BEST PRACTICE GUIDE

Situational Awareness

BEST PRACTICES GUIDE FOR SITUATIONAL AWARENESS

About This Document

This Best Practice Guide is designed to support situational awareness application selection and deployment by public safety agencies across the State of Minnesota. It is vital for agencies embarking on acquiring situational awareness tools to **engage with your user groups and stakeholders to understand their needs upfront and to integrate them into the solution architecture**. The guide provides key factors to consider in your decision making and planning. Knowing what factors to consider and what requirements your users and experts have will help you make the best decision for your agency, regardless of your agency's unique requirements. The guide also includes questions to pose within your agency or to prospective vendors to provide you a comprehensive understanding of your needs and the available solutions.

Introduction

The *Minnesota Wireless Broadband Data Use and Application Survey* conducted by the State in early 2020 identified substantial interest in situational awareness. Representing approximately 300 agencies and departments, the survey found that more than 54% of respondents require and currently lack situational awareness capabilities. The gap existed across all primary disciplines: law enforcement, fire, EMS, PSAP, and emergency management. Additionally, 48% of respondents indicated that they want to share situational awareness information. During the initial interview conducted in January 2020, stakeholders identified an interest in developing "standard" data sets to create a common operating picture among neighboring jurisdictions and first responder agencies.

However, this baseline gap provides only a high-level understanding of the solutions to unmet common operating needs. The term Situational Awareness means different things to different people, depending on their job function and the situation. Clearly, the "situations" differ, and the associated information to provide awareness differs for every situation. And, depending on your incident preparedness and response role, your needs for information can vary widely. Importantly, the existing information and public safety information sharing systems for each agency can vary widely. Some may have existing video camera feeds, others may have information available from their Computer Aided Dispatch (CAD) system, and others may have a variety of real-time mapping information that can be integrated into a situational awareness solution. As a result, depending on the specific needs of your agency, the tools you need to acquire to achieve your situational awareness goals can vary widely. To support agency specific needs and objectives, this guide provides a broad view of what your situational awareness goals may be, the kinds of systems you may need to integrate with to achieve your situational awareness

goals, and also addresses ideas regarding general operational and deployment considerations that are largely independent of what you want to achieve.

However, this guide does make one critical assumption about the types of situations public safety agencies may encounter: it focuses on the needs of day-to-day incidents. Other tools are available for public safety agencies to manage large-scale crises. For example, WebEOC is a Crisis Information Management Software (CIMS) that provides incident management capabilities, including situational awareness, event reporting, and resource management. In fact, 29% of those survey respondents who indicated they already have a situational awareness tool identified WebEOC as their application. WebEOC allows for resource requests and task assignments to be submitted at the emergency operation center (EOC) or in the field using a mobile device. Information management features can be used to track files, contact information, plans, procedures, and compliance reporting. Fortunately, the State of Minnesota maintains a statewide license for WebEOC and it is a solution that is widely used and available at no cost to qualified Minnesota agencies to help agencies statewide coordinate, collaborate, and manage major incidents.[1]

As a result, we assume that large-scale EOC type situational awareness can be achieved throughout the State with WebEOC. Agencies who have such situational awareness needs should use the State's WebEOC platform. For the purpose of this document, we interpret the primary gap in situational awareness to be at the individual incident basis – before the Emergency Operations Center is activated, if activated at all. Therefore, this guide will focus on situational awareness at the field level, and address information needs from the initial stages of the incident for law enforcement, fire, emergency medical services, 9-1-1 centers, and emergency management incident managers. Importantly, because the information needs are immediate, it is critical to pursue existing information sources from up-to-date systems to provide your situational awareness.

And to that end, it is critical to understand how important your Computer Aided Dispatch (CAD) is with regard to situational awareness. The CAD frequently contains critical situational awareness information such as unit locations, unit status, incident location, and incident status information, among others. These four elements are often thought to be some of the most important pieces of information for most incidents. Generally, this information is shared within an agency, and frequently, the information is available to personnel in the field via mobile applications. In many circumstances, CAD software can integrate map information such as road closures or hazards to provide additional situational awareness to personnel at the incident and operation centers. Consequently, your CAD may provide a substantial portion of your situational awareness needs. Or, if your primary gap is regarding CAD based information with your mutual aid partners, a CAD-to-CAD interface may facilitate the majority of your needs. This factor underscores that for situational awareness projects, it is critical to engage early with your stakeholders regarding their specific needs and to engage with your CAD vendors to understand how your existing platforms can achieve your situational awareness goals and objectives.

[1] To become a user on the State of Minnesota WebEOC platform, email your request to HSEM.WEbEOC.Tech.Support@state.mn.us, or contact the Emergency Manager for your county.

Before you embark on your quest to secure situational awareness tools and capabilities, we recommend that you consult various expert resources available to get started. There are a number of specialty resources that agencies can leverage to support their situational awareness objectives.

- The Minnesota Geospatial Advisory Council's Emergency Preparedness Committee (EPC) is Minnesota's principal organization for promoting, coordinating, and standardizing GIS use across all levels of the state's Emergency Management community. The Committee's mission includes facilitating relationships between the geospatial and emergency community as well as to increase awareness regarding opportunities to leverage geospatial technology to enhance emergency management. The Committee creates "Tiger Teams" to address specific objectives regardless of the size or the scope of the work. It is possible that your geospatial needs could be addressed in collaboration with the EPC.[2]
- The Minnesota Geospatial Commons provides a catalog of data which can be used to advance situational awareness. The catalog is available at https://gisdata.mn.gov/group. The Commons provides access to data and web applications that agencies may find useful for their solutions. MnGeo will also host geospatial data sets that could become part of your situational awareness solution. The State of Minnesota also has county and city GIS contacts that can help with your project.[3]
- The Homeland Security Information Network (HSIN) is an information sharing system for federal, state, local, and tribal homeland security data. It includes geospatial services, event and incident management, secure messaging, and other capabilities to manage operations and coordinate events. HSIN includes a DHS Common Operating Picture (DHS COP) Application that provides situational awareness available to public safety users at no charge; however, access to DHS COP may be limited. This application may provide you with ideas regarding datasets and systems with which to interface, or independently, it may fill a void on a limited budget.[4] Another federal resource is the Homeland Infrastructure Foundation-Level Data (HIFLD), which contains a catalog of geospatial datasets that may also be helpful. A private site with sensitive and potentially useful information is also available.[5]

Because the goals, objectives, and solutions could vary so widely, the Wireless Broadband and Applications Committee (WBAC) recommends agencies reach out to the vendor community to understand the types of tools available. This strategy will provide agencies with a frame of reference to identify features and functionalities required in the solution procured by their respective agencies.

[2] See https://mgacepc.org/ for more information.

[3] See Minnesota GIS Contacts (state.mn.us) for more information.

[4] To join HSIN or find out more about how it can help your operations, visit Homeland Security Information Network (HSIN) | Homeland Security (dhs.gov).

[5] See HIFLD Data Catalog | HIFLD (dhs.gov) for more information.

Functional Requirements

It is critical that you engage early with your stakeholders to understand their situational awareness requirements and gaps. The solution must provide the functional capabilities and information required to enhance their situational awareness and enable timely and informed decisions to address emergency situations. The solution needs to provide the necessary data and the means (software and hardware) to consume the data when needed, where needed, and how they need to consume it. It may also involve unique functionality, such as delivering customized information to the user's attention through a visible or audible alert. Conducting an exercise where you identify and map stakeholders (users/roles) to functional requirements is often helpful in gaining understanding of these requirements.

Situational Awareness Information

Situational Awareness means different things to different people, but at the minimum, it must provide the ability to identify and process the information critical for making informed decisions during an incident. The proliferation of broadband networks, powerful mapping capabilities, video sources, sensors and other technologies (such as CAD add-on tools, asset tracking of personnel, and inventory) have dramatically expanded the types of information available to enhance the common operating picture. The following table provides a sampling of situational awareness data sets, and examples of specific data sets in each type:

Text	GIS	Video	Images/Files
• Personnel info • Unit info • Incident info • Criminal data • Motor vehicle info • Information from news media and social networks	• Unit/Personnel locations • Road/traffic information • Incident information • Weather • Sensors (e.g., gunshot) • Critical infrastructure and assets • Assignments	• Traffic • Drone • Building • Bodycam	• Building plans and Pre-Plans • Suspect photos

This information can be contained in a variety of forms or formats. Video content can be contained in a video management platform or can be made available for streaming in a web page, and the video can use either standards-based coders or proprietary technologies for encoding the video content. Text can be housed in a database or be contained in open formatted messages. GIS information can be maintained in open geospatial databases or formats or in proprietary file formats. If all of these information elements need to be aggregated into one application to provide comprehensive situational awareness and a common operating picture, integrating these disparate information types from multiple sources must be meticulously managed.

Whatever data the Situational Awareness solution is intended to share, the agency should take multiple factors into consideration. Each situation drives its own data needs, as illustrated in the table below. You should engage with your end users early in your process to fully understand what information and alerts are required. The following table provides a sample of data elements for two incident types:

Situation	Data Sets	
Building Fire	• Unit/personnel locations (branch/division/sector) • **Personnel status / biometrics** • Building / Body / Dash / Drone video • Pre Plans - Building floor plans	• HAZMAT data • Map: Hydrant/standpipe, ventilation, staging areas, helicopter video • Weather/wind speed and direction
Active Shooter	• Unit/personnel locations • **Personnel status / biometrics** • Traffic camera video • Building / Body / Dash / Drone video	• **Gunshot sensors** • **Video analytics sensors** • Building floor plans • Criminal records • Map: Perimeter, entrances/exits

Data types in **bold** may require an alerting mechanism to direct the incident commander's attention to mission critical information. Your analysis should explore which agencies, and groups within agencies, need access to the information. Your investigations may expose important decision-making needs for other support agencies for certain information.

The situational awareness information may be static, or it may be dynamic or real-time (i.e., the data may be modified or updated over the course of the incident). Agencies should consider if real-time information is needed, and if so, how often the real-time information is refreshed. If the information is delivered from a third-party system, and especially if it comes from another agency, the source of the data, and the need to provide updates, will become a key aspect to your planning.

You should also understand whether the data flows are unidirectional or bi-directional. Will the data only flow into the situational awareness solution, or does specific information need to be shared with other third-party systems? For example, does the solution only need to provide maps for road-closures from a third-party system, or are inputs to the road information database based on feedback from field users required. The latter dramatically complicates the solution and requires the third-party system to support Application Program Interfaces (API) or the equivalent.

Ultimately, the type of information needed in your situational awareness solution will drive the interface. For example, if the information includes geospatial information, the solution will need a mapping component with various features to allow the user to focus attention to a location. If incorporating building data, a simple PDF viewer may suffice, but may also drive additional viewing requirements such as an indoor GIS interface that shows real-time personnel locations and allows for queries of different map layers. The information requirements may also define the type of devices required. For example, if the form factor of a smartphone will not support the volume of information needed to provide the appropriate common operating picture, larger form factors, such as tablets or personal computers may be required.

User Functionality

The situational awareness solution should provide the required features and include a client application that is user friendly, with an intuitive interface. Request a demonstration and pilot the situational awareness applications with stakeholders from your various user groups. These demos and pilots will help your stakeholders better understand the capabilities of the platforms and gaining insight into the solution will address the essential situational awareness gaps. This is also an opportunity to gather and record a list of required and desired functionalities (feature sets) for situational awareness capabilities.

The situational awareness platform must provide agencies the ability to obtain the right information at the right place and time from disparate sources, to process the data into logical outputs, and to share those outputs with users so they can make informed decisions. For the solution to be effective, it must convey decision-facilitating information in an easy, intuitive way. It should deliver information that is germane for each incident type, and it should be customizable (i.e., user-defined filters) to deliver information for each job function and discipline (e.g., law enforcement or fire). Overloading the user with data and making it difficult to find and organize lifesaving information is counterproductive. To prevent this, data should be prioritized based on the mission type and focus.

Ensure that the situational awareness application functions alongside other primary applications installed on their devices. For example, can the application be configured to provide the user with both situational awareness and CAD information at the same time on the same display? You will need to verify that it can coexist with all other mission critical applications operating on user devices and that they have the processing and storage capacity to support operational requirements without degrading performance.

You should understand the immediacy of the information required by your users. It is important to know what information is needed, and when it is needed. This may require automatic data set updates and may dictate what information must be provided in real-time. Importantly, there are limited resources to create (or enter) data in real time during an incident, and your user functionality requirements must investigate how information will be obtained, who possesses the information, and how it can efficiently and quickly be delivered in a single common operating picture to end users.

As was addressed in the basic application guide, your solution should address the user requirements for mobile use scenarios. Specifically, if the solution must be available where there is no or limited wireless coverage, it may require that data be downloaded to local client machines prior to arrival at the event. And likewise, user actions on the client application may need to support uploading of information when service becomes available.

Finally, consider your users' notification or alert requirements. Public safety applications need to make it easy for users to quickly receive lifesaving information. Notifications are a preferred method for your users to become immediately aware of critical information. The items in bold in the table above are examples of information that may be desirable to have associated notifications. You may also want to create geofences that alert users when certain assets or personnel enter a region or area.

Administrative Functionality

It is important to engage with those users who will be administrators of the system. When considering agency administrator requirements, focus should be given to the following:

- User accounts and access privilege management,
- Use of the tool to conduct audits or after-action reports,
- Ability to generate usage reports, monitor user needs and issues, and
- Responsibility for policy compliance.

Administrator needs may dictate your solution's functionality and you should ensure that those functional requirements are documented and delivered by your vendor. Administrative requirements may include user access levels, groups and the ability to up-lift users and groups to higher access levels. Likewise, agency specialists who are responsible for IT system administration must also be engaged. They may have particular requirements for monitoring interfaces to ensure that the system is operating properly and that the application updates, expands access to new data, and that the information is continuously shared as planned.

Interoperability and Integration

Interoperability is likely the cornerstone of your situational awareness solution. As discussed above, it is likely that most of the data in your situational awareness solution is contained in third-party communications and information systems. Some of these systems may be under your control, while others may be under the control of other agencies or third parties. It is critical to determine upfront what systems or data sets the situational awareness tool will interface with or need to consume. Once your users' information and functionality needs are identified, the assessment plan should consider:

- How the new system will access the required information.
- The steps necessary to achieve cross agency, cross system and application data integration. It is important to identify how often (e.g., annually, monthly, weekly, daily, or in real-time) third party data sets will be consumed and how to reach agreements for accessing third-party data providers.
- The technologies or formats that are needed for integration and interoperability.
- The roles and responsibilities of the various parties that make all the interfaces and integrations operable.

Inter-System and Data Interoperability

Data interoperability provides your situational awareness software platform the ability to receive and understand data generated by different software platforms. Achieving this level of interoperability requires a common set of definitions for the types of data and a data exchange standard. A data exchange standard generally includes a data dictionary that provides definitions of the data parameters included in the standard. There are multiple industry accepted data exchange standards for public safety information that may be used to achieve data interoperability. Many of these standards are based on the Extensible Markup Language (XML) which is one of the most common data sharing structure. The Emergency Data Exchange Language (EDXL) standard provides emergency message formats including a Common Alerting Protocol. The National Information Exchange Model (NIEM) is a reference model

based on XML and includes structured data elements in Emergency Management. The Emergency Incident Data Document (EIDD) is also XML based and is intended for sharing among Next Generation 9-1-1 systems. There is also the National Fire Protection Association (NFPA) 950 for structure fire-related data including geospatial data. Where possible, it is a good practice to use open standards. Unfortunately, there is minimal support for many of these standards in today's tools; however, with customer demand, that could change. In order for two disparate system to interoperate, they need to contain the data elements desired for sharing, and they need to be able to exchange the data. Standards are ideal, but the solution could also use translations and other techniques such as Application Programming Interfaces (API), mentioned below, to share the information.

There are potentially other open formats and standards that could be leveraged as part of the overall solution. For example, geospatial applications could create or use ESRI file formats to facilitate information sharing. In fact, most jurisdictions standardize on ESRI and your GIS department can likely produce a wide variety of GIS data layers in this format if your situational awareness vendor supports it. In addition, applications can exchange information through an API. The API defines how one application can request another application to provide certain information in a consumable format. The API could be customized based on your unique needs, or your vendor(s) may have standard APIs that could be reused to share or consume different data associated with your needs. It is highly likely that due to the lack of interoperability using open standards, employing APIs to achieve inter system interoperability will be essential.

The functional requirements must also define whether the information sharing is unidirectional or bi-directional. For example, if the requirement is that existing system information must be delivered to a new centralized data hub, that unidirectional flow of information is less complicated than a bi-directional flow of data between systems. If your situational awareness solution needs to provide information to other third-party systems, then those systems must also be configured to accept that new data. An example of this might be a situational awareness solution that ingests CAD data from your CAD and a neighboring jurisdiction's CAD system, versus a solution that enables both CADs to be updated in lock step. This bi-directional data flow could then allow your users and your neighbor's users to maintain the same CAD interface and to visualize information from your neighbor's CAD. Such a bi-directional flow of information is more complex but is often more desirable as it allows the use of your existing systems and interfaces to be able to be maintained and enhanced.

The evaluation of the required inter-system interoperability should take a comprehensive assessment of your existing systems and applications. Various systems may support a "click-to-talk" feature that ties into a push-to-talk application. In addition, your video system may also provide web links that allow third party video streams to be integrated into your situational awareness solution. Your GIS department is likely to have valuable existing content that could be directly useful and usable in your final solution.

Inter-Agency Interoperability

Generally, the greater the scale and complexity of the emergency incident, the more responding agencies and personnel required to effectively manage the incident. Larger scale incidents are more likely to require resources from additional agencies within the same jurisdiction or from neighboring mutual aid agencies, and with those resources, interoperable data sharing needs are amplified. In the

absence of reliable data system interoperability and the critical data supported by these systems, there is a greater risk of delayed and uneven distribution of the information to first responders. Effective inter-agency interoperability must be anchored on sound governance, policy, and data sharing agreements. If the situational awareness solution involves an inter-agency data sharing component, these requirements must be defined up front and collaboration with the affected agencies and jurisdictions will be integral to the planning process.

Your mutual aid partners should agree on what information will be mutually shared, with whom it will be shared, and what technologies or solutions will be employed to share the data inter-agency. As discussed above, you should inventory major types of data per discipline that are required to support situational awareness. For each data type that will be shared, your plan would address the technical, policy, and data governance implications.

As you seek technical solutions for interoperability, it is important to first investigate the capabilities of your existing vendors. CAD-to-CAD interoperability is increasing among current CAD versions which may allow neighboring public safety agencies, with common or dissimilar CAD vendors, to connect and share information with minimal effort. However, it is possible that one or more of the vendors may require an API to interface disparate CAD systems. Within these models, a direct interface with each CAD required to share data with may enable the use of one system platform to host a multi-jurisdictional CAD-to-CAD sharing network.

Under various configuration scenarios, the CAD-to-CAD capability may not support sharing all of the required data elements. Additional systems or interoperability hubs may be needed to share data that is not contained in the CAD or is otherwise not supported over the CAD-to-CAD interface. Furthermore, agencies with whom you need to share information may not operate a CAD, and your solution should address how these agencies will participate in your information sharing plans.

Security

The *Best Practices Guide for Basic Application Selection/Deployment* covers the core security requirements for data protection, authentication, and confidentiality. This guide focuses on the core security aspects that are particularly important for your deployment of a situational awareness solution. The security implications of a situational awareness tool that integrates several third-party sources of information can be complex. The system is only as strong as its weakest link, and a system that does not have the appropriate security infrastructure and policies can become a back door to create vulnerabilities in other accessible systems. The confidentiality of situational awareness data is of vital importance, and therefore, all systems, interfaces, user accounts, and data must be secured. Due to the critical need to maintain data security, which is a fundamental public safety industry requirement, you should consult your agency IT experts, or those of a trusted partner, regarding the complexity and risks associated with security.

It is important to recognize that situational awareness data is very time sensitive. Therefore, users cannot be added to confidential systems in real-time to avoid exposing security breaches. System users should be authenticated prior to obtaining access to existing systems and should have immediate access to critical information. Agencies might leverage existing Identity Credentialing and Access Management

(ICAM) systems to enable user access to the situational awareness common operating picture. The sharing of credentials between systems is known as a federated ICAM. This shared credentialing would facilitate operations and could automatically enable access to information when added to other systems.

In many cases, you may want to provide access rights to information based on an entire agency, or groups within agencies. In that case, the ICAM system will need to accommodate those groups and have the capability to associate each data set with the appropriate group – to become federated across agencies. In such cases, cross-agency groups may need to be coordinated. Most data owners will want to ensure that their data is only shared on a "need to know" basis and only during the relevant incident. Importantly, limiting shared data access may be required within individual agency departments. For example, the law enforcement special operations team in two jurisdictions may need to be specifically labeled for the sharing of particularly sensitive law enforcement information. Or, your solution may require the creation of groups based on rank, or even using National Incident Management System (NIMS) standard roles. In the best possible situation, where administrators and users have the utmost control over accessibility and confidentiality of the data, the access permissions could be policy or attribute based. For instance, an individual who identifies as having a role in a specific incident could be provided access to sensitive information about that incident. An individual's geographic location could also determine what information is shared. Most systems are not expected to support such advanced access control, but over time as public safety ICAM matures, systems may support these operational attributes. You should understand the access control capabilities of the various systems being integrated, along with the prospective vendors' situational awareness tools and evaluate their respective capabilities against your requirements.

In addition, specific data is protected legally by federal and state regulations. For example, the Health Insurance Portability and Accountability Act (HIPAA) policies protect patient data, and Criminal Justice Information Services (CJIS) policy protects federal criminal data. CJIS policy specifically requires policies to validate a requestor of Criminal Justice Information (CJI) before dissemination.[6] Other state or local level sharing policies or laws may also exist (e.g., the State of Minnesota statue on the treatment of law enforcement data available here: https://www.revisor.mn.gov/statutes/cite/13.82). Your information sharing mechanisms and confidentiality of data must observe these and all associated regulations. Also be aware of whether there are regulations or policies for data retention for your devices or applications.

It is important to understand the requirements and policies for access control up front to ensure that the solution adheres to them. And, as we will address in the operational factors section, your plan must include data governance to ensure consistent integrity within the information sharing program. Data governance is fundamental for ensuring that the data owner's requirements are constantly monitored and modified as necessary. Data sharing governance will also accommodate changes to federal, state, or local policies that may adapt over time. As public safety's use of data sharing systems accelerates, data governance will become more integral among the Minnesota public safety community. Information sharing governance will be essential for creating a program of ongoing trust among the

[6] See Section 5.1.1 of the CJIS Security Policy available here: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

agencies involved. Conditions for sharing may also consider dictating the types of access control requirements, such as multi-factor authentication. There is substantial nationwide work underway that may result in a national schema for federated ICAM and trust management that should be continually monitored.[7] This initiative may become a nationwide standard for federated ICAM and trust management making it easier for agencies to manage access to their information, and to become more comfortable with their trust relationships.

Due to the likely sensitive nature of the information contained in a situational awareness solution, all other elements of a sound security posture are critical. The systems should be protected from accidental disclosures of information, and the data should be encrypted at rest and in transit. As identified in the *Best Practices Guide for Basic Application Selection/Deployment*, your plan should address security policies and training to ensure continued availability and information security. But in particular, regarding the type of sensitive information frequently associated with situational awareness data, your efforts should be focused on the storage and data retention requirements of the information owner. This may be of particular concern if users can leverage personal devices to access situational awareness systems. The basic application guide also highlights the State of Minnesota IT Services (MNIT) information security policies and standards that are an excellent resource for IT security.[8] You and your IT Security support are encouraged to leverage these helpful tools.

Deployment Factors

There are a variety of general factors to consider, including the procurement process, policies and agreements that will affect the situational awareness client application's use, system deployment, and staffing impacts. These are discussed in the *Best Practices Guide for Basic Application Selection/Deployment*. This section highlights the deployment factors that are particularly unique or critical to the situational awareness tool implementation. Data inventory and acquisition, the interoperability data hub, GIS information, operational policies, data sharing agreements and others are particularly important and will require substantial attention during your planning and deployment process. Agencies should develop a detailed plan and checklist to ensure a successful deployment that meets their situational awareness objectives.

The deployment plan should start with the user agency requirements. As previously noted, situational awareness means different things to different users. The functional requirements section of this document provides recommendations regarding how to optimally document user requirements regarding situational awareness. The interoperability and integration section also highlight important documentation and planning activities for integrating with third party systems. Included in that section, you should identify what existing systems may have already achieved much of your situational awareness objectives. The plan should identify what neighboring jurisdictions your users need to share data with and their existing CAD systems. Inquire if any of those jurisdictions already have a CAD-to-CAD

[7] DHS SAFECOM has a major initiative to enhance information sharing among public safety agencies nationwide that is founded on the Trustmark Framework as a component in your ICAM solution. More information is available here: https://www.cisa.gov/safecom/icam-resources

[8] Policies and standards are available here: https://mn.gov/mnit/government/policies/security/

hub that could be leveraged for your objectives. This type of interface may provide most of the capabilities required for improved situational awareness.

One major deployment factor to consider is where to host the solution. As with the basic application guide, whether you deploy a system that is hosted inside your agency data center, or within the cloud, can have substantial impacts on operational costs. Importantly, if the system will store, even temporarily, third-party sensitive information, your mutual aid partners may have concerns about storing their information in the cloud.

The procurement of the situational awareness solution must carefully consider all of your functional and operational requirements. Because vendor capabilities may vary widely, it's possible that one vendor or system may not meet all requirements. Likewise, requirements that are extensive could limit the competitive space for your system. To maximize the number of bidders to your solution, generally articulate your needs and allow vendors to be innovative in addressing those needs. It is important to receive demonstrations and trials from prospective vendors to understand each solution's capabilities and limitations. This effort could have substantial impacts on the final configuration of your situational awareness solution.

New policies and agreements governing confidentiality and access control will likely be needed. It is recommended that your data sharing initiative, whether intra-jurisdictional or inter-jurisdictional, include a data governance body to guide policy and operations. The data governance body should be established during the pre-deployment phase to continually oversee the success of the data sharing initiative and to ensure trust, confidence, and that the required benefit is derived from the solution. New mutual aid agreements may be required or modified accordingly between agencies to control the sharing of information. For example, your planning efforts must address whether further dissemination of data is allowable beyond the existing group of agencies. Depending on the capabilities of the systems, it may become necessary to implement new user policies that further dictate the conditions for data sharing (who, when, and for how long). Ideally, the new system would integrate the new policies into the access control mechanisms, but dependence on users may be required to enact those controls through policy if the systems cannot support the level of necessary detail. During the deployment phase, you should develop the policies and agreements required to achieve the desired operational objectives of your system.

Integration with other systems will require substantial planning and testing to ensure all interfaces are properly designed and deployed and that the required data can be shared properly and securely. If the information flows are bi-directional, your testing and planning must ensure that both ends of the system are properly behaving and updating. System integration will require substantial up-front work and planning, among potentially multiple vendors for several integrated systems, even if expanding situational awareness beyond your own organization is not required. If it is required, the level of complexity of the deployment now requires the efforts of management and IT resources from the other agencies as well as additional vendors. It is important that you develop a detailed plan regarding the roles and responsibilities of each party in developing the integrated solution. During the deployment process, you should conduct periodic meetings to implement your plan among mutual aid partners, their vendors, and your vendors. The testing of the new system should include simulated incidents that

test all interfaces and data sources. You should check to ensure that data sets that periodically update are fully functional.

Invariably, your deployment plan must address training. Even if the situational awareness capabilities can be achieved through existing systems, you are enabling new capabilities from those existing systems or your existing capabilities will now be infused with third-party data. At a minimum, your users will need to be aware of the third-party data, its limitations, frequency of occurrence, source, and your organizational policies regarding that third-party data. The deployment plan should include training system administrators and operators who will be responsible to ensure continued operations, adherence to policy, and continued benefit of the system.

Due to the complex nature of information sharing, you should carefully plan for the staff resources needed to implement your system. Prior to beginning system deployment, carefully and conservatively develop a capital and operational budget to ensure that all parties are on board with the expectations and impacts of the system. These operational and funding elements are detailed below.

And finally, if your situational awareness solution involves new hardware or software, the plan should address those factors. For example, if you intend to deploy a sensor-based solution, new video cameras, firefighter biometrics and/or other features and capabilities, the testing, rollout and training of those systems must be managed as integral independent projects.

Operational Factors

The same operational factors apply as were identified in the *Best Practices Guide for Basic Application Selection/Deployment*. The hosting model, customer support requirements, and the lifecycle of the different application and systems all must be considered in your operational plan. However, the operational complexity required to sustain the situational awareness solution will be a factor of how many systems are being integrating into your common operating picture, how many organizations are part of the data sharing initiative, the number of third-party systems included, and the amount of customization required to achieve the integrated solution.

As discussed above, you should create a data governance group overseeing the sharing of your information among all parties. That body should be responsible for ongoing policy development, regulatory changes, system monitoring and maintenance, and other aspects of sustaining a multi-agency situational awareness and interoperability solution. Your operations plan should identify the roles and responsibilities of the governance body and should become an integral part of the overall operations plan.

For each system interface, your operations team will need to constantly monitor and assess proper system performance and operations. The underlying software for all components that feed into your system may change over time as new software versions are released. It is important that the operations plan ensures that the responsible interface leads are alerted when operational changes occur and that all affected parties are informed of the plan to maintain interoperability. And, importantly, these operational needs may drive specific vendor requirements. For example, all parties involved in the data exchange may need to require their respective system/application vendors to temporarily support key interfaces to ensure that the investment remains whole during the timeframe required to integrate a

new software version. Nonetheless, IT staff will need to monitor these interfaces and troubleshoot the symptoms when operational errors occur. Plan for resources to continuously monitor all system interfaces and to make necessary upgrades to maintain interoperability. The costs associated with managing and implementing your operational plan are addressed below, but it is important to make sure that your budget covers all the anticipated operational costs throughout the lifecycle of the new solution.

As the different systems in your situational awareness solution change, the training needs may also evolve over time. Whenever new capabilities are integrated, the training program will require refresher training to address the changes. If the governance body authorizes expanding the number of mutual aid partners into the common operating picture, and those groups introduce new data elements, specialized training will be required to raise awareness of the new information and associated policies.

Finally, due to the sensitive nature of much of your data, an annual system and vendor security audit should be conducted to ensure the integrity of the system and associated data. The audit will drive confidence in the overall system among all involved parties.

Financial Factors

The varied nature of what constitutes situational awareness information will also drive substantial variability in the financial operating picture for your solution. The types of data your users need access to and what they plan to share will impact operating costs. The shared data sets along with the total number of disparate system integrations, and the number of solution mutual aid partners also impact operating costs. As discussed above, your solution could be built and integrated into an existing CAD system or may need to be an entirely new system. As a best practice, you should approach this initiative with a full understanding of the capital and ongoing operational expenses associated with these new capabilities. Therefore, a capital and operational budget should be developed up-front to guide the effort and to ensure the ongoing continuity of operations. Because these initiatives frequently involve regional data sharing initiatives, those budgets should identify the costs associated with each agency's contribution to the solution and who will ultimately bear the shared costs (both the one-time costs and the recurring costs).

During the deployment phase, key considerations and elements that are integral to the system budget analysis, if applicable include:

- **Agency hosted data hub:** The budget will include system server hardware, software, analytic tools and the associated costs of designing, installing, testing and commissioning the solution. The onetime costs may also include the equipment required to create secure, encrypted, connections between agencies. If there are multiple agencies integrated into the information exchange, an architecture that has one entity provide the hub hosting services can reduce costs. You will also need to determine the costs to establish and maintain each connection to each system.
- **User devices:** If a cache of user devices must be maintained for use during an incident to access the system, a budget for these devices will be required. The cache may also need to have

commercial cellular network access capabilities and the cost of this service would also be required for the budget.

- **Training:** If you choose a formal training program, a budget for trainers and a plan to accommodate the downtime for operational personnel will be required.
- **Staffing:** The staffing plan should include project management time, together with the management time to create policies, plans and other upfront efforts. Governance will incur additional time and money for the agency. You will need to budget the resources to create and continuously update policies on the data sharing within your agency and the policies governing the interoperability with other agencies. For example, whenever a new data type is introduced to the situational awareness solution, access policies may need to be updated to specify who and when the data can be accessed, and the new interface(s) must be designed, purchased, and implemented. Even if you already have an existing team that can support the important role in helping coordinate interoperability initiatives in your region, the team may need to expand to sustain the additional level of effort.
- **One-Time Licensing Costs:** Your vendor's model may involve one-time licensing fees that place more of the financial burden at the initiation of your project. If so, make sure you budget for these one-time costs and any advanced features or functionality of all or a subset of your users.

For the operational expenditures, there are several other costs that need to be factored into the annual budget. Below are a variety of key costs to include in the operational budget for your situational awareness solution:

- **Per user licensing/subscription fees:** The solution provider may charge a monthly or annual subscription for each mobile or mobile support (e.g., PSAP or backend) user. Consider whether there are costs associated with uplifting users, temporary access or read-only access. Also be sure to account for whether extended contracts require an open purchase order. Your assessment should also address any special functionality for some or all of your user base.
- **Vendor maintenance:** This budget covers the annual solution provider vendor maintenance fee, including the costs to maintain the inter-system APIs. This cost may vary based on the number of interfaces the agency has with other jurisdictions and other internal systems.
- **Staffing:** If staff hires are required, or if existing employees' time is diverted to operations or provide ongoing training for your situational awareness system, these costs need to be quantified and integrated into the annual operating budget. Governance and policy updates will also require some additional level of effort from the system manager.
- **System hosting services:** Includes hosting costs if the situational awareness system is cloud hosted, regardless of whether it is under your own control or under the control of the solution provider.
- **Spare parts inventory:** If the server and hardware are hosted on your premises, hardware spares dedicated to your solution are required along with a budget to support equipment repairs and replacement. You may also need additional data throughput bandwidth and to maintain dedicated networking and security equipment that should be added to the operational hardware, software, and staffing budget.

- **System upgrades:** If your vendor provides upgrades or updates to the system and you intend to leverage these upgrades, your budget should include these costs.
- **System refresh:** How will you budget for refresh of hardware, including the user equipment and personnel to oversee configuration and distribution? If that is an operational cost, make sure that you include it in the appropriate budget.

You should develop and maintain budgetary management spreadsheets outlining your one time and annual costs to ensure the availability of sufficient budget to implement the solution and to sustain it to the appropriate level of service.