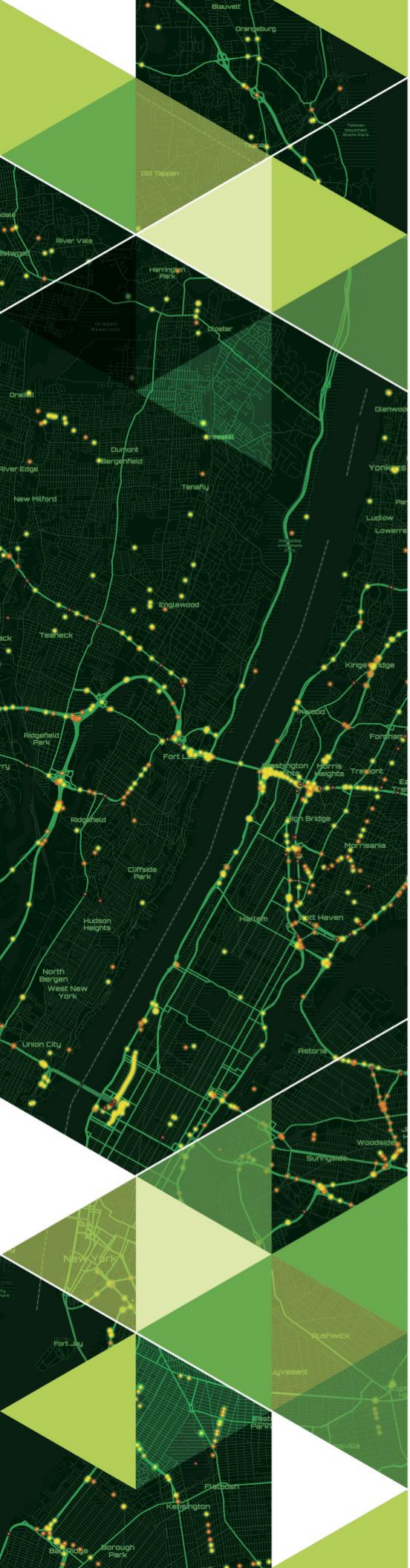

AN ESRI
TECHNICAL PAPER

January 2021

Site Security and Critical Incident Management: A Geospatial CONOPS

Managing Safe Campuses and Venues

380 New York Street
Redlands, California 92373-8100 USA
909 793 2853
info@esri.com
esri.com

esri | THE SCIENCE OF WHERE®

Copyright © 2021 Esri
All rights reserved.
Printed in the United States of America.

The information contained in this document is the exclusive property of Esri. This work is protected under United States copyright law and other international copyright treaties and conventions. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as expressly permitted in writing by Esri. All requests should be sent to Attention: Contracts and Legal Services Manager, Esri, 380 New York Street, Redlands, CA 92373-8100 USA.

The information contained in this document is subject to change without notice.

Esri, the Esri globe logo, The Science of Where, ArcGIS, Insights, StoryMaps, esri.com, and @esri.com are trademarks, service marks, or registered marks of Esri in the United States, the European Community, or certain other jurisdictions. Other companies and products or services mentioned herein may be trademarks, service marks, or registered marks of their respective mark owners.

Table of Contents

Executive Summary

Global events remind us on a routine basis of the perilous and interconnected worlds of site security and critical incident management (SS-CIM). From natural disasters to widespread occurrences involving active assailants motivated by political unrest, crime, or terrorism, these all reflect the heightened need for coordinated prevention and response capabilities to protect employees, elected officials, customers, organizational assets, and the public. Securing our critical facilities demands unprecedented coordination and access to all available information that can support prevention, provide the earliest indication of risk, and enable a more rapid and effective response. Access to up-to-date information requires close collaboration and data sharing agreements between a host of local, state, federal, and private security organizations. Geographic information system (GIS) technology is the platform that can unify this complex mission.

Security organizations have a responsibility to protect both lives and property during planned events and critical incidents. To succeed at this mission, organizations need to be able to

- Understand their operating environment.
- Anticipate threats and manage risk.
- Embrace a multiagency planning process.
- Deploy resources effectively.
- Establish shared awareness.
- Execute a coordinated response.

Security organizations have complex protection requirements when it comes to securing large-scale facilities and campus environments. These requirements do not stop at the walls of a building, campus, or adjacent properties. Security planners must address protecting an outer perimeter too, which may include parking lots, transportation hubs, commercial zones, and even neighborhoods. Additionally, security challenges increase when traffic and crowd movement flow are legally permissible.

Understanding the Environment Precedes Action

Only with awareness and understanding of the operational environment can security professionals effectively plan for and mitigate critical incidents; reduce injuries; and improve the safety of individuals, assets, and critical facilities.

By creating a digital twin of the built environment from building to community scale, SS-CIM provides the framework for fusing operational data—weather, social media, incident, and intelligence data—with foundational data. And to provide optimal visualization within buildings and across campuses, these foundational data and operational data feeds integrate with 2D and 3D facility and data models.

To align the many complex and overlapping security missions, SS-CIM must provide simple mechanisms for collaboration and data sharing between trusted organizations.

This entails locating and exploiting open access to publicly available data from government agency sources, social media, and third-party data providers.

Integrating information from multiple data sources, data types, and organizations with advanced maps and spatial analysis can only be accomplished through the effective use of GIS technology.

The Goal of This Technical Paper

This technical paper outlines a geographic approach to site security and critical incident management. This location-centric approach goes beyond using GIS to support common operating pictures (COPs) for visualization. This document chronologically aligns configurable security information products with internationally recognized best practices for facility security. When a location-centric platform acts as the unifying technology between security officials; security protocols; and varied, disparate data sources, organizations tasked with an SS-CIM mission can

- Collect, analyze, and integrate information for rapid analysis.
- Create repeatable and shareable information models.
- Reuse information and services across systems, organizations, and jurisdictions.
- Modernize risk, threat, and vulnerability assessments.
- Provide enhanced informational dissemination and reporting.
- Evolve the common operational picture to a common operational platform.

A GIS-Based Strategy Works

When it comes to SS-CIM, it is important to remember that all security issues have one thing in common—location.

Successful security strategies use geographic information as the foundation for integrating business intelligence across organizations. When location is a common identifier for different data types, workflows, and processes, key information can be integrated regardless of who owns it. In today's threat environment, it's important to remember that homeland security is now viewed as a much larger enterprise, where government agencies at all levels and commercial enterprises are required to collaborate and share. More than 85 percent of all critical facilities are owned by the private sector. As such, commercial security entities are now an integral partner in the homeland security enterprise.

Ensuring the protection and security of critical facilities involves an unprecedented partnership between government agencies and other security organizations. GIS technology is the unifying system that can guarantee success in today's fluid and complex security environment.

Why GIS?

Security personnel make it a priority to keep decision-makers informed, prevent incidents, manage responses to incidents, and quantify impacts when they occur. To achieve these goals, personnel must collect and process data from various sources for current and accurate situational awareness, then they must develop actionable processes and plans for prevention and response. GIS is a unique technology that excels in these areas.

GIS is a complete system that goes beyond powerful visualizations. It provides the ability to organize information as well as analyze and understand trends and

protection priorities in new ways. GIS also supports streamlined data dissemination. It is an effective tool for both internal and external communication.

Integrating structured and unstructured information, including sensor, imagery, social media, 3D, and video data, empowers security officials to fully analyze, exploit, and create actionable information out of raw data. As it pertains to the complex environment of site security and critical incident management, one GIS platform can support multiple missions.

Perhaps most importantly, GIS provides a common language and reference system for multiple disciplines and sectors, including private security, law enforcement, emergency management, intelligence, public health, and defense. It allows stakeholders to collaborate and make data-driven decisions.

ArcGIS is a system that evolves the common operational picture to a common operational platform.

SS-CIM Common Requirements and Best Practices

As with any iconic facility, event, or occasion that draws large crowds, countering terrorism, active assailant, civil unrest, and other mass casualty scenarios remain formidable challenges. Deployed technology must inform operations, counter threats and vulnerabilities, and align with industry best practices. GIS technology, when employed as the foundational security platform for SS-CIM, is best suited to manage these complex requirements.

A review of SS-CIM best practices from a variety of government and industry publications indicates that there are core best practices that need to be addressed. These include the following:

- Collaborative security and operational planning—Routine and for critical incidents
- Crowd control
- Critical incident response
- Vulnerability, risk, and threat assessments
- Disaster prevention through facility environmental design
- Modern command center
- Technology—Situational awareness, intelligence fusion, GPS tracking

This document does not intend to detail every best practice or security requirement. It should also be understood that each solution may not be applicable to every facility or incident. That said, when properly implemented, the configurable workflows contained within—in conjunction with other security procedures—can significantly work toward security organizations achieving their safety and security goals.

The Argument for Configurable Solutions

When searching for a SS-CIM solution, security leaders' largest struggle comes down to this: Procuring a custom application or investing in a COTS-configurable platform. When deciding on a custom application, it is expected that it meets a set of exact requirements. Security is a complex and fast-changing environment, making it very unlikely that all requirements can be met. To meet the requirements, the software must be customized.

Customizing a static application is a considerable undertaking. It requires programmers to make modifications to core code, making the software do something that it was not originally designed to do. It introduces significant effort, cost, and risk. Routine upgrades to the core application become difficult.

Investing in a COTS-configurable solution provides unique advantages as it is built on a flexible development platform. Tools within the environment are used to make enhancements in a manner that the application was designed to have changes made. The configuration is inherently better because it is working within the application. Configurable GIS apps make it easy to create and share interactive web applications. Based on the requirements of SS-CIM, numerous configurable workflows can be deployed rapidly and simply. From conceptual requirements to a digital map, cumulating in numerous interactive web mapping applications, GIS is the platform that provides security professionals with the flexibility to integrate evolving requirements into their SS-CIM solution.

The examples below represent a best practice of how to operationalize GIS to support SS-CIM. It includes a menu of technical workflows, in chronological order, describing a variety of tools to consider deploying when executing a complex SS-CIM program objective.

Workflow: Acquire GIS Platform and Portal

Procuring a mapping and analysis software platform—or GIS—is the first step toward unifying a cross-sector and multiagency operational and analysis capability for SS-CIM.

A GIS portal provides the front-end access that allows security staff to manage content and share maps, scenes, apps, and other geographic information with authorized personnel within an organization(s). With a GIS portal, you can

- Create, host, and share web mapping apps like dashboards, viewers, and business intelligence tools.
- Search for GIS data and other content within multiple security organizations.
- Create groups that can share GIS information between personnel from different organizations and agencies.
- Share links to GIS apps and relevant information products to internal and external partners.
- Share map and layer packages to use in ArcGIS® Desktop apps.

Workflow: Sketch/Planning

For effective SS-CIM, defining the space in and around a facility includes two primary zones that identifies an inner and outer security perimeter. They are the following:

- Area of Operations (AOO)—AOO is defined as the inner perimeter where tactical operations are conducted to ensure the safety and security of persons and property inside the walls of a facility or the inner boundaries of a campus.
- Area of Influence (AOI)—AOI is defined as the outer perimeter where tactical operations are conducted to ensure the safety and security of persons and property outside the walls or campus boundary. This usually includes parking lots and other land areas adjacent to the facility or in the immediate vicinity.

Planners can digitize tactical zones that represent the AOO and AOI as the first step in creating tactical plans for a variety of planned events or unplanned critical incidents. These are predefined geographic regions that provide a simple graphical reference of the primary protective area during an operational period. GIS allows security planners to

- Identify AOO/AOI zones.
- Digitize zones into an operational plan.
- Share plans for situational awareness.

Workflow: Establish a Common Basemap

A basemap is a collection of GIS data and imagery that form the background of a map view of your AOO/AOI. A basemap is the foundational geographic layer required for all subsequent operational planning, incident response activities, and situational awareness. Enforcing the use of a common basemap is critical as it ensures that all parties are making decisions using the same authoritative map.

Steps toward establishing an effective, robust common basemap include the following:

- Leverage existing authoritative collections of global location data for use in ArcGIS, starting with data from ArcGIS Living Atlas of the World.
- Leverage near real-time basemaps, imagery, demographics, and environmental and business data to establish minimal foundational support for any security operation.
- Add basic functionality that supports Find and Locate tools to identify key layers like buildings, parcels, streets, paths, and utilities.
- Enforce the use of one common basemap among all organization/agency participants.
- Consider drone flyover for enhanced near real-time imagery of AOO/AOI.

Workflow: Imagery Collection and Processing

Acquiring near real-time imagery can sometimes be an operational requirement. Relying on existing imagery is oftentimes not ideal as it provides an outdated operational picture that can create confusion during critical events. Security planners now leverage drone technology to collect near real-time imagery for more current basemaps. GIS-enabled drone solutions support an infield imagery collection process used to support real-time critical decision-making required by incident commanders. Imagery products are equally useful to back-office or command center analysts who can conduct detailed processing of large image collections to understand changes over time. Near real-time imagery is ideal for large-scale special events where temporary structures, stands, and tents are routinely set up creating new challenges for security operations.

This workflow can also be used to collect imagery after a critical incident occurs, allowing commanders to visualize and quantify the impact. Drone technology and image processing techniques are easy to implement for GIS users with minimal expertise in imagery. This workflow involves the following activities:

- Deploy a drone to collect, process, and deliver near real-time imagery to your operations plan.
- Deploy new imagery as an additional base layer establishing a near real-time image for your common basemap.

- Conduct change detection operations if multiple flights are conducted.
- Deploy a drone after a critical incident to quantify the impact.

Workflow: 3D Basemap Enablement

Security planners can no longer rely on 2D data. A modern GIS builds on your existing GIS infrastructure and helps you integrate data from many sources to create a 3D model of your environment. You can qualify your threat landscape by representing urban forms and structures in 3D, assessing your infrastructure, and applying real-world context to improve tactical plans and operational decisions.

Workflow: Visibility Analysis

Some tactical questions can only be answered in 3D. There is a growing awareness among security organizations that three-dimensional space needs to be accounted for in preplanning and response activities. Currently, most security organizations have only limited capabilities for visualizing and analyzing the 3D characteristics of specific sites, facilities, and public spaces. Characteristics like line-of-sight visibility and viewsheds can't be accurately represented and understood in 2D. This inhibits the ability to identify and analyze threats that a sniper or active assailant could present, making it difficult to plan effectively and respond quickly to security incidents when they occur.

Effective tactical planning requires a clear understanding of threats and guidance on the most efficient way to respond. A 3D GIS provides visualization and analysis tools that let tactical users run line-of-sight and viewshed calculations for areas in or around a gathering space—such as windows, rooftops, and other locations above ground level—helping identify vantage points that could be exploited by assailants with firearms. These insights can help determine the optimal strategy for allocating and coordinating security resources (including countersnipers) so personnel can respond rapidly and effectively when incidents occur.

A visibility analysis strategy involves the following activities:

- Enable 3D content.
- Build capacity for creating, managing, analyzing, and sharing 3D content for tactical operations.
- Configure operational use cases that support line-of-sight analysis (countersniper).
- Configure operational use cases that support viewshed analysis (field surveillance, closed-circuit television [CCTV] analysis).

Workflow: Demographic Analysis

Understanding your AOO at the operational level is an important step in setting conditions for success during a security planning phase and the response phase when unplanned incidents occur. By analyzing and understanding the characteristics of an AOO, security officials can then determine how best to allocate tactical resources.

Access to demographic and community data helps security planners and leaders identify, understand, and share the relevant community characteristics that make up an AOO/AOI. This is useful for a variety of planning and emergency response workflows like knowing the details about schools, nursing homes, and other vulnerable populations.

These tools, integrated into a GIS platform, allow security personnel to share and leverage content they and others have created. Additionally, web maps published in an online environment can be viewed and used within the demographic analysis application. Details of why this capability is important for facility security include the following:

- Data interrogation tools make it possible to know more about a community beyond intuition.
- Color-coded maps or targeted searches are based on specific demographic, economic, or other criteria.
- Custom and preconfigured reports allow personnel to quickly interpret complex community environments for better-informed decision-making.
- Targeted populations are identified by digitizing user-defined areas or through traditional reporting by numerous geopolitical boundaries.
- Easy-to-use tools are available for nontechnical security professionals.

Workflow: Threat Assessment

A threat assessment is one of the most important elements of a comprehensive site security plan. Security planners must know where threats and vulnerabilities exist to adequately manage risk. A threat assessment is the practice of determining the existence, credibility, and seriousness of a potential threat.

GIS business information (BI) tools fuse location analytics with open data science and business intelligence workflows. It empowers analysts and operators—at all skill levels and across departments, organizations, and agencies—to directly connect data, perform advanced analytics, and develop robust information products. Users can automatically document analytical workflows to share tradecraft and reports or solve similar problems with alternative datasets. Users can easily link and interrelate charts, maps, graphs, and tables and produce robust analytical products describing identified threats.

As part of the preplanning process, GIS BI tools can help planners understand historical threat trends in and around the AOO such as the following:

- BI tools to discover historical and near real-time trends
- Crime/911 and incident data around the perimeter of your campus (from other public safety agencies)
- Incident analysis within your campus perimeter using in-house record management system (RMS)
- Supplemental data from open data sites (e.g., crime index)
- Supplemental demographic data and other community datasets
- Historical data from stored third-party threat feeds
- Link charts and link maps for understanding networks and relationships
- Desktop applications for more advanced clients and/or workflows

Workflow: Site Survey

Conducting a site survey is a common approach to security planning. Pinpointing sensitive locations is a core activity during this process.

A tactical site survey is a product derived from a comprehensive inspection of high-threat facilities (AOO) and their surrounding grounds (AOI). It is a catalog of critical data points and emergency plans and can help security personnel respond to a crisis quickly and efficiently.

Security officials must use mobile field collection apps to locate and track all sensitive locations in the AOO/AOI supporting the build-out of a tactical site survey.

The foundational component of the survey requires collecting location intelligence on facility features, emergency plans, and points of interest that has a bearing on the safety of a facility or the handling of a crisis at or near a facility. These features may include the location information for the following:

- Safe rooms
- Gun room/Armory
- Electric and telephone boxes
- Hazardous materials, underground utilities
- Fire extinguishers/Automated external defibrillators (AEDs)
- Ingress/Egress routes, evacuation zones
- Building schematic plans

Using a mobile device to update sensitive building features—while connected and disconnected—transforms a paper process to a digital solution using smart devices.

Workflow: Preoperation Planning

Preoperational planning for security incidents begins with a design. It starts as an idea that guides the conduct (the plan, preparation, and execution) of operationalizing security around potential incidents or threats. Core elements of the design involve GIS tools to aid security planners in visualizing and plotting tactical resource assignments as an overlay to the AOO and AOI, including 3D facility data. This process helps clarify and refine a commander's security vision by providing a framework to design, edit, and share the preoperational plan for the facility/event to any authorized personnel, agency, or organization.

The Tactical Operations Planner app is a configurable solution template designed for security planners to build operational plans. In addition to creating plans for known events (e.g., inaugurations), the Tactical Operations Planner can be used to strategize responses to unplanned events like active assailant, riots, barricaded gunmen, and other high-risk operations.

Tactical Operations Preplanning includes the following activities:

- Create operation preplans for various security events
- Plot tactical assets throughout AOO/AOI based on vulnerabilities and threats
- Plot fixed resources, denial operations, roadblocks, and barriers
- Use plans during operational and nonoperational periods

Workflow: Tactical Response

No security plan survives its initial implementation. Technology solutions must be adaptable and reconfigurable, so security personnel can edit and design tools spontaneously. From a command center or in the field, all users need real-time updates of security incidents and new operations plan configurations to address these emergencies.

The Tactical Operations Planner app is a configurable solution template designed for security planners to build incident response plans for unplanned emergency

situations. It can be used to strategize responses to a variety of situations quickly and efficiently. Examples may include the following:

- Evacuation plans
- Active assailant
- Riots
- Barricaded gunmen
- Suspicious packages
- Other high-risk incidences

Workflow: Transportation Planning

Preoperational planning for any security scenario must include a transportation plan.

Most large facilities require significant planning around traffic and transportation. Private vehicles, taxis, city buses, subways, trains, and/or ferry boats may be used to travel to and from critical facilities. Security planners must be able to coordinate and anticipate the volume, safety, and security of passengers.

When facilities are required to manage complex traffic scenarios, security planners can:

- Plot points that represent the traffic plan including the location of tactical assets securing drop-off and pickup locations.
- Digitize lines that show planned routes and emergency ingress and egress routes.
- Leverage real-time traffic and CCTV feeds to better inform transportation planning.

Workflow: Evacuation Planning

Emergency evacuation planning involves the urgent, immediate egress or escape of people away from an area that contains an imminent threat, an ongoing threat, or a hazard to lives or property. When securing a critical facility, emergency evacuation routes and zones must be digitized onto the operations plan basemap. Evacuation zones must be outside an anticipated impact area and depend on proximity to the facility, available open space, and other safety factors. This process includes the following:

- Map out primary and alternate evacuation routes
- Digitize evacuation zones
- Use the crowd size widget to calculate/understand evacuation zone parameters or estimate the size of a protest group (Jacobs Method)
- Base calculations on the following specifications:
  - One person per 2.5 square feet—mosh pit
  - One person per 4.5 square feet—elbow to elbow to elbow
  - One person per 10 square feet—light crowd

Workflow: Tracking and Dispatch

Incident dispatch applications allow command center personnel to initiate a call for service assignment based on the incoming threat or incident being reported. With GIS, enhanced service is provided through real-time awareness—knowing the location of the incident and all available security assets. Field personnel can receive assignments and report status updates via smart devices, establishing greater overall efficiency. As field personnel are carrying their maps and assignments on a smart device, they can stay organized, report progress, call for help, and stay productive.

This process includes the following:

- Plan—Use maps to create and assign calls to field personnel
- Navigate—Leverage routing tools for efficient response times
- Capture—Collect and submit incident updates
- Monitor—Visualize the location of all active incidents and personnel
- Understand—Conduct after-action analytics and assess facility coverage

Workflow: Security Personnel Tracking

Location matters when it comes to deploying tactical teams in complex security situations. Proper command and control necessitate knowing the real-time location of security teams and related assets. Establishing operational awareness means that a tactical team can visualize the location and communicate with its members. This all must be done through an easily deployed and easy-to-use mobile field app.

The location of GPS tracks of field personnel must be effortlessly captured, recorded, and fed into your GIS. Location tracks must be visualized to support the effective allocation of personnel relative to operational plans and responding to critical incidents. Location tracks can be analyzed to identify where personnel were situated prior to an incident or to determine if work assignments like an explosive ordnance (EOD) canvass were properly conducted in high-threat geographic areas. With tactical tracking, you can perform the following:

- View precise locations of tactical teams
- Enable peer-to-peer field communication
- Enhance command and control between the command center and the field
- Provide location awareness among all field personnel
- Discover missing or redundant territory coverage
- Evaluate patterns of movement against reported critical incidents
- Understand productivity and efficiency

Workflow: Indoor Facility Mapping

Workplace security and business continuity are under constant threat in the face of increasingly frequent natural disasters and human catastrophes. A facility map serves as a record of assets and the perfect tool for planning and responding to critical incidents.

Indoor mapping solutions create a connected workplace and establish a common view of the built environment for 2D or 3D situational awareness. To support complex security requirements, indoor mapping solutions must

- Use spatially enabled facilities data to visually activate indoor spaces for optimized security operations.

- Leverage precise indoor mapping and positioning technology.
- Create 2D or 3D digital indoor maps of buildings, visualizing all rooms or an entire campus.
- Collect, catalog, and plot critical data points and emergency plans.
- Integrate tools into security operations to enhance command and control between the command center and field personnel.

Workflow: SAR/Incident Dashboard

A dashboard is a configurable web app that allows security planners to create information products, such as maps, charts, graphs, and other visual indicators, to reflect the status of incidents, events, personnel, and field assets in real time.

Dashboards provide an executive-level view of critical activities and key performance indicators (KPIs) that matter most to a security mission. Users can monitor progress and identify critical vulnerabilities that may compromise the safety and security of a critical facility. Advanced mapping capabilities yield data analyses that support better-informed decision-making.

The integration of suspicious activity reporting (SAR) from the field to the command center is one example of how dashboard technology supports the mission. The SAR/Incident Dashboard workflow may include the following:

- Submit SAR data from mobile field applications to the command center
- Leverage GIS/maps for situational awareness
- Use a dashboard to manage if an incident is open, closed, or pending
- Interrelate with other operational layers
- Enable wide dissemination through Web GIS

Workflow: Real-Time Traffic Dashboard

Using dashboards to manage transportation-related events entails integrating traffic mapping services that present historical and near real-time traffic information in and around your AOO/AOI. A traffic dashboard can support the following use cases:

- Accidents, construction, and road closures that could impact the flow of traffic can be identified.
- Reported traffic incidents to inform emergency vehicles on routing, navigation, and field operations can be analyzed.
- Data service works globally and can be used to visualize traffic speeds and incidents near an AOO.
- Live, predictive, and historical traffic views can be leveraged.
- The dashboard can interrelate with other operational layers.
- Wide dissemination can be enabled by Web GIS.

Workflow: Live Threat Dashboard

Live threat feeds are constantly updating streams of indicators derived from multiple sources that report on weather, social media, wildfires, earthquakes, flooding, and more. Threat dashboards help compare multiple threat feeds simultaneously with other operational layers, enabling security analysts to produce and disseminate robust operational intelligence.

Security staff can focus on what really matters by setting up automated alerts that occur when external threat feeds intersect with high-value internal assets (people, property). Live threat dashboards can support the following:

- Real-time monitoring via keywords and user-defined algorithms
- Early detection of high-impact events
- Situational awareness of worldwide threats
- Prioritized threats based on proximity to agency assets
- Triage and manage incidents

Workflow: Proximity Search

Proximity search tools can be used to quickly identify operational layers from a user-defined incident location. These situational awareness tools are designed to optimize security workflows and simplify interaction with incident and operations data. Security commanders need configurable tools and widgets to quickly understand the impact of an incident in and around an AOO/AOI on human populations and key infrastructure. A mission-focused application must deliver tools that organize incident and operations data layers, so commanders can quickly quantify incident impact and respond accordingly.

After a critical incident occurs, security officials must be able to quickly locate and identify the following:

- Affected infrastructure/facilities
- Affected employees
- Affected population
- Nearest hospital
- Nearest police station
- Nearest shelters
- Nearest schools
- Area roadblocks

Workflow: Rapid Hazard Analysis

Rapid hazard analysis (RHA), consequence assessment, and impact analysis are mandatory procedures when responding to the threat or damage caused by industrial accidents, weapons of mass destruction (WMD), and high explosive (HE) events.

To facilitate critical decision-making before, during, and after a catastrophic event, GIS, demographic, and infrastructure data must fuel powerful geoprocessing tools to predict consequences to an impacted area. This includes damage assessments of the built environment and casualty predications to the area population. RHA tools provide the following:

- Casualty estimates
- Evacuation zones
- Shelter in place zones
- Hazmat response guidance to events involving toxic and industrial materials

Workflow: Mobile Field Reporting

Security personnel need a solution for rapidly capturing and reporting data from the field, even when disconnected, that works alongside other GIS field applications. This entails smart forms with predefined questions that are easy to answer. Tools must be configurable to craft surveys to the unique needs of the organization. Two primary use cases include reporting suspicious activity and reporting officer status (safe, not safe). This eliminates paper-based data collection that relies on the legibility of handwritten notes. GIS mobile-based field reporting supports the following:

- Rapid collection of field observations
- Real-time information updates between the field and the command center
- Immediately available incoming data for visualization and analysis
- Designed to rapidly collect data and photos

Workflow: Single Pane of Glass

Establishing complete situational awareness through a viewer or dashboard involves integrating and managing multiple sources of information in real time.

The concept of a "single pane of glass (SPOG)" is frequently sought after and constantly mentioned in facility security conversations. In principle, SPOG is a management tool—such as a unified viewer or dashboard—that integrates information from varied sources across multiple applications and environments into one single display. SPOG provides the following:

- Informative use of maps, charts, graphs, and tables in one view
- Executive-level view of interrelated critical activities and KPIs
- Progress monitored and critical vulnerabilities quickly identified
- High-level analysis for better-informed decision-making

The concept of a single pane of glass is so good—every security operations center (SOC) should have several. The configuration in a Web GIS environment is simple to perform. As such, security personnel do not have to figure out the requirements around one master viewer. As needs change or different problems emerge, users can simply reconfigure the dashboard or viewer and build a second or third—all depending on the needs of the organization.

Workflow: Executive Briefings

GIS is a communication tool that can be used for executive briefs and after-action assessments. An after-action review (AAR) is a structured review or debriefing process for analyzing the response to a major incident or event. This includes what happened, why it happened, and how the response can be done better.

Conducting a security briefing or providing an after-action report gives users the opportunity to come together and combine authoritative maps and apps with narrative text, images, and additional multimedia content. This allows the briefer to verbally communicate and interrogate data in live applications simultaneously.

Integrating GIS technology into an AAR or security briefing can

- Visually establish a common understanding of all event-related activities.
- Replay success and failures from the event using GIS tools.
- Respond to deeper questions through direct access to GIS apps and data.

- Identify lessons learned.
- Drive organizational change.

Getting Started

Technology solutions for facility security are generally managed out of a Security Operations Center. To lay the foundation for a successful GIS implementation, SOCs need to implement GIS as an initial operating capability (IOC). The IOC provides immediate and robust mapping and spatial analysis capabilities without any custom development. Technical implementations for a SOC IOC must follow a "configure first" strategy.

The advantage of this approach is that the SOC immediately benefits from its investment in a set of COTS apps for desktop, web, and mobile users. This first phase of implementing a COTS-based platform allows organizations to use industry best practices rather than creating new, customized processes.

When implementing GIS platform capabilities into a SOC environment, the solution architecture should comprise local and web-based software. The envisioned solution is a web-enabled environment that provides a wide range of GIS capabilities supporting data collection and management, analysis, visualization, and sharing. The foundation for this system is ArcGIS, which can run behind an organization's firewall, in its infrastructure, on-premises, or in the cloud. This flexible deployment works with enterprise systems and policies.

- Web GIS—ArcGIS Enterprise and ArcGIS Online, which have server and secure portal functionality, are used for securely creating, organizing, publishing, and managing geographic information. Most users (non-GIS professionals) will access and use geographic data and apps through these products. Content management capability administers access to data and services.
- IOC Apps—ArcGIS provides access to a set of powerful productivity apps, including web map viewing templates, data collection apps such as ArcGIS Collector, analytical tools such as ArcGIS Insights℠, apps for monitoring activities and events such as ArcGIS Dashboards, and apps for data dissemination such as ArcGIS StoryMaps℠. While powerful, these apps are ready to use with minimal effort. They can be easily configured to support SOC needs, providing personnel with quick access to information.
- Desktop—ArcGIS Pro provides very powerful tools for spatial analysis, data management, workflow management, and modeling. A small set of GIS professionals within the organization needs this tool. ArcGIS Pro is deeply integrated with the entire ArcGIS system so online content such as municipal data or community baseline data, as well as content managed in your own ArcGIS environment, is readily available to center users.

Conclusion

GIS enriches data sources through spatial enablement, facilitating a deeper understanding by linking and analyzing the relationship between data, incidents, and the built environment. A proper GIS deployment ensures that technical tools and capabilities remain strongly aligned with operational requirements. The common operational picture transforms into a common operational platform to foster enhanced public safety.

In our new global security environment, SS-CIM workflow configurations require solutions that enable the free, yet protected exchange of geospatial information among vetted partners to ensure collaboration and eliminate traditional information silos. Esri alone provides technology that best supports the evolving security environment.

About the Author

Carl Walter is the global director of Homeland Security Solutions at Esri. He works out of the corporate headquarters in Redlands, California.

Mr. Walter joined Esri in 2010 bringing with him more than 20 years of government experience in law enforcement and intelligence operations. He most recently served as director of the Boston Regional Intelligence Center and director of the Bureau of Intelligence and Analysis for the Boston Police Department. Post 9/11, he established a coordinated regional intelligence capability in the Boston metropolitan area operationalizing local, state, and federal law enforcement, public safety and private sector resources for preventing and responding to terrorist threats and violent criminal activity. His current role at Esri involves developing strategies that help integrate technology and operations to support the security needs of government agencies and Fortune 500 organizations worldwide.

esri | THE SCIENCE OF WHERE®

Esri, the global market leader in geographic information system (GIS) software, offers the most powerful mapping and spatial analytics technology available.

Since 1969, Esri has helped customers unlock the full potential of data to improve operational and business results. Today, Esri software is deployed in more than 350,000 organizations including the world's largest cities, most national governments, 75 percent of Fortune 500 companies, and more than 7,000 colleges and universities. Esri engineers the most advanced solutions for digital transformation, the Internet of Things (IoT), and location analytics to inform the most authoritative maps in the world.

Visit us at esri.com.

Contact Esri

380 New York Street
Redlands, California 92373-8100 USA

1 800 447 9778
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations

For more information, visit **go.esri.com/SS-CIM**.