spillman®
technologies, inc.
reliable innovation

Creating a Multi-Agency Shared Software System: Best Practices

A Spillman Technologies White Paper

Table of Contents:

Introduction .... page 1

What is a Multi-Agency Shared Software System?

The Benefits of a Multi-Agency Shared Software System

Best Practices for Creating a Shared Software System .... page 1

Technology and Leadership Committees

Organizing System Administration

Upgrading the System

Selecting the Host Agency

Creating Data Entry Standards

Managing Billing and Maintenance Fees

Organizing System Administration

Overcoming Obstacles

Multi-Agency Case Study: Spillman Data Sharing in Utah County .... page 3

Overview

Identifying the Need

Establishing a Data Sharing System

Data Sharing in Action

Spillman: A History of Seamless, Reliable Data Sharing .... page 5

Final Note .... page 6

Introduction

Forming a multi-agency shared software group enables participating public safety agencies to share data, minimize costs, improve crime-fighting strategies, and boost officer safety. Agencies with a common vision of how to manage the system, and a willingness to cooperate, can overcome organizational challenges and jurisdictional conflicts to successfully share data.

What is a Multi-Agency Shared Software System?

A multi-agency data sharing system allows agencies to seamlessly share data with other agencies across multiple jurisdictions. In most scenarios, agencies will use a single database to store the data collected by all participating parties. One agency acts as the host by storing the server at its location, and other participating agencies store data on a designated segment of that same server.

The Benefits of a Multi-Agency Shared Software System

Data sharing allows agencies to achieve interoperability, enhancing the ability of emergency responders to work together to prevent crime and improve efficiency. By sharing law records, fire incidents, names, vehicles, property, digital images, and other data on a daily basis, agencies can better identify regional crime trends and develop prevention strategies. The ability to access live data from the field and view alerts and warnings in real time gives field personnel the information they need to stay safe. Interoperability also provides agencies with information needed to coordinate responses to large-scale disasters and strengthen homeland security.

Best Practices for Creating a Shared Software System

Technology and Leadership Committees

One of the first steps in forming a shared software system should be to form a technology committee to direct the implementation and function of a shared system. Each participating agency should appoint at least one member to the committee. The technology committee should research vendors and solicit RFPs, make recommendations for a software purchase, and ultimately, set the groundwork for the day-to-day working of the system.

Support from chiefs, sheriffs, and other top administrators is crucial for the success of a shared system. By also forming a leadership committee that operates separately from the technology committee, agency leaders have the ability to approve the technology committee's recommendations and appropriate funding without becoming directly involved in the technical details of the system.

Organizing System Administration

To administer the system, the technology committee should appoint “super users” to act as system administrators for one or more participating agencies. Each super user becomes the contact point for any questions or concerns that his or her assigned agency may have. It is important that those selected have the technical experience for the job and can provide their agencies with adequate support.

Upgrading the System

The technology committee may wish to enhance the shared system through the purchase of additional modules. One way the committee can accomplish this is by making a presentation to all agencies to inform them about the benefits and costs of the new modules. Each agency can then make the decision as to whether or not to purchase the new software.

The technology committee can also serve as an advisory board for agencies wishing to independently purchase additional software modules. Agencies without sufficient technological expertise can turn to the committee to help them research their decision and decide if the modules will help them accomplish their goals.

Selecting the Host Agency

Hosting a shared system comes with increased technological responsibilities. Because the server will be stored at the host agency, the host agency will need to have the resources to implement proper server maintenance and support.

In some scenarios, host agencies have volunteered to manage the financial costs of hosting the server, such as hardware expenses and maintenance fees. At other agencies, those costs are split between all participating users.

Creating Data Entry Standards

Data entry standards need to be defined upon creating a shared system. All personnel that will be entering data into the system should be trained to follow the same data entry rules. These standards can be based on those already in use by participating agencies. Holding regular post-implementation meetings helps to ensure that all users are complying with data entry standards.

The technology committee should also determine as a group what data to populate into the system. The code tables will enable agencies to easily gather the statistical data needed to meet reporting requirements.

Managing Billing and Maintenance Fees

In some systems, host and shared agencies may want to work together to find a way to share maintenance and billing costs. The host agency can also collect maintenance fees by requiring agencies to contribute a set amount each year, based on the number of sworn officers employed by each agency.

Overcoming Obstacles

When trying to form a shared system, agencies may face opposition from within and outside the group of participating agencies. Top administrators may be reluctant to give up full control of what they consider to be "their" data. The shared system's technology committee can meet with administrators to explain how the ability to access a wide range of data will give all agencies involved the ability to solve more crimes and improve officer safety. The committee can also explain how a shared system leads to cost savings. By using a shared system, agencies save the expense associated with hosting and administering their own servers.

When an agency shares data with another agency, the first concern is often about what information will be shared and what will be restricted. For example, administrators may want to share data about a common burglary while restricting access to information about an internal investigation. The technology and leadership committees need to carefully evaluate any data sharing solution to ensure they will have the ability to control access to sensitive information.

Once administrators are comfortable with the content that is being shared, they can turn their attention to making sure that the data is secure as it traverses public networks such as the Internet. This level of security can be accomplished using software that utilizes security tools such as Secure Sockets Layer (SSL) and a Criminal Justice Information Services (CJIS)-approved encryption methodology, such as Advanced Encryption System (AES) or Triple Data Encryption Algorithm (Triple DES).

Multi-Agency Case Study: Spillman Data Sharing in Utah County

Overview

As the second-largest county in Utah, Utah County is home to more than half a million residents and acts as a conduit for people driving the I-15 corridor from Salt Lake City to Las Vegas and California. Public safety agencies throughout the county needed a way to track criminals as they moved across jurisdictional borders. Sharing data enables these agencies not only to work together, but also allows the smaller jurisdictions to benefit from technology that they would not be able to afford on their own.

Identifying the Need

In 2003, Utah County had 20 fire departments, 15 police departments, 15 EMS providers, and five PSAP centers using disparate CAD and records management systems. The Utah County Sheriff's Office's CAD and records management systems were failing, and the Orem City Department of Public Safety was seeking a new CAD/RMS system. Many other agencies in Utah County were actively seeking an upgrade to their existing systems that would allow them to share information.

Establishing a Data Sharing System

In the aftermath of 9/11, the federal government offered funding to help improve interoperability between jurisdictions to prevent future acts of terrorism. During a discussion in a monthly meeting of police chiefs, the Utah County agencies decided to utilize Homeland Security funds to implement a shared interoperable communications and records management system.

After extensive research into software vendors, Utah County Sheriff's Office and Orem City Department of Public Safety selected Spillman Technologies as the vendor best suited to meet their CAD/RMS needs. Eight smaller agencies in the county were already using Spillman software and were unwilling to consider changing vendors. The agencies implemented their shared Spillman system in December 2004.

Data Sharing in Action

Among the cases that have been solved using Utah County's shared system was a hit-and-run incident involving a 15-year-old boy. In April 2007, 15-year-old Josh Evans was hit by a red Pontiac Firebird while riding his bike in Springville. The driver left the scene of the crime. Two days later the suspect drove the car up a nearby canyon, ignited the vehicle using an accelerant, and pushed the Firebird off a cliff.

A group of campers noticed the resulting flames and called the Spanish Fork Fire Department. The Utah County Sheriff's Office was notified and was able to recover part of the vehicle identification number (VIN) from the charred wreckage.

Three days after the accident, the sheriff's office ran the partial VIN number through the state's vehicle registration system but was unable to find a match. The partial VIN was then entered into the Spillman system, which instantly retrieved a vehicle record out of the more than 256,000 records in the system.

A record had been created for the Firebird the previous month, when the driver, Edwin Ruiz-Gomez, was pulled over by the Spanish Fork Police Department for speeding. The deputies then searched for Ruiz-Gomez's name in the Spillman system and discovered that he was already booked into the Utah County Jail, serving time for a DUI unrelated to the hit-and-run incident. Deputies then confronted Ruiz-Gomez, who confessed to hitting Evans and leaving the scene of the crime. Evans made a full recovery.

Without Spillman, the vehicle search would have been much more time-consuming. The Firebird was registered in Oregon, which is why the Utah vehicle registration system contained no information about it. Deputies would have had to search the vehicle registration databases of all 50 states for information, said former Utah County Lieutenant, Dave Snyder.

"It would have been much more difficult, and required much more time and effort without Spillman," Snyder said. "Spillman made everything so much easier."

Spillman: A History of Seamless, Reliable Data Sharing

In addition to agencies in Utah County, 79% of Spillman customers use Spillman software to share data with anywhere from two to 51 other Spillman and non-Spillman agencies.

Spillman software is designed to make it easy to create a multi-agency shared software system. Users can store data on a single Spillman database, which can then be accessed in real time by all participating agencies. Each agency has the capability to restrict access to specific data while still providing users with a collective pool of information.

Agencies can also customize their Spillman software to meet their unique needs. They can purchase modules individually or as a shared system, allowing each jurisdiction to create a software system that fits its needs and budget.

Every 12 to 18 months on average, Spillman releases a software enhancement with upgraded features, taking the guesswork out of software upgrades. Customers with annual maintenance agreements receive these upgrades along with telephone and online support at no charge.

Spillman maintains system security by allowing agencies to set user privileges, defining which users can access data and at what level. Spillman offers encryption that complies with the following standards: National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS).

Final Note

Participating in a multi-agency shared software system provides agencies with the data they need to maximize their law enforcement capabilities. By following these best practices, agencies can increase interoperability, improve efficiency, and reduce technology costs through a successful shared system.

To learn how to share data with other agencies using Spillman software, contact us at 800.860.8026 or salesinfo@spillman.com.

spillman®
technologies, inc.
reliable innovation

4625 West Lake Park Blvd.
Salt Lake City, UT 84120
Toll-free: 800.860.8026
FAX: 801.902.1210
E-mail: info@spillman.com
www.spillman.com

About Spillman

Spillman Technologies meets the needs of public safety professionals with a comprehensive suite of integrated software solutions. The software is installed at more than 850 agencies nationwide.

Police Sheriff Communications Fire Corrections