Collecting, archiving, and utilizing critical infrastructure information

S. Conway, R. Cameron, S. Hermann & J. P. Nelson
Urban Environmental Research, LLC, USA

Abstract

Silver Shield is the USA (US) state of Nevada's Critical Infrastructure Protection Program in compliance with the US Department of Homeland Security's (DHS) National Infrastructure Protection Plan e.g. US DHS and the Target Capabilities List e.g. US DHS. Silver Shield's mission is to identify, catalogue, prioritize, and protect critical infrastructure and key resources to support federal, state, local, and tribal readiness, prevention, mitigation, and response efforts. Silver Shield operates in coordination with public and private sector entities to collect, archive, and disseminate information that representatives from fire departments, law enforcement, bomb squads, Special Weapons & Tactics (SWAT) medical response teams, and emergency managers deem vital to the protection of critical infrastructure. This paper details Silver Shield's process of collecting critical infrastructure information through Phased Site Assessments and the means by which this information is archived, evaluated, disseminated, and utilized via the Nevada Critical Infrastructure Protection System (CIPS), the DHS Automated Critical Infrastructure Protection Systems (ACAMS) and Orator Plus™ Presentations.

1 Introduction

Silver Shield is Nevada's Critical Infrastructure Protection Program with the mission to identify, catalogue, prioritize, and protect critical infrastructure and key resources to support federal, state, local, and tribal readiness, prevention, mitigation, and response efforts. The Department of Homeland Security (DHS) defines critical infrastructure as: "Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any

combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction." e.g. DHS [1] Silver Shield supports an unprecedented partnership between public and private sector entities to facilitate the ongoing process of critical infrastructure protection.

1.1 Compliance

Silver Shield is compliant with the responsibilities of developing, coordinating, integrating, and implementing plans and programs that identify, catalogue, prioritize, and protect critical infrastructure/key resources (CIKR) in cooperation with all levels of government and private sector entities , e.g. US DHS [2]. These responsibilities are set forth in the National Infrastructure Protection Plan, which was created by DHS in direct response to Homeland Security Presidential Directive 7, e.g. Bush [3]. Silver Shield also aligns with the priorities of the National Preparedness Guidelines, e.g. DHS [4] which establish a vision for national preparedness and provide a systematic approach for prioritizing preparedness efforts across the nation; and the Target Capabilities List, which describes the collective national capabilities required to prevent, protect against, respond to, and recover from terrorist attacks, major disasters and other emergencies. The National Preparedness Guidelines and the Target Capabilities List were produced as a result of Homeland Security Presidential Directive 8, e.g. Bush [5].

1.2 Fusion centers

Silver Shield operates in conjunction with Nevada's three fusion centers, in which numerous local, state, and federal agency representatives engage in a concerted effort to facilitate the exchange of information and intelligence, optimize efficiency, and ultimately enhance the ability to combat crime and terrorism. Nevada's fusion centers are the Northern Nevada Counter Terrorism Center (NNCTC) in Reno, the Southern Nevada Counter Terrorism Center (SNCTC) in Las Vegas, and the Nevada Threat Assessment Center (NTAC) in Carson City. Fusion centers and Silver Shield share the objective of developing a statewide network for the collection, analysis, and sharing of information that representatives from fire departments, law enforcement, bomb squads, SWAT, medical response teams, and other emergency managers deemed vital to the protection of critical infrastructure.

1.3 Data call

Critical infrastructures are identified through the DHS data call process, which is broken into four phases. The first phase is Nomination, where infrastructures are nominated by Sector, State, and Territory partners for review. Subsequent to Nomination, infrastructures go through the Adjudication phase, where nominated assets are evaluated by subject matter experts based on criteria established by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) National Critical Infrastructure Prioritization Program (NCIPP). Sector, State, and

Territory partners have the opportunity to review the results of the evaluations and resolve any disagreements over the results during the Reconsideration phase. Publication is the final phase of the data call process and involves providing the finalized list to Sector, State, and Territory partners for review and comment before it is disseminated. State plans for the prioritization of sectors and sector leads must be approved by DHS, which provides for a higher level of standardization and therefore, greater protection capabilities.

2   Phased site assessments

Phased Site Assessments of an asset commence subsequent to its clearance of the data call process. Site assessments are divided into phases in accordance with the controlled implementation approach prescribed by DHS and the Critical Infrastructure/Key Resource Asset Protection Technical Assistance Program (CAPTAP).

2.1 Phase I site assessments

Phase I Site Assessments consist of making initial contact with the asset, capturing and cataloguing critical infrastructure information, and completing the Common Operating Picture (COP) survey. Emergency points-of-contact are established once initial contact is made with the asset. Critical infrastructure information, such as aerial photographs, parcel maps, emergency response plans, perimeter still photographs, and floor plans, are collected during Phase I Site Assessments. The asset manager and, if possible, facility engineer and security manager participate in completing the COP survey, which includes sections such as contact information, facility description, occupancy, utilities, hazardous materials, exposures, available resources, security measures, sprinkler information, as well as sector-specific sections.

2.2 Phase II site assessments

Phase II Site Assessments involve a more comprehensive visual capture of the asset. Still photographs of items and locations of particular importance, spherical panoramic photographs of the exterior and throughout the interior of the asset, and SPIDR Panoramic Video Digital Camera footage are collected during Phase II Site Assessments. Vulnerability assessments of the assets are made during Phase II Site Assessments and proposed security enhancements are suggested as "Options for Consideration."

3   The critical infrastructure protection system

The Critical Infrastructure Protection System (CIPS) was conceived as an interactive, web-based tool for archiving and disseminating critical infrastructure information to emergency responders and was designed to integrate geospatial/geographic information system (GIS) software. The integration of

critical infrastructure information and GIS technology, in a tool that is accessible to emergency responders, is intended to enhance incident command capabilities, support the development of site-specific protective programs, and improve the ability to plan for and manage special events.

3.1 Geo-referencing

The CIPS tool extensively incorporates the geo-referencing capabilities of GIS technology. Geo-referencing is the process of relating spatial information to a geographic location. In other words, something is geo-referenced when its existence is defined within a physical space.

3.1.1 Asset creation

An asset is created in the CIPS tool by geo-referencing its location, specifically the perimeter of its property, to a map display. Once an asset is in the system, the structures that it is comprised of can be created in a similar manner, as well as individual floors within those structures. The process of locating and identifying assets and structures is simplified by geo-referencing their locations to the map display.

3.1.2 Items of interest

Visual representations of hazardous materials, fire hydrants, first-aid stations, emergency power generators, and other items of interest can be geo-referenced in their exact locations within the map display. Floor plans can be geo-referenced to the structure they are associated with, at which point their movement and size will adjust in direct correlation with the navigation of the map display. Geo-referenced floor plans can be viewed individually, which allows for visual representations of items of interest to be geo-referenced to the plan of the floor on which the items are located.

3.1.3 Benefits of geo-referencing

Scenarios where incident command has the ability to guide emergency responders to the exact locations of items of interest, especially in scenarios involving impaired vision, demonstrate the advantages of geo-referencing capabilities. The less time spent locating critical information, the less time an incident has to escalate in severity. The benefits of geo-referencing are compounded by the ability to utilize the process on individual floor plans, which allows for emergency responders to be aware of the particular resources and hazards that are located on a specific floor of a structure.

3.2 Microsoft InfoPath

Every asset in the CIPS tool has a Microsoft InfoPath questionnaire form associated with it. Each asset's respective Microsoft InfoPath form is populated with the information that was collected in the COP survey during the Phased Site Assessments. The utilization of Microsoft InfoPath allows emergency responders

to readily access critical infrastructure information, which enables them to make more informed decisions.

3.3 Attachments

Electronic versions of critical infrastructure information can be incorporated into the CIPS tool in the form of attachments. A greater level of specificity in associating the content of an attachment is provided by the tiered creation approach, where structures and floors are created within a critical infrastructure and attachments are associated at the tier they are most relevant to.

3.3.1 Associating attachment content
An example of an attachment that would be associated at the critical infrastructure level is an aerial photograph that completely encompasses the asset. An evacuation plan, or similar tactical pre-plan, for a specific building would be associated at the structure level. Attachments that are related to an individual floor, such as a floor plan, are associated at the floor level.

3.3.2 Benefits of tiered association
The process of locating and retrieving specific information is expedited by the tiered classification of attachments. In a scenario where a floor plan for a specific floor of a building needs to be accessed, rather than sift through all of the attachments associated with the asset, emergency responders can navigate to the attachments associated with the respective floor of that structure.

3.4 Map layers

The integration of GIS capabilities in the CIPS tool provides the ability to create, access, and review map layers that accentuate various, significant points of interest within the map display. Law enforcement can evaluate map layers that mark the locations of reported criminal activity and refer to those assessments as a basis for the allocation of resources. Map layers can be used by fire department personnel to identify locations in the vicinity of a fire that house hazardous materials. In the event of a significant crisis, emergency responders can refer to map layers that highlight locations, such as schools, hospitals, and senior centers, that would need to be evacuated or serve as staging areas.

4   The Automated Critical Asset Management System (ACAMS)

The Automated Critical Asset Management System (ACAMS) is a secure, online database created by DHS as a means of archiving and managing critical infrastructure information. ACAMS allows for the cataloguing, screening, and sorting of critical infrastructure information, as well the development of asset-specific reports and multiple pre- and post-incident response plans.

4.1 Protected critical infrastructure information

Information that is entered into ACAMS becomes Protected Critical Infrastructure Information (PCII) and is subsequently sheltered from disclosure under Freedom of Information Act requests, state and local sunshine laws, and civil litigation proceedings. The PCII Program was designed to encourage private sector entities to cooperate with critical infrastructure protection efforts by providing safeguards for sensitive business information.

4.2 Asset inventory management

ACAMS serves as a comprehensive asset inventory and inventory management system. An asset is entered into ACAMS by creating an Inventory page that contains general identification information, such as the asset's address, point-of-contact information, and sector information. Once an Inventory page is created for an asset, the critical infrastructure information collected in the COP survey during Phased Site Assessments is used to populate an Asset Manager Questionnaire (AMQ) and an Initial Asset Visit (IAV) form. Information regarding utilities, types and locations of hazardous materials, specific security procedures, dependencies, and interdependencies is contained in the AMQ and IAV forms. Electronic versions of critical infrastructure information can also be incorporated in the form of attachments.

4.3 Vulnerability assessments

ACAMS provides the tools to perform vulnerability assessments of critical infrastructure.

4.3.1 MSHARRPP+V
The Mission, Symbolism, History, Accessibility, Recognizability, Recoverability, Population, Proximity, and Vulnerability (MSHARRPP+V) report is used as a means of numerically evaluating the criticality and vulnerability of individual assets in terms of the continuity of operation in a particular area of responsibility. The MSHARRPP+V score of an asset in a given sector is compared to the scores of other assets within that sector and prioritized accordingly.

4.3.2 CARVER
The Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability (CARVER) report is an analytical tool used to evaluate the criticality and vulnerability of an asset's critical nodes, which are physical locations, pieces of equipment, technology, or other items that if lost or destroyed, would significantly affect the asset's ability to function. The sum of the values assigned to each factor is the CARVER score, which represents the likelihood of the critical node being the target of an attack.

4.3.3 Post-assessment

The MSHARRPP+V and CARVER reports are instrumental while generating the "Options for Consideration" proposals, which are suggestions for enhancing security and reducing risk. Subsequent to the implementation of any proposals, the MSHARRPP+V and CARVER assessments are preformed again to measure the effectiveness of the changes.

5 Orator Plus™

Orator Plus™ presentations provide the ability to simultaneously display multiple media formats, which allows for non-linear, interactive presentations. Orator Plus presentations incorporate the critical infrastructure information collected during the Phased Site Assessments in a unique way. The types of files that can be incorporated into an Orator Plus project include streaming video, 360 degree panorama photographs, still photograph, digital surveillance cameras, and chemical sensors.

5.1 Hot-spotting

A link to a media file can be hot-spotted to an image or panorama file so that the hot-spotted file will launch from within the image or panorama containing the hot-spot. In this way, panoramic and still photographs of the exterior of an asset are hot-spotted to an aerial photograph, while those from the interior are hot-spotted to a floor plan, in the locations that they were taken. Panoramic photographs can be hot-spotted to other panoramic photographs allowing for an interactive, non-linear, virtual tour of the asset. The ability to virtually navigate the asset under baseline conditions could prove invaluable to emergency responders in scenarios where vision is impaired. The visualization capabilities of Orator Plus™ presentations are augmented by the ability to access and view live camera feeds from digital surveillance cameras.

5.2 White board

White board scenarios are a very useful feature of Orator Plus™ presentations for planning, conducting exercises, as well as working out real time events. Objects from a library of symbols can be placed on maps, aerial photographs, floor plans, lot diagrams, blueprints, or any image to illustrate different incidents and scenarios. Objects can be added, deleted, and moved on the image to show changes at the actual scene. In the event of an emergency at an asset, the white board feature can improve incident command's ability to allocate and manage the available resources by placing symbols of those resources on an aerial photograph of the asset. The white board feature allows incident command to visualize possible developments, before they occur, and alternative courses of action, before they are implemented, and optimizes emergency management capabilities.

5.3 Access and distribution

Orator Plus™ presentations are compiled into a standalone presentation file, which allows for security, ease of use, and distribution on CD's or thumb drives either to emergency responders with no web-based access, or to asset personnel for internal planning use. The Orator Plus™ presentation for an asset is also incorporated into the CIPS and ACAMS pages of that asset in the form of attachments. Although the presentations can be distributed through web-based systems, like CIPS and ACAMS they can be viewed on laptops, notebooks, or desktop computers as they are standalone files.

6 Special events

Special events include live events where mass population safety is a concern and both tabletop and full-scale live exercises involving multiple scenarios, emergency response agencies, and role-players conducting training.

6.1 Situational awareness

Silver Shield promotes better situational awareness for responders and planners. Situational awareness involves three sequential processes; perceiving, comprehending and projecting.

6.1.1 Perceiving
Perceiving involves recognizing and being aware of relevant elements, such as structures, systems, resources, critical nodes, and the population of the event, in the environment and the status of those elements. Structures, systems, and resources are identified in CIPS and detailed descriptions of them are contained in the Microsoft InfoPath questionnaire. Critical nodes are identified in ACAMS. The population of the event and the statuses of all of the relevant elements in the environment can be monitored utilizing the live camera feed capabilities of Orator Plus™ presentations.

6.1.2 Comprehending
The comprehending process involves interpreting and understanding the relationships and dynamics between the various elements in the environment. Dependencies, interdependencies, redundancies, and similar relationships are described at length in ACAMS and the Microsoft InfoPath questionnaire in CIPS.

6.1.3 Projecting
The process of projecting involves the ability to predict the future behavior and status of elements in the environment and is only possible once these elements, and their current statuses, are identified and the relationships between them are understood. Silver Shield uses CIPS, ACAMS, and Orator Plus™ to evaluate a situation, and the white board to display scenarios, which significantly enhances response and management capabilities.

6.2 Incident command

Silver Shield provides incident command support for various special events, using the CIPS tool, ACAMS, and Orator Plus™ presentations. In the event of an incident, Silver Shield utilizes the mapping capabilities of CIPS and Orator Plus™ presentations to assist response efforts.

6.2.1 Navigation

The floor plans and aerial photographs that are stored in CIPS and Orator Plus™ presentations are used to provide response personnel with direct or alternative routes to an incident. Silver Shield alerts response personnel to the exact locations of nearby items of interest.

6.2.2 Emergency management

When the response to an incident requires an evacuation, Silver Shield uses CIPS to access map layers that highlight possible staging areas near the asset. In the event of a specific emergency, Silver Shield can access any tactical pre-plans for study, revision and implementation. The white board feature of Orator Plus™ presentations enhances the ability to efficiently manage personnel and resources by monitoring their projected locations, response routes, deployment time considerations and proximity issues.

7   Conclusion

The US Department of Homeland Security has provided emergency responders, government officials, and emergency managers across the country a framework for enhancing critical infrastructure protection. The ACAMS system facilitates inventorying, archiving, and utilizing information for planning purposes with basic tools accessible on a web-based platform.

The state of Nevada, with its Silver Shield program, has added additional information acquisition, archiving, distribution and display capabilities. These capabilities typically are more visually oriented and designed to facilitate more rapid access, viewing and manipulation than the national system.

A consensus among Nevada emergency responders and managers is that Silver Shield performs an invaluable function in enhancing emergency preparedness in the state.

References

[1] National Infrastructure Protection Plan, Glossary; U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
[2] National Infrastructure Protection Plan, Appendix 3C ; U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
[3] Homeland Security Presidential Directive /HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection. The White House, Office of the

Press Secretary. December 2003. http://www.dhs.gov/xabout/laws/gc_ 1214597989952.shtm

[4] National Preparedness Guidelines; U.S. Department of Homeland Security. September 2007. http://www.fema.gov/pdf/government/npg.pdf

[5] Homeland Security Presidential Directive/HSPD-8: National Preparedness. The White House, Office of the Press Secretary. December 2003. http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm