Public safety data should be completely accessible at all times in its original form or other easily usable format with no penalties for switching cloud providers or other burdens attached to its access. As a safeguard, any contract with a cloud provider should clearly affirm agency ownership of all its data and the method by which it can be accessed or reclaimed.

There is one additional precaution. There are two types of information stored in the cloud—data that is sent there and data that is created or aggregated in the cloud. Public safety leaders should be aware of how the second type of data can be created out of the original agency information, much the way raw materials are used to construct finished products in a factory. Contracts with cloud providers should be written so that agency information is not used to help create other data sets.

Here are descriptions of the types of cloud data and the ownership distinctions between them:

- **Data created pre-cloud**

  Any information that is gathered or created prior to the cloud environment, such as agency records, files, images, and most other forms of public safety material, is clearly the property of the originator. A large majority of government data in the cloud is this type of data, with all ownership rights and privileges implied and recognized in most states and courts. It is generally acknowledged that data created by an agency which is then uploaded to be stored or processed in the cloud should always be controlled by the government entity that sent the information there in the first place. Proper contract language can ensure this understanding.

- **Data created in the cloud**

  Some data can be processed or otherwise transformed in the cloud to the extent that it becomes a totally new set of data. To illustrate, consider the following fictitious scenario involving the transformation of citizen reports that document complaints about barking dogs. A cloud provider, or third party, with permission could possibly anonymize the reports to remove the PII and then correlate the cleaned data with other information, such as local dog licenses or pet store taxation records. The results could reveal a trend that could be used to guide marketing efforts for a national pet food supplier. Would the set of cleaned, transformed, and correlated data ultimately be owned by the public safety agency that originally generated the barking dog complaint reports? The answer is unclear and depends on the jurisdiction but the original law data will always belong to its creator.

  One thing is clear—transformed data can be very powerful and useful, providing governments, citizens and even businesses with information that is otherwise locked away in silos prior to its

The cloud is auditable and secure.

Original information and exact working copies are stored in the cloud

Processing and/or sharing according to agency guidelines

Encrypted agency information flows through protected network into the cloud

Agency can easily retrieve and use information from the cloud merger with other data. Much like small clues in a police investigation, individual data sets may not seem useful on their own, whereas together they can paint a clearer picture of certain trends or patterns. This type of data synergy can be harnessed by public safety officials to increase citizen safety and, in fact, potentially reduce overall technology costs through its effective and appropriate sharing with interested parties. The cloud can provide the most efficient and secure platform for such data transformation, which, in all cases, should protect the privacy of individual citizens and be used in good public faith. Use of others' data and transformation after storage can, however, bring about a whole new dimension of ownership, which should be mitigated by strong contractual language that controls the use of agency data by cloud providers or third parties to avoid any misunderstandings or misuse.

Can public safety agencies ensure chain of custody of their data while using the cloud?

Yes. Strong contract language is encouraged to ensure that agency information gets to the cloud and stays there in a safe, reliable, and auditable fashion.

Here are some basic recommendations for ensuring appropriate chain of custody of public safety data in the cloud:

- Cloud providers should provide immediate notifications to public safety agencies of any process made against agency data, such as court requests to produce records and any data breaches or substantial breach attempts.
- A formal process should be provided to detect, identify, and respond to data threats.
- No data should be released to any third party without written permission of the public safety agency.
- Since information held or processed in a cloud may become evidence in an investigation, strict integrity procedures should be mandated, including retention of original unmodified files in addition to accurate redundant copying.
- Data should be encrypted both while in motion and at rest.
- Hashtags (sometimes called digital fingerprints) can be added to digital records to prove that files have not been altered.
- Cloud service providers should be contracted to maintain legal records of uploading, access, processing, and downloading to ensure that a precise chain of custody can be established.
- The cloud solution should provide a solution for needing to transfer collected data directly to other partner public safety agencies, such as to the courts, to minimize unnecessary chain-of-custody risks.
- Network security should be equal to or exceed cloud chain-of-custody standards, ensuring that data is safe and auditable while being uploaded or downloaded from cloud computing environments.
- All chain-of-custody procedures should comply with applicable evidentiary admissibility standards.

Essentially, anything that can be done on agency computers or servers theoretically can be performed in the cloud.

What services are offered by cloud vendors?

Essentially, anything that can be done on agency computers or servers theoretically can be performed in the cloud. Cloud services should provide the ability to accept, store, process, analyze, or otherwise compute any type of digital content including text files, records, all types of data, video, audio, and images. In addition, services should include immediate access, retrieval, management, hosting, and sharing. However, while a properly administered cloud-based system accessed via the Web is very secure, nothing is guaranteed to be 100 percent impenetrable. The following is a list of key safeguard recommendations for cloud services.

- Protection and storage of the original media, including metadata from digital multimedia evidence.
- Ability to securely download original media and metadata.
- Automatic transcoding of multimedia assets to a working copy in an interoperable format.
- Media management, editing, and sharing from within the Web-based software tool.
- Digital "curation" (see definitions).
- Access provided anywhere from any device including mobile devices, such as Smartphones and tablets, as well as notebooks and desktop computers.
- Sufficient bandwidth and quality of service to accept multiple simultaneous submissions.
- Logging and audits.
- Georesilience through multiple data centers separated by hundreds of miles to ensure that a disruptive event in one location will not impact back-up copies of data in a separate data center.
- Contractual commitments to comply with standards, such as the FBI's CJIS Security Policy for protection of criminal justice information, HIPAA for the protection of patient health information, IRS Publication 1075 Safeguard for the protection of federal tax information, and FedRAMP for the protection of federal data.

A cloud services system must be robust, secure, and redundant. Services should provide scalability that allows public safety agencies to purchase the level of services they can afford.

Should an agency take preliminary steps before contacting a vendor or generating a request for Proposal or information (RFP/RFI)?

Yes, before contacting a vendor, public safety agencies should assemble a team of stakeholders and subject-matter experts who clearly understand the mission and goals of the cloud services under consideration. This team might include contract and procurement specialists, IT and network managers, legal counsel, and end users. Putting the right team together will help move negotiations quickly, identify potential problems, and make it easier to communicate the agency's needs and expectations to potential vendors. In addition, teams should research and evaluate the long-term stability of potential cloud vendors. Because of the hardships an agency can face, due diligence should be taken when selecting and contracting with a cloud vendor.

Federal agencies that want to secure data in the cloud, or public safety agencies wanting to narrow their vendor searches to only those providers who comply with FedRamp security requirements, may refer to FedRamp's list of compliant cloud service providers, www.fedramp.gov/marketplace/compliant-systems/. FedRamp requires cloud vendors wanting to secure federal data in the cloud to undergo a security assessment to ensure that they are compliant with the *Federal Information Security Management Act of 2002* (FISMA)[13] and with the National Institute of Standards and Technology's (NIST's) *Assessing Security and Privacy Controls for Federal Information Systems and Organizations* (NIST 800-53A).[14]

Should agencies require vendors to meet certain minimum qualifications via contract or service level agreements (SLAs)?

Yes, public safety agencies contemplating the use of cloud computing services should ensure that their planning and implementation of cloud solutions satisfactorily address several key operational principles that must be spelled out in the contract or SLA. These may include the following:

Impermissibility of Data Mining

"Law enforcement agencies should ensure that the cloud service provider does not mine or otherwise process or analyze data for any purpose not explicitly authorized by the law enforcement agency. The cloud provider may process or analyze data as necessary for ongoing and routine performance monitoring to ensure continuity of service and/or to project future dynamic provisioning requirements."

Guiding Principles on Cloud Computing in Law Enforcement, International Association of Chiefs of Police (IACP), June 2015

- System availability, resilience, and redundancy that guarantees that mission-critical operations and data are available 24/7/365. This should include geographically disparate failover and redundant backups, with all services and storage occurring within the United States.
- A clear understanding of data ownership (i.e., perpetual ownership of public safety agency data and any metadata associated with the stored data). This includes data access, control, derivative work product, or the anonymized third-party use of the data by anyone other than the agency. See call-out box on data mining.
- A vendor must make a public safety agency's data available upon request, within one business day or within the time frame specified, and that data shall not be used for any other purpose. The vendor shall provide the requested data at no additional cost to the agency.
- As with any data storage, vendors should have reliable backup systems in case of any damage to stored data, with version controls and levels of redundancy. Copies of a corrupted file are still corrupted.
- A vendor shall use multiple content acceptance and delivery networks with multiple points of presence (POPs) to efficiently and reliably accept and provide access to content.
- The vendor shall provide to the public safety agency notifications of all incidents and/or issues affecting service and/or availability and notifications, at least five business days in advance, of pre-scheduled maintenance or out-of-service events. If new or unanticipated threats or hazards are discovered by either the public safety agency or the vendor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
- The vendor shall provide public safety agency administrators with a clearly defined trouble escalation process to address issues.

- The vendor shall provide a roster of employees with access to systems supporting the public safety agency as part of a fingerprint-based state or federal background check. If required by the agency, such as in the contract or SLA, all vendor employees assigned to the contract must successfully pass a background check as defined by the public safety agency. The vendor shall be responsible for providing personnel who are acceptable to the agency. Vendor personnel working on any part of the public safety agency's data or cloud services, at the agency's request, may be required to sign formal nondisclosure and/or conflict-of-interest agreements to guarantee the protection and integrity of the agency information and data.
- The public safety data that is processed and stored by the various applications within the cloud network infrastructure may contain financial data as well as PII. This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The vendor shall ensure that the facilities that house the network infrastructure are physically secure.
- The vendor shall provide statistics and report content submission information, including IP addresses and any available metadata.
- The agency may require the vendor to successfully complete user acceptance testing during the first 30 days of the contract.
- Public safety agencies must be confident that the terms of any cloud service agreement include specific provisions to ensure continuity of operations and the continued security, confidentiality, integrity, access, and utility of all data subject to the agreement, irrespective of the commercial viability of the service provider or changes in operations, ownership, structure, technical infrastructure, and/or geographic location.
- The cloud vendor should provide to the public safety agency evidence of an independent assessment of the security of the vendor's systems and services, performed by a duly authorized organization with the appropriate credentials to verify the technical, operational, and practices of the vendor.
- The cloud vendor also should provide timely and appropriate documentation that verifies that the vendor currently maintains cybersecurity liability insurance in an amount appropriate to the level of risk associated with managing data and services for and supporting the public safety agency, and agree that it will maintain said insurance throughout the course of its contract or SLA with the agency.

- Well-established cloud vendors are members of industry groups or organizations that impose privacy and security industry standards on their members. The public safety agency should ask the vendor for assurances, or at least an acknowledgement in the contract, that the vendor has received these certifications or is a member of these groups. A vendor's willingness to acknowledge these affiliations in contracts creates a baseline for transparency and helps manage expectations and foster trust.

Who is responsible for privacy?

Privacy is a shared responsibility, in that both the agency and the cloud provider must adopt and implement a privacy policy to protect agency data. Service level agreements should specifically identify procedure and responsibility distribution between the cloud provider and the agency for activities related to privacy data or sensitive data breaches, to include investigation, redress, and resolution of the sensitive data involved.[15]

How Can Privacy be Protected in the Cloud?

As stated above, privacy is a shared responsibility between the agency and its cloud provider. Privacy and security are some of the most heavily negotiated parts of cloud service contracts. Typically, cloud service contracts contain language that articulates that the cloud service provider is responsible for protecting its networks and systems, while the customer is responsible for its users and data. Negotiating these areas typically involves moving risk around to try to get vendors to accept more responsibility or make stronger assurances about their efforts to secure data, preserve confidentiality, and provide adequate access controls. In addition to the contracts themselves, cloud vendors have privacy policies, information-security policies, retention policies, hosting and delivery policies, and other internal documents that govern how they secure and manage customer data. Public safety agencies should review potential cloud vendors' privacy policies that affect the way the vendors manage data.[16]

Survivability

"The terms of any agreement with cloud service providers should recognize potential changes in business structure, operations, and/or organization of the cloud service provider, and ensure continuity of operations and the security, confidentiality, integrity, access and utility of data. Law enforcement [and public safety] agencies must be confident that the terms of any agreement with cloud service providers will include specific provisions to ensure continuity of operations and the continued security, confidentiality, integrity, access, and utility of all data subject to the agreement, irrespective of the commercial viability of the service provider or changes in operations, ownership, structure, technical infrastructure, and/or geographic location."

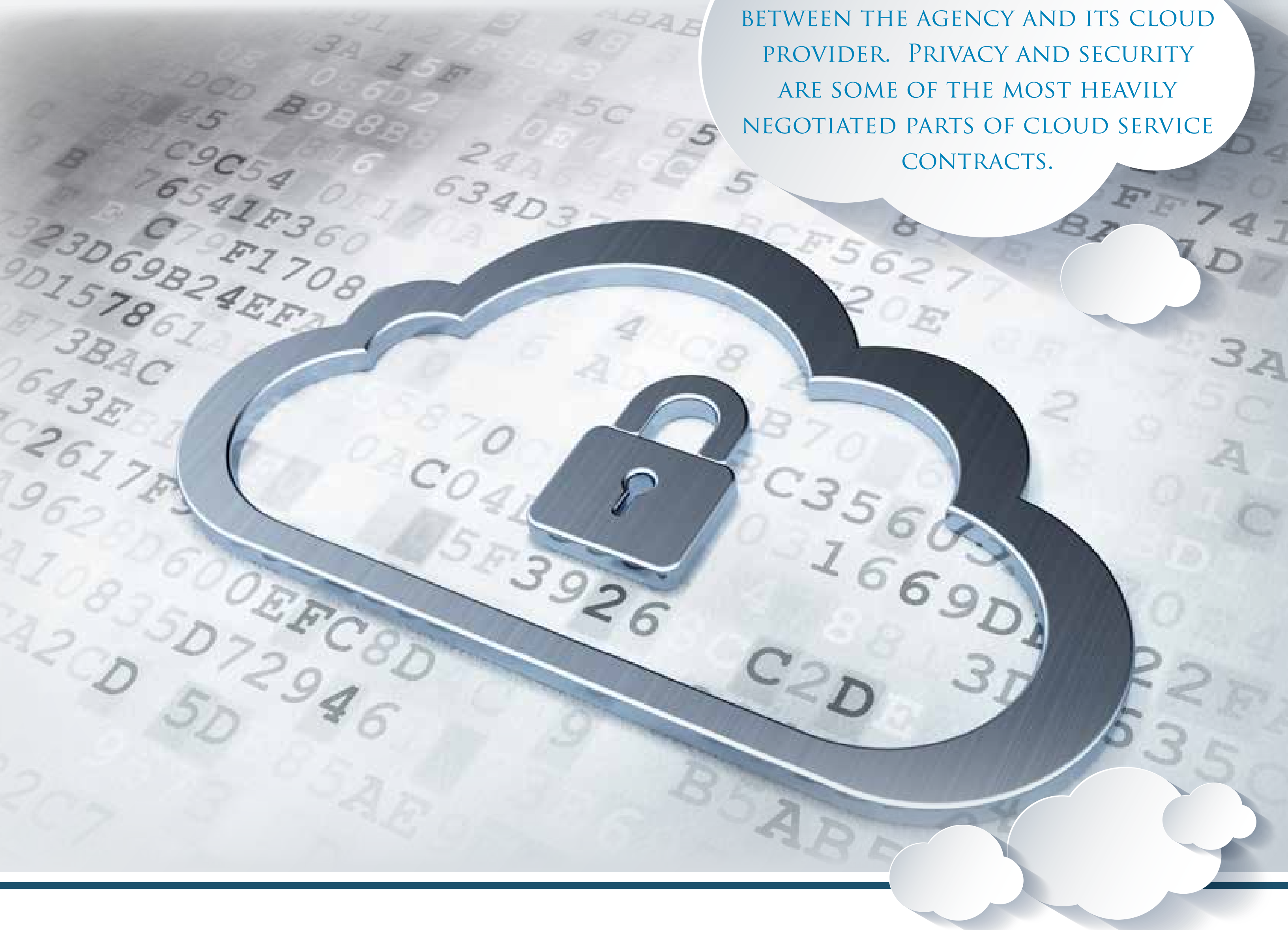
Guiding Principles on Cloud Computing in Law Enforcement, International Association of Chiefs of Police (IACP), June 2015

The following are some recommendations regarding privacy protections, privacy policies, and negotiated protections within a contractual agreement.

- Law enforcement and public safety agency storage policies should outline who is authorized to access cloud data and include an audit system for monitoring access.
- In addition to providing copies of internal policies, a vendor should be contractually obligated to provide all future addendums of the vendor's policies to a specific point of contact at the public safety agency.
- Any agreement with a cloud service provider must take precedence over, and replace, any of the cloud provider's generally applicable privacy, data access or use, or similar policies that might otherwise permit data mining for purposes not explicitly authorized in the agreement.[17]
- Agencies should consult with legal advisors to ensure that data storage policies and practices are in compliance with all relevant laws (e.g., CJIS) and other requirements and that they preserve evidentiary chain of custody.

- The cloud service provider should ensure in its contractual agreement the confidentiality of the public safety agency's data it maintains. The agreement should clarify that the provider will take all necessary physical, technical, administrative, and procedural steps to protect the confidentiality of the data. These steps may include physical security measures, access permission requirements, cybersecurity requirements, criminal history background security checks on employees and vendors with access to systems and data, security awareness training, encryption, regular auditing, and geographical location limitations. Data confidentiality may be further ensured by customer-held key encryption of the data using encryption processes.
- As stated earlier in this FAQ, well-established cloud vendors should be affiliated with privacy and data security organizations or certified with industry-recognized privacy and security standards organizations. When reviewing a cloud vendor's internal policies, be on the lookout for affiliations to privacy and data security organizations and for certifications with industry-recognized privacy and security standards organizations.[18]
- There should be protections in the contractual agreement regarding vendor acquisition: what protections are in place if the vendor is bought. See the call-out box on survivability.

PRIVACY IS A SHARED RESPONSIBILITY BETWEEN THE AGENCY AND ITS CLOUD PROVIDER. PRIVACY AND SECURITY ARE SOME OF THE MOST HEAVILY NEGOTIATED PARTS OF CLOUD SERVICE CONTRACTS.



- The vendor contract should include language that prohibits changes to the policies that materially reduce the level of security and privacy protections promised when the contract was signed or, at a minimum, includes language that requires advanced notice of material reductions in security or privacy controls with an option for the public safety agency to get out of the contract if the agency deems it to be unacceptable.[19]
- While a vendor may publish its baseline security controls, vendors should be prohibited from publishing or disclosing in any manner, without written consent of the public safety agency, the details of any custom policy provisions or safeguards designed or developed by the vendor under the agency's contract. Further, the vendor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under the agency's contract.
- If new or unanticipated threats or hazards are discovered by either the government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
- The vendor will clearly state in the contract and/or privacy policy its sanctions for any employee or vendor violations to the agreement/policy. These will include discontinued access, suspension, demotion, transfer, or termination, administrative actions or sanctions as provided by the state or public safety agency's rules and regulations, if from an external agency request that the organization initiate disciplinary proceedings. The vender may refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy or agreement.
- Any information made available to the vendor by the agency shall be used only for the purpose of carrying out the provisions of the contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.
- The vendor assumes responsibility for protection of the confidentiality of the agency's records and data and shall ensure that all work performed by its subcontractors shall be under the supervision of the vendor or the vendor's responsible employees. Each officer or employee of the vendor, or any of its subcontractors, to whom any agency record or data may be made available or disclosed, shall be notified in writing by the vendor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions.
- The vendor shall protect all agency data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as sensitive but unclassified (SBU) information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If vendor personnel must remove any information from the primary work area, they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act information.
- No data shall be released to a third party by the vendor without digital notification to and consent from the public safety agency. All requests for release must be submitted via digital notification or in writing.

Conclusion

The rising volume of digital evidence (photos, videos, etc.) available to public safety agencies is having a significant impact on agency budgets and resources. As public safety leaders consider the capabilities of the cloud environment to meet digital evidence storage demands, increase capabilities, and reduce costs over time, they should do so with a clear understanding of what cloud technology is, the services the cloud can provide, and the security and privacy protections required for agency data. Ideally, public safety agencies should form teams of stakeholders and subject-matter experts who clearly understand the mission and goals of the cloud services under consideration before contracting with a cloud vendor, and due diligence should be taken to evaluate the stability of potential cloud vendors. In addition, agencies are guided to become familiar with the contractual recommendations contained within this resource, as well as others unique to the agency, and to proactively pursue such assurances through the agency's vendor selection and negotiation process.

Glossary of Terms and Definitions

The following are some key terms an agency should be familiar with regarding cloud technology.

Cloud Application—A cloud application is the phrase used to describe a software application that is never installed on a local computer. Instead, it is hosted by a cloud provider.

Cloud Backup—Cloud backup, or cloud computer backup, refers to backing up data to a remote, cloud-based server. As a form of cloud storage, cloud backup data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

Cloud-Based—The storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

Data—Includes all text, numerical data, database records, media files, demographic information, search history, geolocation information, metadata, or any other data and information, including criminal justice information (law enforcement data) that law enforcement users or vendors provide to a cloud service provider, or to which the cloud service provider otherwise gains access as a direct or indirect product of the cloud services provided to the law enforcement agency.[20]

Digital Curation—The selection, preservation, maintenance, collection, and archiving of digital assets. Digital curation establishes, maintains, and adds value to repositories of digital data for present and future use. This is often accomplished by archivists, librarians, scientists, historians, and scholars. Digital curation is used to improve the quality of information and data within operational and strategic processes. Successful digital curation will mitigate digital obsolescence, keeping the information accessible to users indefinitely.

Digital and Multimedia Evidence (DME) —The analysis of evidence stored or transmitted in binary form.

Infrastructure as a Service (IaaS)—Computer infrastructure, such as virtualization, being delivered as a service. IaaS is popular in the data center, where software and servers are purchased as a fully outsourced service, and is usually billed on usage and how much of the resource is used compared with the traditional method of buying software and servers outright. May also be called enterprise-level hosting platform.

Media Management—A term used for several related tasks throughout post-production. Any task that relates to processing media is considered to be media management, such as capturing, compressing, copying, moving, or deleting media files. Media management also refers to keeping track of media files via clip properties such as notes, comments, hashtags, metadata, etc.

Multitenant—In cloud computing, “multitenant” is the term used to describe multiple customers using the same public cloud instance.

Open Stack—A free and open-source cloud computing software platform used to control pools of processing, storage, and networking resources in a datacenter.

Platform as a Service (PaaS)—A cloud computing model that delivers applications over the Internet. In a PaaS model, a cloud provider delivers hardware and software tools—usually those needed for application development—to its users as a service. A PaaS provider hosts the hardware and software on its own infrastructure.

Point of Presence (PoP)—An Internet point of presence is an access point to the Internet. It is a physical location that houses servers, routers, ATM switches, and digital/analog call aggregators. It may be either part of the facilities of a telecommunications provider that the Internet service provider (ISP) rents or a location separate from the telecommunications provider. ISPs typically have multiple PoPs, sometimes numbering in the thousands. PoPs are also located at Internet exchange points and colocation centers.

Service Level Agreement (SLA)—A contractual agreement by which a service provider defines the level of service, responsibilities, priorities, and guarantees regarding availability, performance, and other aspects of the service.

Software as a Service (SaaS)—A software delivery method that provides access to software and its functions remotely as a Web-based service. Software as a service allows organizations to access business functionality at a cost typically less than paying for licensed applications, since SaaS pricing is based on a monthly fee.

Transcoding—The process of converting a media file or an object from one format to another.

Additional Resources

The following is a starting list of resources provided for public safety agencies wanting to learn more about cloud technology.

Beyond Body Cameras: How to Adapt to New Technologies Like the Cloud (And Whatever Comes Next) (PowerPoint presentation), International Association of Chiefs of Police (IACP), Rick Smith, Matt Mitchell, Jenner Holden, www.theiacp.org/Portals/0/documents/pdfs/LEIM/Executive%20Track%20Workshops/E4%20Beyond%20Body%20Cameras.pdf.

Cloud Best Practices Network (Web site), http://cloudbestpractices.net/. This Web site offers case studies and social media connections to help build enterprise solutions.

Cloud Computing in Law Enforcement: Survey Results and Guiding Principles, David J. Roberts, Police Chief Magazine, March 2013, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2892&issue_id=32013.

Cloud Security Alliance (Web site), https://cloudsecurityalliance.org/. The Web site promotes the use of best practices for providing security assurance in cloud computing.

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, CJISD-ITS-DOC-08140-5.4, Federal Bureau of Investigation (FBI), October 6, 2015, https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.

Executing Search Warrants in the Cloud, John M. Cauthen, FBI Law Enforcement Bulletin, October 7, 2014, https://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud.

Guiding Principles on Cloud Computing in Law Enforcement, IACP, June 2015, www.theiacp.org/Portals/0/documents/pdfs/CloudComputingPrinciples.pdf. Designed for law enforcement agencies using or contemplating the use of cloud services, this resource contains a recommended list of key principles that can be embodied in contractual agreements with a cloud service provider or in service level agreements.

Federal Risk and Authorization Management Program (FedRamp), www.fedramp.gov. FedRamp is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), U.S. Department of Homeland Security (DHS), U.S. Department of Defense (DoD), National Security Agency (NSA), Office of Management and Budget (OMB), and Federal Chief Information Officer (CIO) Council and its working groups, as well as from private industry.

Guidelines on Security and Privacy in Public Cloud Computing, NIST, NIST SP - 800-144, December 9, 2011, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.

Leveraging the Cloud for Law Enforcement: Exploring Operational, Policy, and Technical Opportunities and Challenges (PowerPoint presentation), IACP, 2013, http://www.theiacp.org/Portals/0/documents/pdfs/CloudSurveyResults.pdf.

Mitigating Risk in the Application of Cloud Computing in Law Enforcement, Paul Wormeli, Using Technology Series, IBM Center for the Business of Government, IJIS Institute, 2012, www.ijis.org/resource/collection/232074EF-6453-4014-BC4E-018BF818D291/Mitigating_Risks_in_the_Application_of_Cloud_Computing_in_Law_Enforcement.pdf.

National Body-Worn Camera Toolkit (Web site), Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), www.bja.gov/bwc.

Outsourcing the Evidence Room: Moving Digital Evidence to the Cloud, Vern Sallee, Police Chief Magazine, IACP, April 2014, www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=3319&issue_id=42014.

Police Body-Worn Cameras: Lessons from the Early Adopters, Microsoft, 2014, www.nascio.org/events/sponsors/vrc/Police%20Body-Worn%20Cameras_Lessons%20from%20the%20Early%20Adopters.pdf.

Recommendations for Implementation of Cloud Computing Solutions, Technical Report, Criminal Justice Information Services Division, Federal Bureau of Investigation, April 10, 2012, www.fbi.gov/about-us/cjis/CJIS%20Cloud%20Computing%20Report_20121214.pdf.

Third-Party Vendor Management Means Managing Your Own Risk, Chapter Five: The Cloud, Pedro Pavon, CIPP/US, The Privacy Advisor, International Association of Privacy Professionals, January 27, 2015, https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk-chapter-five-the-cloud/.

ACKNOWLEDGEMENTS

A special thank-you to Global's cloud drafting team for their valuable contributions in authoring and guiding the development of this resource.

Mr. Patrick Doyle
Justice, Law Enforcement, and Border Security
Unisys Corporation©
Retired from New Jersey State Police

Sheriff Mike Milstead
Minnehaha County Sheriff's Office, South Dakota
Representing: National Sheriffs' Association

Mr. John Powell
Retired from Los Angeles County Sheriff's Department (LASD) Cyber Investigations Center and the Large Emergency Event Digital Information Repository (LEEDIR) program

Inspector Sandra Putnam
Child Exploitation and Computer Crimes Unit
Georgia Bureau of Investigation

Mr. Richard Zak
Justice and Public Safety Solutions
U.S. State and Local Government
Microsoft Corporation©

Global Justice Information Sharing Initiative

ABOUT GLOBAL

The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment.

GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global. BJA engages GAC-member organizations and the constituents they serve through collaborative efforts to help address critical justice information sharing issues for the benefit of practitioners in the field.

IT.OJP.GOV/GLOBAL

Endnotes

1. The Federal Bureau of Investigation's (FBI's) Criminal Justice Information Services (CJIS) is the central repository for criminal justice information services in the FBI. Programs under the CJIS Division include the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the National Incident-Based Reporting System (NIBRS). https://www.fbi.gov/about-us/cjis
2. Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—Criminal Intelligence Systems Operating Policies, http://it.ojp.gov/documents/28CFR_Part_23.pdf.
3. *Criminal Justice Information Services (CJIS) Security Policy*, Federal Bureau of Investigation (FBI), www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.
4. Ibid.
5. *Guiding Principles on Cloud Computing in Law Enforcement*, International Association of Chiefs of Police (IACP), June 2015, www.theiacp.org/Portals/0/documents/pdfs/CloudComputingPrinciples.pdf.
6. *Criminal Justice Information Services (CJIS) Security Policy*, FBI, www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.
7. Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—Criminal Intelligence Systems Operating Policies, http://it.ojp.gov/documents/28CFR_Part_23.pdf.
8. The Federal Risk and Authorization Management Program (FedRamp) is a federal governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, www.fedramp.gov.
9. Frequently Asked Questions, Authorize category, FedRamp, http://www.fedramp.gov/resources/faqs/
10. Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160, 162, and 164, HIPAA Administrative Simplification Regulation Text, Office for Civil Rights, U.S. Department of Health and Human Services, March 26, 2013, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. HHS Health Information Privacy portal, www.hhs.gov/hipaa/index.html.
11. *Tax Information Security Guidelines for Federal, State, and Local Agencies, Safeguards for Protecting Federal Tax Returns and Return Information*, Internal Revenue Service (IRS) Publication 1075 (IRS 1075), https://www.irs.gov/pub/irs-pdf/p1075.pdf.
12. *Guiding Principles on Cloud Computing in Law Enforcement*, IACP, June 2015, www.theiacp.org/Portals/0/documents/pdfs/CloudComputingPrinciples.pdf.
13. The *Federal Information Security Management Act of 2002* requires each federal agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
14. *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Special Publication 800-53A, Revision 4, National Institute of Standards and Technology (NIST), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.
15. *Recommendations for Implementation of Cloud Computing Solutions*, Technical Report, Criminal Justice Information Services Division, Federal Bureau of Investigation, April 10, 2012, www.fbi.gov/about-us/cjis/CJIS%20Cloud%20Computing%20Report_20121214.pdf.
16. *Guiding Principles on Cloud Computing in Law Enforcement*, IACP, June 2015, www.theiacp.org/Portals/0/documents/pdfs/CloudComputingPrinciples.pdf.
17. Ibid.
18. *Third-Party Vendor Management Means Managing Your Own Risk*, Chapter Five: The Cloud, Pedro Pavon, CIPP/US, The Privacy Advisor, International Association of Privacy Professionals, January 27, 2015.
19. Ibid.
20. Ibid.

IIR
Institute for Intergovernmental Research

This project was supported by IIR through Grant No. 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Issued 10/2016