



FORCESIGHT

FREQUENTLY-ASKED QUESTIONS

Disclaimer: This document is written with assumptions based upon the state of the Bishop Rock products at the time of writing. These assumptions are subject to change as product engineering changes occur and new releases are created.

FAQ QUESTIONS

Q: We have CAD and RMS systems that provide reports, as well as crime analysts that do manual Excel reports. What capabilities does ForceSIGHT provide that we do not already have?

Q: We have been getting along just fine without one of these “data warehouse” projects so far.

Q: We already have an “information fusion” strategy. We are participating in various information sharing programs.

Q: How can Bishop Rock help implement interagency data sharing?

Q: We already have a data warehouse. What does ForceSIGHT provide us?

Q: Is ForceSIGHT UCR and NIBRS-compliant?

Q: Is ForceSIGHT GJXML-compliant?

Q: We require strict security around our information. For example we are required to keep certain information confidential between managers and direct reports, and we certainly must restrict access to IA data. How does ForceSIGHT support our needs?

Q: How do you ensure security over the Internet?

Outbound to Bishop Rock

Inbound from Bishop Rock

Q: How is information secured while housed with Bishop Rock?

Q: How scalable is ForceSIGHT?

Q: Isn't the US government going to provide these capabilities to us soon through various DOJ/DHS programs?

Q: We have CAD and RMS systems that provide reports, as well as crime analysts that do manual Excel reports. What capabilities does ForceSIGHT provide that we do not already have?

A: Firstly, RMS and CAD database schemas are not designed for “data warehouse” applications. They tend to be highly normalized and indexed for fast transaction processing, not summary query processing. OLAP-style queries run against highly normalized schemas also tend to perform poorly due to large numbers of joins. The kinds of queries that ForceSIGHT supports could have major performance implications if they were run directly against RMS or CAD systems.

Secondly, ForceSIGHT is an integrated analytical application, not a library of independent reports. Users can seamlessly navigate between different views of the data



in ForceSIGHT, rather than having to flip between various reports in a conventional reporting solution.

Q: We have been getting along just fine without one of these “data warehouse” projects so far.

A: Law enforcement is now following a similar trajectory to what the commercial sector followed in the 1990s. Online transaction processing (OLTP) systems were first implemented for major business functions (sales, service, manufacturing). These are analogous to RMS and CAD systems in law enforcement. After awhile, businesses found that in order to get insight and visibility into strategic issues that crossed different systems, merely capturing the data electronically and running reports wasn't enough. Data needed to be consolidated and transformed into a central platform for analysis that became known as the data warehouse. “Business intelligence” tools were implemented to access this information. Today many organizations are implementing advanced features such as executive dashboards and statistical data mining.

Law enforcement has just finished the widespread adoption phase of computerized RMS and CAD technology. Recent focus has been in linking independent agencies' systems together for distributed search purposes, as well as acquiring supporting sensor systems such as shot location, street camera, and license plate reader systems.

Predictably, without a strategy for integrating these systems together into a data warehouse, they will become stovepiped “data islands”. You can't find out how many proactive officer vehicle stops result in drug arrests without a special study because the data sits in two different systems that don't get consolidated together except for special ad hoc projects. The realization is starting to sink in that *just because you're now collecting information electronically now doesn't mean that you can effectively leverage it strategically without the right tools.*

ForceSIGHT is the online analytical processing (OLAP) platform for law enforcement. By focusing on this particular sector, we are able to provide both an integration strategy and a complete set of analytical applications “out of the box”.

While agencies may have been able to get away with a lack of a business intelligence platform in the past when there was little electronic data to analyze, now that agency databases are ubiquitous, executives are demanding that they start getting some of the strategic insight value that they thought they were going to get out of deploying RMS systems in the first place. The only way to do that is through business intelligence.

Law enforcement agencies differ from the Fortune 500 companies in that most do not have \$20 million to budget for a custom data warehouse. Bishop Rock's goal is to take the lessons learned from the commercial implementation of business intelligence, package it as a ready-to-use law enforcement application, and save law enforcement organizations the pain of learning these lessons on their own by delivering a turn-key solution.

Q: We already have an “information fusion” strategy. We are participating in various information sharing programs.

A: If there is one thing we wish we could communicate to every law enforcement executive and CIO about about “information fusion” and data sharing initiatives is that there is a huge difference between **application integration** and **data integration**. Application integration involves one application asking another application to perform some well-defined function, such as displaying a suspect profile or returning a list of records that match an input parameter. Data integration involves the merging of all application databases into a single model that can support virtually any inquiry such as, how many officers from Sector 3 called in sick last Tuesday? Application integration is generally easier to implement, and it lends itself well to federated architectures (aka service-oriented architectures (SOA), broker-message-based architectures, etc.). Data integration is required to answer a lot of the really interesting business questions, but achieving application integration does not give you the benefits of data integration “for free”.

With respect to current data sharing and information fusion initiatives, virtually all of these systems are application integrations focused on providing “search” style services to allow officers to pull together detail case information from different systems (or agencies) and display the search results on a single screen. Without such capability, officers may have to search across several different applications to research a complete suspect profile, or make special requests of neighboring agencies to do searches on their behalf. An integrated search capability improves productivity and increases the amount of case information at an officer’s fingertips, increasing the likelihood of a key case connection being made.

This type of application lends itself well to a federated architecture.

However, the choice of a federated architecture there is a huge class of information needs that this does not address, and indeed these federated architectures are inherently incapable of meeting them:

1) Queries with criteria that cross system boundaries

Examples:

Find the persons whose DMV registrations have expired and were involved in a traffic incident after expiration.

Find the persons who own Ford Mustangs (DMV database) who are gang members (Gang database) and were involved in a crime in the past six weeks (RMS).



Suppose for the above examples that the RMS, DMV, and Gang databases are part of a distributed, federated system. You might be able to individually get lists of people who own Mustangs, are gang members, or were involved in a crime in the past six weeks. These would be three very large lists. But getting a list that is just the intersection of those three lists is problematic due to the data volumes involved.

2) Summarization

How many people are there whose DMV registrations have expired and were involved in a traffic incident after expiration. Can we see them by age groups?

This query requires the crossing of two conditions that apply to two different databases: DMV expiration (DMV) and traffic incidents (RMS). A federated system would have to pull all expirations into some middle tier and match them up with all traffic incidents. These are two potentially huge groups of people that would have to be pulled from the DMV and RMS databases. Finally, the results have to be summarized by a field, "age group". Most federated search systems don't even try to support these types of queries. At best, a custom process could be built at great time and expense, that would solve only this particular example. What if you also like to see age group and gender? That's another round of programming...

With respect to data sharing integration, the same types of restrictions apply. We have found that most federated data sharing systems at present cannot answer the following question:

Who are the top robbers across all of the jurisdictions participating in the data sharing program?

Answering that question would seem like a basic benefit of an interagency data sharing arrangement; indeed it might have been an expectation if not a stated requirement. However, because these systems are built for searching rather than business intelligence, you could not answer that question with these systems short of exporting a raw list and summarizing it yourself in another software product.

In summary, ForceSIGHT fills a key gap in many information fusion initiatives: providing strategic analytics to executive decision makers.

Q: How can Bishop Rock help implement interagency data sharing?

A: There are a number of lengthy, costly interagency data sharing projects going on in the United States today between law enforcement agencies at all levels. One of the "side benefits" granted to agencies who leverage Bishop Rock's hosted platform is that interagency data sharing can be implemented through administration screens, rather than by initiating a separate costly systems project. After a group of agencies agrees to who will share what data with whom, the system administrators can simply go into



ForceSIGHT and set up the sharing rules. This has the potential to **save agencies millions of dollars** in systems integration costs. It does assume that each participating agency is already a Bishop Rock customer, but in most cases the systems integration savings alone will pay for ForceSIGHT.

Q: We already have a data warehouse. What does ForceSIGHT provide us?

A: ForceSIGHT is a prepackaged analytical application for law enforcement. It is not a toolset, such as many business intelligence software vendors provide. Our application is comprehensive, touching a vast array of topics.

We can leverage your existing data warehouse investment as a feed of clean data into ForceSIGHT. ForceSIGHT then becomes a value-added data mart within your agency's technical architecture, unlocking the hidden value in your data warehouse by deploying an extraordinary set of analytical applications to the entire agency.

Q: We have consultants and academics that produce analytical studies. Why do we need to bring a system into the agency to monitor these metrics?

A: Historically, agencies have relied upon these outsiders because they did not have the infrastructure to do it themselves. Consultants and university researchers typically spend a very large percentage of research time simply manipulating and restructuring data to be suitable for analysis. Research projects tend to be one-time events that produce a study that may or may not be actionable. In any case, it does not leave the department with a monitoring tool in place going forward. This in turn makes it difficult to institutionalize any type of metrics-based management systems.

ForceSIGHT enables you to monitor key metrics without having to call in outside consultants for an ad hoc study. It also makes consulting engagements more effective because the time typically spent in data research can instead be spent on finding solutions to the problems that are exposed by ForceSIGHT.

Q: Is ForceSIGHT UCR and NIBRS-compliant?

In short, yes—both UCR and NIBRS categories are available in ForceSIGHT. However, ForceSIGHT's modern information modeling approach has some tremendous advantages over both UCR and NIBRS.

Collecting more detailed information from officers filing incident reports is a process discipline imposed by the agency through its policies and its RMS system. Classifying crimes is a matter of assigning attributes to the legal code. You don't need NIBRS to collect better information, nor to develop a crime classification system that makes sense for your agency. NIBRS adds an extra conversion step to the process that.



UCR was designed in 1929 before computerization was available. It was designed to rollup all crime attributes into a three-level hierarchy (PartI/II, Primary, Secondary). Although crime has evolved, UCR has barely changed over time. It required an act of Congress in 1972 to add a new tracking category, arson.

NIBRS represents a classification approach developed in the 1970s. It takes several steps in the right direction, by tracking individual incidents, effectively handling multi-crime incidents, and expanding the number of categories. However, it tends to double the data entry workload per incident, and is perceived as having no value to local law enforcement.

Fundamentally, these programs are not designed to service local law enforcement. They are designed to makes it easier for 1970s-era mainframes still in use at DOJ to produce consolidated statistics. NIBRS projects often have the stated goal of “improving the quality of data gathered”. Agencies can do that without a NIBRS program—in fact they can probably do a superior job at that than a lowest-common-denominator federal standard can.

We at Bishop Rock use an approach developed in the 1990s called dimensional modeling. We start from the lowest levels of entities--basic events, expanding this not just to incidents but to sensors (e.g. gunshots detected, geofence violations by probationers), proactive police activities such as field contacts, and non-crime-related service calls. This model gives you a total picture of force activity, including crime-related activities.

If you want to classify carjacking as a vehicle-related crime, you can. If it is categorized as a violent crime, you can do that too. If you want to enforce the hierarchy rule, you push a button in ForceSIGHT to do turn it on or off. There has been much controversy with NIBRS, for example, in that because it dispenses with the hierarchy rule, incidents with multiple crimes will tend to inflate overall crime statistics. ForceSIGHT uniquely gives you the ability to apply the hierarchy rule to NIBRS-based categories.

We have a flexible categorization system that can be expanded whenever an agency wants, without having to gain a nationwide consensus first. Once freed from the constraints of the federal categories, we believe that much more insightful analysis are possible.

Q: Is ForceSIGHT GJXML-compliant?

A: ForceSIGHT is capable of integrating with GJXML messaging systems. However, we are not at this time recommending this as the preferred integration option. The reasons are as follows:

GJXML is still a relatively immature standard for which there are virtually no commercially available off-the-shelf solutions. As of May 2007, our research has found

very little commercial market support for GJXML gateways. The US DOJ provides extensive schema specifications but no implementation tools. Individual states and agencies are creating “homegrown” solutions that utilize the standard but these are not general-purpose solutions. What is currently available are general-purpose XML middleware engines that consultants can configure according to the GJXML standards to create information exchange packets (IEP). The level of effort associated with this type of solution should not be underestimated.

What it means to be “GJXML-compliant” is currently left up to agencies and vendors. Therefore, we cannot rely upon any given RMS or messaging gateway having specific data elements available in their schemas. This limits the ability to reuse IEPs.

GJXML is a very large and unwieldy specification. Industry surveys have revealed an *average implementation time between 12-18 months* just for an interface gateway. A significant part of ForceSIGHT’s value proposition is in how quickly we can start delivering value. Using a GJXML-based integration strategy would therefore greatly increase our implementation times.

GJXML was designed for sharing and querying of individual case data between agencies. It was not designed for the summarization, trending, and performance management application of the sort that ForceSIGHT represents. We therefore would have to extensively extend the GJXML specification in order to serve our purposes.

GJXML-based processing of data records is relatively slow. Its performance is adequate when you are simply doing a search for a single person across multiple systems and returning any matching documents. However, in an analytical application such as ForceSIGHT, we have to pull all of the information all of the time, because we don’t know in advance which information will prove interesting to the end users. This could potentially involve thousands or millions of records per day; we have seen very few XML-based gateway implementations that scale to that level, and none involving GJXML.

To summarize our position, we believe that implementing a GJXML-based data transport solution would be much more expensive, take longer to deploy, and involve much more technical risk than a simpler database-oriented extraction, transformation, and load (ETL) paradigm that bypasses GJXML altogether. ForceSIGHT therefore provides its own high-speed ETL adaptors for the various systems we interface to.

As the GJXML market matures, as more RMS systems support it, as our products move into the realm of real-time latency, and as commercial GJ XML gateways emerge, Bishop Rock intends to robustly support GJXML interfaces. At present, however, we believe other technologies can get our customers up and running cheaper and faster.



Q: We require strict security around our information. For example we are required to keep certain information confidential between managers and direct reports, and we certainly must restrict access to IA data. How does ForceSIGHT support our needs?

A: ForceSIGHT is designed with law enforcement security needs in mind. At every step along the way, ForceSIGHT is uniquely designed to maximize information security.

ForceSIGHT group-based security can be applied in many different ways in the application. User access is defined by combining the rights to all of the groups to which they are assigned.

Security Type	Description
Role-based application security	User groups may be restricted from access to certain modules, such as risk or internal affairs-related applications
Role-based screen security	Specific screens may be restricted, such as a detail search screen.
Role-based column security	Certain data elements may be restricted, such as SSNs and investigator notes
Role-based row security	Certain rows may be restricted, such as restricting child abuse victims from access by general user groups
Agency security	Columns and rows may be restricted from outside agencies, in a data sharing arrangement.
Record ownership security	Row visibility may be restricted only to those who created the rows.
Chain of command security	Row visibility may be restricted to those associated within a supervisor’s reporting chain. E.g. a sergeant may only see citizen complaints related to his or her own direct reports.

Q: How do you ensure security over the Internet?

A: When ForceSIGHT is deployed via the Internet, a security concern naturally arises around the vulnerability of information to interception. We have taken extreme care in designing our architecture to maximize the security of this information.

ForceSIGHT Security Architecture

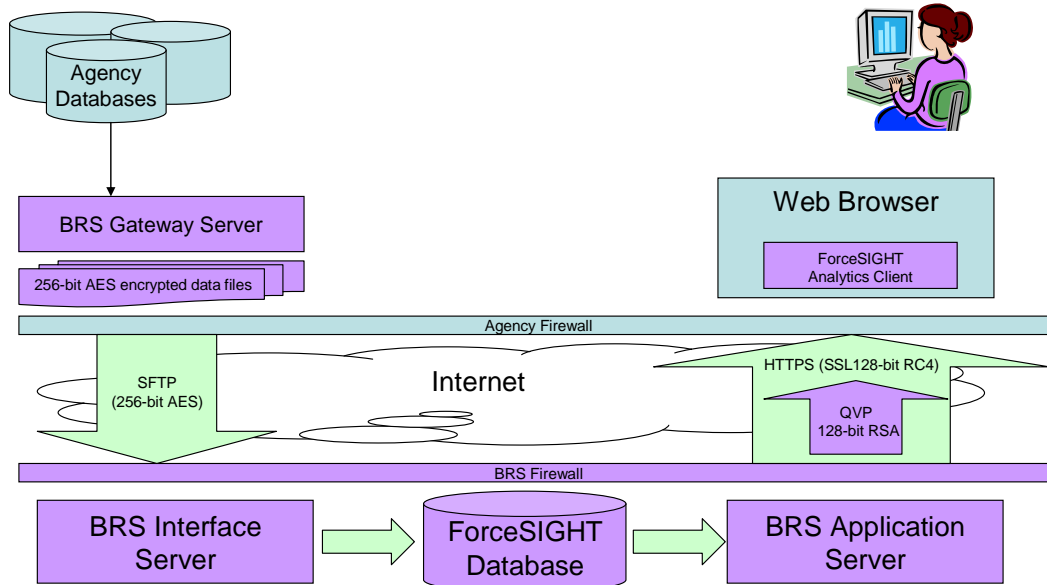


Fig. 1 Bishop Rock ForceSIGHT Security Architecture

Outbound to Bishop Rock

Our extract processes require a read-only database login to each system we are interfacing to. As we extract data from the databases, each file is compressed and encrypted using 256-bit AES encryption, which is approved by the US National Security Agency for TOP SECRET information. These files are picked up by the Gateway Server and send via SFTP using AES-256 bit encryption (with a distinct key from the one used in the file compression step). SFTP is preferred because it requires opening up only a single port in the agency's firewall, and it supports advanced encryption.

Once on the Bishop Rock Server, the information is decrypted using an agency-controlled password for the incoming files. This password is set in the Administration console by the agency administrator and is not otherwise available to Bishop Rock employees.

Inbound from Bishop Rock

Unlike most web-based applications, ForceSIGHT information is displayed via ActiveX controls, not HTML tables. Therefore, ForceSIGHT is not vulnerable to attacks based on intercepting HTTP traffic or reading HTML. This architecturally ensures that



ForceSIGHT is **simply not vulnerable to a whole class of attacks** that most web applications are vulnerable to.

ForceSIGHT clients communicate to the server over a **proprietary, not publicly-published protocol (QVP)**. Any theoretical interception would also have to either acquire or reverse-engineer this protocol to make sense of the information.

ForceSIGHT clients communicate to the server using 128-bit RSA encryption.

Finally, the web browser itself uses SSL, which uses the 128-bit RC4 algorithm. As Windows Vista clients become more common, this will be upgraded to 256-bit AES.

A hacker would therefore need to crack 128-bit RC4 encryption, then separately crack 128-bit RSA encryption, reverse-engineer the protocol, and finally find a way to translate graphics rendering commands into useful information, in order to decrypt the contents of a single user session. The use of an additional encrypted protocol to secure information above and beyond SSL is **unique in the industry** and ensures that your information is probably *more secure with Bishop Rock than it is in your own RMS*.

To summarize, Bishop Rock Software has designed ForceSIGHT to use the latest in encryption technology. We also follow security industry best practices by incorporating **multiple layers of security**. This ensures that the failure of a single layer of security will not expose the system.

Q: How is information secured while housed with Bishop Rock?

A: Our security protocols are as strong or stronger than many of the agencies we work with. Employees with systems access undergo extensive background checks. We also permit agencies to conduct background checks of their own if desired. We use multiple levels of firewall security on our network. Agency data is housed in an encrypted database. Physical access to machines is restricted to authorized personnel, in the access-controlled data center.

Q: How scalable is ForceSIGHT?

A: ForceSIGHT is designed to handle thousands of users on a commodity “Wintel” quad-processor server. We recommend the 64-bit version of Windows for maximum performance and scalability. Larger agencies will require larger amounts of RAM (4GB-8GB+), depending on how much history is to be made available online.

Data is not transferred to ForceSIGHT clients for processing—all data processing is handled at the server tier. The client is just responsible for drawing charts and tables on the user’s screen.



Our tests have shown average loading performance of approximately 2GB per minute during refreshes, which is more than enough for even the largest agencies today.

Finally, one of our major differentiators is that we utilize technology that is orders of **magnitude faster** than competitors using conventional RDBMS technology. Users of ForceSIGHT can summarize and scan through millions of records with **subsecond response**. No other law enforcement analytics platform delivers anywhere close to the performance.

Q: Isn't the US government going to provide these capabilities to us soon through various DOJ/DHS programs?

A: Current projections in DOJ's information technology long-term plan envision that by 2030 there will be full federal-state-local application integration. As discussed previously, this does not mean that you will be any closer to the kinds of strategic analysis that ForceSIGHT enables today.

We do encourage potential buyers to research the availability of DOJ and DHS grants for funding ForceSIGHT implementations, as they tend to qualify under multiple programs.