Benchmarking Best Practices for Information Sharing

Terina Edmond

AJS/594

Jon Stern

University of Phoenix

January 26, 2021

Table of Contents

1. Introduction
2. Identification of Program Goals
3. Outcome Objective
4. Resources Needed to Implement the Program
5. Eliciting Stakeholder Participation
6. Conclusion
7. References

**(Week One) Information Sharing**

Abstract Law enforcement agencies depend on several communication platforms for operations. Communication is an essential key for the flow of information and data to one agency to another. One of the most evolving platforms is the Internet. “Using available technology to integrate existing resources will provide law enforcement professionals with expanded access to information that will aid in current investigations and could help prevent future criminal activity” (University of Phoenix, 2018). This proposal will contain information relevant to information sharing in the criminal justice sector.

**Case Study Problem**

It is vital that law enforcement agencies receive and have access to information in an appropriate time frame to alleviate any foreseen dangers. Although, the attaining information can often become burdensome for many law enforcement officers since substantial about of information is embedded in online and trying to retrieve the criminal threat can consume an enormous amount of time. “Protecting the country from ever-evolving, transnational threats require a strengthened homeland security enterprise that shares information across traditional organizational boundaries” (Information Sharing). In the Information Sharing case study the dilemma revolves around the inadequacy of officers to response to crime because of information sharing among other law enforcement entities.

When law enforcement agencies fail to share information, it can be disastrous action that can be felt on a macro level. For example, on January 6, 2021, the United States Capitol was stormed by rioters because they did not approve of the endorsement of the next president. After the unprecedented act information revealed that the FBI warned The United States Capitol Police of potential security threats, but they did not take the necessary steps to avert such a riot from occurring.

It is mandatory for law enforcement agencies to engage in information sharing to regularly compare data. By doing so they can cohesively agree that a location or persons need to be secured expeditiously. According to the case study reading this move will aid law enforcement agencies by the providing capability to request multiple centralized repository resources. (University of Phoenix, 2018). The unification of information sharing has the potential of reducing criminal activity beyond the city crimes but also in under privilege, where most criminals will be most likely to become sinister citizens.

**Problem Resolution**

Law enforcement agencies must be able to sustain an adequate system of communication to satisfy various operational needs. Law enforcement agencies officers must maintain critical access of lawbreakers’ criminal records and having the proper systems in place allows for a smoother line of communication among responding agencies. “Law enforcement agencies increasingly demand sophisticated information technology (IT) capabilities to support their operations” (Hollywood &Winkelman, 2015). Information sharing among law enforcement agencies can be sufficiently reduces by applying programs such as Records Management Systems and Computer-Aided Dispatch. Such technology will also be beneficial to law enforcement agencies operating in secluded areas. These systems also allow the command base to respond quickly to an officer’ distress call when inquiring about a suspect’s identification and criminal history.

Although these systems are costly there is an essential need for them in every sector of law enforcement for information sharing to reach all available applicable agencies when possible. Evolving strategies have been created to lessen the affordability of these systems, “including comparatively inexpensive off-the-shelf systems, shared licensing schemes in which agencies in a region share systems, and software-as-a-service/cloud migration models in which a third-party host,” (Hollywood &Winkelman, 2015) but control of the data is still maintain through the agency. The execution of policies and cost deduction will help law enforcement agencies to devise a plan that includes information technology such as RMSs AND CAD.

The need for both instruments is necessary the RMSs allows officers to retrieve data in real time and CAD is a vital communication response call mechanism for an officer’s need for service. Understanding the effort, it takes to reduce crime begins with this technology. According to a study conducted by Hollywood & Winkleman regarding information sharing they explained the INFORMATION SHARING 6 importance of having the ability to know what is going on and the location of an officer is sufficient part of RMSs and CAD systems. While the RMS systems answer, “why can’t we know?” the CAD resolves the question “why can’t we talk?” (Hollywood & Winkleman).

**Process Identification of Problem**

“Problem identification is part of the scientific method, as it serves as the first step in a systematic process to identify, evaluate a problem and explore potential solutions” (Kember, 2018). The identity of a problem overrides finding a solution to it. The identification of solving seeks to resolve a problem by understanding the diagnostics of the problem and the fundamentals of the problem, rather than its developed warning signs. Diagrams and flowcharts are the means to solving the fundamental approach it focuses on the cause-and-effect.

By analyzing the cause-and-effect diagrams and flowcharts an emerging image can be developed that understands root of the problem. It could prove to be detrimental if policies, procedures, and practices among all players are not adequately reviewed and applied when trying to validate data to identify the problem. An assessment is needed to identify the problem including present and past data, communication and data platforms, and all involved law enforcement agencies. The article, *Understanding law enforcement information sharing for criminal intelligence purposes*, the writer, Rick Brown, discusses how law enforcement agencies information sharing can prevent linkage blindness, which agencies are unknowingly investigating the same criminal offense.

**Data Collection Methodologies**

Law enforcement agencies can rely on the abundance of methodologies on the requirements of information sharing. It is essential part of data collection is it ability identifying INFORMATION SHARING 7 any gaps during the investigation stage. As such data should be obtained through RANDs, focus groups, and interviews to ensure its credibility. Prominent conferences data such as IACA (International Association of Crime Analysts), or IACP (International Association of Chiefs of police) should give a guideline of problems law enforcements officers encounter. Furthermore, having this data at their fingertips gives them the opportunity to study the data that instigating the problem.

**Identification of Data**

The daily operation of law enforcement agencies reliance on technology is imperial investment. Law agencies collect vital information which allows them to identify a problem within the process, transport, or an infrastructure setting. The communication between officers and their superiors can be exhibited through strategic planning. “Sharing information to improve criminal intelligence serves first and foremost to increase knowledge available for decision making” (Brown, 2018). The concept of law enforcement agencies sharing information has always been used in the past among many agencies.

**Involving Key Personnel in Data Collection and Analysis**

The role of key personnel in data collection and analysis is an instrumental part of conducting research. One of the most influential roles they carry out is to provide data on their investigation operations. It is the responsibility of crime analysis unit to identify key suspects which is the backbone of any investigation. Other criteria during the collection of data will give investigators a possible image of a suspect. This data will assist commanders and crime analysts in understanding how to implement operations in investigations.

**Conclusion**

Law enforcement agencies are relying more frequently on criminal intelligence. An emphasis has been placed on criminal intelligence in hopes it will help to decrease criminal activity. Sharing information among law enforcement agencies appears to be an answer to in collecting data and information on criminal intelligence that law enforcement agencies have been embracing to combat crime. “In a world characterized by increasingly sophisticated crime, it is increasingly important to draw together the fragments of information available from multiple sources” (Brown, 2018). References Brown, R. (2018). Understanding law enforcement inf

**(Week Two) Benchmarking Best Practices for Information Sharing**

Criminal activity has become more modernize than in the past thanks to the increasing advancement in technology. Law enforcement agencies are at a disadvantage in combating crimes involving technology if they lack the appropriate approach. Thus, law enforcement agencies should be equipped with the sophisticated information technology to aid in their operational quests battle the growing technological threats. The use of sophisticated information technologies such as sophisticated information technology (SIT), computer-aided-dispatch (CAD), and record management systems (RMSs) each play a role vital sharing information for law enforcement agencies.

Sophisticated information technology mainly relies on computer-aided-dispatch (CAD), which aids in monitoring an agency’s call response histories for service, and record management systems (RMSs) which stores call histories. All levels of law enforcement agencies are distinct; therefore, they bare the responsible for sharing criminal justice information. Information sharing have impediments despite the efforts law enforcement agencies in the advancement in costly technology systems. Law enforcement agencies who are equipped with sophisticated information technologies helps them to hurdle barriers that prevent which allows officer to obtain vital information which propel them in making the appropriate call in the field.

**Identification of Program Goals**

Information sharing is beneficial to law enforcement agencies to implement because it advances the ability to make precise decisions and criminal intelligence. The central idea of sophisticated information technologies is to seek justice by identifying those participating in criminal activity. The capability of the program to expand sharing information to at risk communities’ agencies is of urgency because of their lack of resource constraints. According to Brown (2018), this necessary to prevent linkage blindness. Brown furthermore explains that linkage blindness was a causally relate to the events of 9/11 indicating “the 9/11 Commission in the United States, which found that a number of intelligence agencies held information on the activities of those involved but failed to connect the dots (National Commission on Terrorist Attacks Upon the United States 2004” (Brown, 2018).

Additionally, the implementation of intelligent systems such as RMSs and CAD is a matter of urgency to avail information to all agencies. Generally, improved IS between relevant jurisdictions enhances intelligence resulting in appropriate tackling of criminal acts. Another problem that information sharing will help support is confliction among LEA. On some occasions, multiple agencies unknowingly investigate the same group or individual, implementing the IS program results in saving resources and time for the concerned agencies. Centralized information depositories provide information for all agencies pursuing diverse criminals resulting in better outcomes. According to Brown (2018), “there is a positive correlation between the number of police agencies involved and the average size of a drug seizure.”

**Outcome Objectives**

As stated above the major failure of intelligence that led to the 9/11 attack was linkage blindness. The terrorist attacks on the USA resulted from combined cultural forces; there was enough intelligence to the imminent attack, partially held by local police, and another by top federal government administrative agencies. There is a rivalry concern of long-enduring low-trust culture among various LEA, especially between the CIA and the FBI. According to Pedro (2004), “political analysts have contended that feuds, turf wars, power struggles, and personality clashes have impeded the critical flow of information between and within these agencies for decades.” On some occasions, officers close unsolved cases prematurely, later resulting in catastrophic atrocities perpetrated by the same individuals. The consequences of linkage blindness can be addressed by implementing RMSs and CADs, to avail information of conspiratorial rehearsal for future crimes (Pedro, 2004).

According to UNODC (2011), “The effective use of intelligence is crucial to a law enforcement agency’s ability to combat criminal groups.” Understanding the targeted population or individuals helps the agencies manage resources effectively. It helps develop strategic plans that help tackle current crimes and prevent future anticipated crimes. Criminal intelligence analysis helps agencies establish an appropriate pro-active response to tackle delinquency. Intelligence will enable the agency to understand identified criminal groups in the vicinity. Criminal intelligence is vital in assessing their current crime trends and plotting a trajectory of their future crimes –this helps the agency to hamper criminal development. An increase in crime has increased resource constraints requiring investigating officers to triage out cases, particularly those with lower risk. Sharing of information from earlier findings will reduce duplication of investigation events, such as revisiting crime scenes. To reduce fiscal constraints, a triage process is necessary to enable officers to prioritize serious criminal threats (Ratcliffe, 2016).

**Resources Needed to Implement the Program**

Implementation of the program will require the pulling of numerous resources to enable LEA to share information. The first and foremost resource required is IT infrastructure, such as centralized criminal justice repositories, especially on the cloud servers. RMSs and CAD software are other essential resources with their sharing standards. A functional data-sharing portal through the website, which will be used to access information, is important to accessing repositories store on the cloud. The emerging technologies enable semantic tagging, which enables content characterization during storage to make it easy to retrieve when searched. With the cutting-edge technology, devices such as smartphones, tablets, which are an important part of life, will be able to access the database.

Law enforcement officers will have access to information in the field using their phones, or tablets. According to Jakkhupan and Klaypaksee (2014), “for the police duty, the record of the crime location is important to reveal the distribution area of crime, which can be used to analyze and plan for the future crime prevention.” The law enforcement officers will require sophisticated capabilities time series analysis or crime mapping analysis while in the field tracking suspects. Network connectivity enables other agencies to access shared information, which creates an information exchange “free market” for all relevant entities. Using the collaborative-network model promotes a more active engagement and interaction among involved agencies sharing information (Brown, 2018).

**Eliciting Stakeholder Participation**

It is imperative to facilitate the involvement of stakeholders in program planning and implementation. Numerous steps should be considered to encourage stakeholder engagement and better project outcomes. Community consultation to understand the existing networks already in place, reaching out to facilitators and leaders in the community will create an acceptance culture. Creating awareness of the proposed program to stakeholders will improve their interest in the program proposal. Stakeholder’s participation in a meaningful way requires sufficient background information and knowledge.

It is significant to identify community champions to encourage participation among members. Apart from using appropriate language in consultation, it is also important to seek approval from stakeholders with sincerity. Using many channels to promote consultation will ensure relevant participants are well informed of the change proposal. Likewise, as the integrity demand, “meaningful engagement requires trust. Say what you mean; mean what you say.” (SustaiNet Software, n.d)

**Conclusion**

There are more benefits in improving LEA’s information sharing in improving intelligence to tackle sophisticated criminals. Likewise, there are more hurdles to improve IS flows, understanding sharing mechanisms, connectivity, and levels of interaction will help close the loopholes. As Hollywood and Winkelman (2015) believe, “implementation of RMSs and CADs is intended to help move agencies from “why can’t we know?” to “we do know.” Improving law enforcement intelligence through information sharing is the key to minimizing crime and avoiding disastrous outcomes.

**(Week Three) Information Sharing Proposal**

In the modern world, there is a rise of data sets “big data”, which exceeds the capabilities of traditional database applications. Most evidence stored is in form of digital pictures, videos, and text files, the evidence includes digital evidence repositories, stationary or mobile videos, offender registries, license plate hits, call records, cases, and police or offender tracking records. Criminal networks exploit information sharing loopholes, and limitations to further their agenda, especially in small agencies**.** “Law enforcement information sharing involves two broad categories, first is fusing data, such as video feeds, sensor feeds, external records collections, and social media data used to make predictions and search patterns” (Law Enforcement Information Sharing). Second, transaction or exchange data, such as routine dispatch requests, calls for service, and querying a database for crime incidents. The proposed information sharing will address both the categories of information sharing across relevant law enforcement agencies (LEA).

**Target Population**

The proposed criminal record management systems (RMSs), and computer-aided dispatch (CAD) is in the perspective of the Criminal Investigation Division (CID), and Crime Scene Investigation (CSI) units. It will improve the LEA intelligence in combating crime across diverse agencies. The program proposed will provide all relevant law enforcement officers (LEO), and federal authorities to update and access information in centralized CADs and RMSs. The LEO platforms will allow them to query the website for information related to the case investigated, such as the suspects, fingerprints, DNA, criminal group geographical area, footprint, Alias names, tattoos, and physical descriptions. The CID handles various investigations, including criminal records, passports, fingerprints, and immigration status.

Equipping the CID will provide vast intelligence that may promote predictive policing. According to UNODC (2020), “the goal of the Criminal Investigation Program for Somalia is to enhance the investigation capacity of the Somali Police Force.” The targeted population was singled out through literature research for their needs to improve CID departmental intelligence. CID and police forces have a growing need for crime intelligence, and LEO requires empowerment to enable them to acquire capabilities to combat crime. The UNODC ongoing program aims to help federal and state governments to improve the capacity of specialized investigators. The effort to empower LEO by UNODC is a clear indication of the lacking information sharing loopholes of the investigating unit across the globe (UNODC, n.d).

**Policies, Procedures, and Job Descriptions**

Policies and procedures are an essential element in empowering and equipping LEO. The officers must investigate organized and serious crime as guided by international standards and treaty obligations. In the RAND corporation project, “priority criminal justice needs initiative” various policies and procedures are necessary for developing-sharing RMSs and CAD, which has substantial progress to establish standards for infrastructure. Global reference architecture (GRA) and compliance testing initiative by the IJIS Institute’s Springboard is among the guidelines for implementing the program (Hollywood & Winkelman, 2015).

According to IJIS Institute (n.d.), “Information sharing in justice, public safety, and homeland security organizations is mission-critical.” Likewise, complying with National Information Exchange Model (NIEM) will be equally important in the implementation of RMSs and CAD. NIEM connects entities sharing information to facilitate their agendas. According to NIEM (n.d.), “It lets your system and my system speak—even if they've never spoken before—by ensuring that information carries the same consistent meaning across various communities.”

Additionally, the new Standards Coordinating Council (SCC) and Program Manager, Information Sharing Environment (PM-ISE) has created the organization’s standards meant to coordinate governance activities and standards prioritization (Hollywood & Winkelman, 2015). The LEO involved in maintaining law and order, include detectives, police officers, special agents, game wardens, state troopers, sheriffs, criminal investigators, and crime scene investigators.

The core job description of LEO is to protect citizens through enforcing the law, preventing crime, apprehending suspects, and investigating a crime through interviewing witnesses and victims, gathering crime scene evidence, and interrogating suspects. The LEO prepares detailed observation documentation and actions by completing reports and radioing information to arraign the suspect(s) in court. The standards provide information sharing platform accepted standards.

**Necessary Pertinent Policies, Procedures, and Job Descriptions**

In the implementation of the LEA information sharing proposal, various procedures, and policies are vital to ensure the program meets international standards. The proposal to implement RMS and CAD for law enforcement must comply with IJIS Institute accepted information sharing standards. “NIEM provides vocabulary efficiency reference for diverse information exchange for private and public organizations” (NIEM). The standard enables the exchange of information among a community of people to facilitate advance agendas.  The initiative by the SCC provides principles for information interoperability.

The program will require both SCC and PM-ISE policies in information sharing. Both standards promote ISE between private, state, local, federal, and tribal agencies with common goals for domestic nexus of public safety and national security (SCC, n.d). The main job description is to prevent crime, enforce the law, and provide vital information that averts disastrous actions. The standard ISE-I2F (information interoperability framework) is designed to assist with sharing of information for national security and public safety mission across territories, local state, and federal agencies (SCC).

**Interagency Collaboration**

Collaborative efforts are necessary means of sharing information, mobilization for disasters, and combating terrorism. Interagency collaboration is involving more than one LEA in operational planning or law enforcement operations that cross the criminal justice system or geographic boundaries. The collaboration among LEO usually attracts unique identity, such as law enforcement councils, task forces, data-sharing networks, and partnerships, with a common mission, to protect citizens, and enforce the law.

The 2001 terrorist attack ushered a new era, robust approaches has been developed in threats assessment, share information, and gather intelligence to reduce vulnerability, and developing crisis intervention strategies. According to Sedgwick and Hawdon (2018), “it is clear that this approach is to be achieved by interagency cooperation and coordination, especially in terms of information sharing.” There is a need for every LEA to be on board to share vital information with counterpart agencies if the information is intended to avert a disastrous crisis. The success of maintaining “law and order” is for all levels of LEA to rely on interagency and intergovernmental collaboration (Sedgwick and Hawdon, 2018).

**Program Implementation Plan and Timeframe**

Implementation of an information-sharing proposal will provide LEA means to share vital information across multiagency. Acquiring necessary resources for the implementation of RMSs and CAD proposed program is the program’s priority.  A systematical structured standard software implementation approach will be used to effectively integrate RMSs and CAD software-based services into existing end-user infrastructure. Acquiring off-the shelves RMSs and CAD, such as N-DEx and NCIS, and sharing with regional existing repositories is significant for the implementation of the proposed program. Training key personnel on how to utilize the program will improve the reliability of the proposed program. Key personnel to be trained include, investigating offices, detectives, crime scene investigators, and relevant stakeholders.

**Training Requirements and Materials**

It is important to train the targeted population on key elements of implemented software. The solid change for the new program requires all relevant personnel to receive need to know the system training. The primary requirement is to induct key personnel on how to access the system portal from their devices. The materials necessary include, system portal documentation, flyers, connectivity gadgets. A well-developed presentation will aid in the demonstration of the uses of the implemented program. Capitalizing on the software free training mode for practice will be essential to maximize the impact of training. According to Roner (2019), “Many Saas and other technology providers have free training programs that walk people through how to use every aspect of the software.” It will be crucial to demonstrate the proper ways to utilize RMS and CAD, both for uploading and accessing information.

**Conclusion**

Information technology allows for law enforcement agencies to provide a sturdy improvement on its development and design to acquire the best information sharing approaches. With constant training and implementing polices helps to secure a safer environment for law enforcement agencies. “A strong foundation already exists to support the inclusion of information sharing as a fundamental component of justice reform and justice reinvestment” (Came). A macro level of training law enforcement agencies on specifics of the use of information sharing in the field and how to effectively rely on the information to their command office.

**(Week Four) Information Sharing Proposal**

The proposed information sharing (IS) program is aimed at addressing the shortfalls of IS across involved law enforcement agencies (LEA).   The proposed computer-aided dispatch (CAD) and criminal record management systems (RMSs) will provide the Crime Scene Investigation (CSI) units, and Criminal Investigation Division (CID) IS capabilities. The stored information will enhance the LEA intelligence in tackling diverse crimes. The IS platforms will avail information on all investigated and logged in cases, such as the suspect's territory, DNA, fingerprints, Alias names, tattoos, associated criminal group, footprint, and physical descriptions. The CID deals with numerous investigations, including fingerprints, passports, criminal records, and borders.

**Project funding**

Funding is one of the biggest administrations’ nightmares in law enforcement, particularly handling the budget. Most of the projects are meant to implement new ways to provide safety needs of the growing population. A wide variety of both public and private entities exist to offer grant funding to state, tribunal law, and local law enforcement in projects, including hiring, equipment, vehicles, and technology programs. The Department of Justice empowers the funding for information sharing provided by federal funding. The funding covers an array of training, victimization programs, enhancement programs for different sectors of the criminal justice system. The funding is based upon a tier of three grant-making factors.

Operational cost will be funded through the state funding, particularly the criminal justice agencies. According to COPS (2020), “Each state and territory also receives an annual Justice Assistance Grant (JAG) from the U.S. Department of Justice’s Bureau of Justice Assistance, which is available to local and state agencies.” Likewise, occasionally the law enforcement agency receives grants from the association, corporate, and utilities, which is set aside for safety equipment, security operations, and tailored law enforcement needs. For example, The Spirit of Blue Foundation Safety Grants assist law enforcement raise funds for training, essential resources, and equipment channeled through participating sponsors (COPS, 2020).

**Evaluating the Success of Your Program**

There is a need to focus on the outcomes of the program that successfully contributes to the LEA strategies and objectives, such as the criminal justice system, violent crime, and drug control. The main aim of the evaluation of the program is to locate loopholes for further development of similar projects in the future. Continuous evaluation is essential, documenting every stage of development and implementation. Project performance evaluation is the basis for the final assessment, which is impact evaluation.

Conducting impact assessment will provide useful information for policymakers to implement. It provides the local, state, and federal officials crucial information to be used in decision making. Therefore, an evaluation will be done continuously to ensure it provides an appropriate framework. At every stage, a systematic assessment is conducted to identify if the program meets the objectives, if not recommendations are provided for improving LEA intelligence in combating crime. Generally, the evaluation will assess the outcomes and the impact of the program in enhancing criminal intelligence.

**Data Collection Methods**

There is a need to focus on the proper data collection methods because generated data is expected to give an accurate trajectory of the program. Data collection for the evaluation process is significant to ensure the program meets its objective. The data methodology to be used will involve both quantitative and qualitative techniques.  The key findings will be if the IS has improved CID intelligence, in isolating noise from useful information to enhance the intelligence of investigating officers. Likewise, it is essential to find out whether the intelligence from the program has improved the knowledge of the officers in mapping and analysis of criminal groups.

Quantitative data will be collected through a departmental questionnaire, to be availed to key personnel in their respective departments. Focus discussion groups will be employed to collect qualitative data from CID officers. According to Paradis et al. (2016), “ideally, they are used when the sum of a group of people's experiences may offer more than a single individual's experiences in understanding social phenomena.” The method will provide clarity, extension, and challenge quantitative data collected. A multipronged approach will be utilized to ascertain the validity of the data collected.

**Feedback and Respond Mechanisms**

Feedback and response mechanisms (FRM) are critical to project accountability and success. Robust FRM systems assist the concerned team to gather vital information from relevant stakeholders, to enable adaptation and improvement of the project. The project FRM promote accountability, it enables the concerned identify and respond to complaints, information request, and suggestions. Using the FRM flowchart to develop and implement the strong FRM is critical in achieving project objectives. The FRM flow chart will map several key elements. The first element is a specific feedback mechanism, defining how the feedback will be gathered. Another key element is assigning staff responsibilities, particularly those receiving the feedback. Likewise, it is important to outline how feedback will be processed, used, and documented. Lastly, is to lay down processes on how to report the feedback to stakeholders to act and for the decision-making process.

 FRM will be an integral part of the program implementation process, to enable the project team to receive feedback constantly and report to stakeholders. Providing meaningful, thoughtful, and timely responses to stakeholders demonstrates accountability and commitment to participation in project implementation. The most appropriate FRM approach for the IS program is phone calls and long-form base surveys. Log form-survey through emails will be used to collect feedback from registered officers in the system. Likewise, frequent phone calls from relevant end-users (officers) will provide credible feedback about the program. According to Hiver “the key here is to focus on the users who can give you the best feedback to improve your product or service.”

**Conclusion**

Even though, there have been groundbreaking success in the criminal justice regarding information sharing more practices and training is needed to reassure that previous barriers on information sharing have been minimized. “Today’s dynamic operating environment challenges federal, state, local, tribal, and private sector partners to continue improving information sharing and safeguarding processes and capabilities” (Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding, 2013). Law enforcement agencies alliance have evolved with the sharing of information, thus, creating measurable preventive measures against threats. It is critical that law enforcement agencies maintain the best practices of sharing information and continuing strategies to seek the efficient outcome.

.

References

Brown, R. (2018). Understanding law enforcement information sharing for criminal intelligence

purposes.

Hollywood, J. S., &amp; Winkelman, Z. (2015). Improving Information-Sharing Across Law

Enforcement: Why Can&#39;t We Know?. Rand Corporation.

Jakkhupan, W., &amp; Klaypaksee, P. (2014, August). A web-based criminal record system

using mobile device: A case study of Hat Yai municipality. In 2014 IEEE Asia Pacific

Conference on Wireless and Mobile (pp. 243-246). IEEE.

Pedro, R. E. (2004). Policy and procedure as a prelude to peril: Linkage blindness, cultural

lag and the terrorism of 9/11. The University of Southern Mississippi.

Ratcliffe, J. H. (2016). Intelligence-led policing. Routledge.

SustaiNet Software (n.d). How to Encourage Stakeholder Participation. Retrieved from

https://www.sustainet.com/how-to-encourage-stakeholder-participation/

UNODC. (2011). Criminal intelligence: manual for analysts. Retrieved from

https://www.unodc.org/documents/organized-crime/Law-

Enforcement/Criminal\_Intelligence\_for\_Analysts.pdf