Homeland Security: Requirements for Installation Security Decision Support Systems

MAJ Gregg Powell, COL Charles Dunn III
POC: MAJ Gregg Powell
Battle Command Battle Lab (Gordon)
Bldg 71600, 16th Street
Fort Gordon, GA 30905
(706) 791-7550
FAX (706) 791-3799
gregg.powell@us.army.mil
21 March 2004

Homeland Security:
Requirements for Installation Security Decision Support Systems

MAJ Gregg Powell, COL Charles Dunn III
Battle Command Battle Lab (Gordon)
Bldg 71600, 16th Street
Fort Gordon, GA 30905

Abstract

The terrorist attacks that occurred on September 11, 2001 caught the nation off guard and made it apparent that existing homeland security capabilities were inadequate. There was also a realization that federal, state, and local government agencies require an installation security system that serves as an interagency communication and decision support tool. This tool would present one Common Operational Picture (COP), and provide common situational awareness in real time. Such a system must enhance the government's ability to effectively combat terrorism and respond to large-scale emergencies and disasters in a coordinated fashion. Installation security is both a force protection and public safety assurance measure that must detect and identify threats, deter attacks, secure key facilities, and protect personnel to ensure national security and mission readiness. There are currently a number of endeavors being undertaken in parallel efforts to field such a system. None of these endeavors, however, are being coordinated to ensure compatibility or to prevent duplicative effort.

This paper will define the requirements for an installation security system, compare the capabilities of the different systems that are currently being proposed, discuss the status of acquiring and fielding these systems, and provide a recommendation about which system best meets the necessary requirements.

Purpose

The purpose of this paper is (1) to show the necessity for a common, interoperable set of installation security systems and standards that fit within the framework of the national Homeland security and Homeland defense requirements; (2) to define what the installation security requirements are; (3) to discuss the progress the government has made in addressing these requirements; and (4) to make recommendations on how these requirements may be better fulfilled in the future.

The United States Government has a non-negotiable contract with the American people to pursue every foreseeable threat and take every possible action in its effort to prevent terrorism. This responsibility also extends to ensuring that there exists the means to respond effectively in the event that a terrorist attack occurs. Unfortunately, no guarantee can be made that every act of terrorism will be prevented. What must be guaranteed, however, is that every possible step is taken in the war against this threat. The business of preventing and responding to terrorist attacks when they occur requires considerable coordination, information sharing, and cooperation among the many federal, state, and local government organizations and agencies, to include the United States Army, other DoD services, the Federal Emergency Management Agency (FEMA), non-government humanitarian organizations, and various intelligence and law enforcement agencies.

What triggered the realization that this requirement exists?

Prior to the terrorist attack on September 11, 2001, Homeland security was essentially taken for granted. The relative geographic isolation of the United States afforded by the North American continent provided a level of security that seemed adequate. The Cold War had ended a decade earlier, and aside from the unlikely menace of nuclear war, no real threat to the nation was perceived. The thought of a catastrophic terrorist attack seemed unlikely and even unimaginable to all except the most pessimistic intelligence analysts. Even as terrorist attacks against American interests began to escalate through the 1980s and 90s, no one foresaw the events that were about to take place. Not even the terrorist bombing in the basement of the World Trade Center in February 1993 caused the American government to face its vulnerability to terrorist attack.

The American public was forced to deal with this reality on September 11, 2001. The terrorist attacks on the World Trade Center towers and the Pentagon were no less infamous than the Japanese attack on Pearl Harbor sixty years before. Aside from the surprise nature and magnitude of these catastrophic attacks, few similarities exist. The 1941 attack on Pearl Harbor was conducted by a sovereign power that was easily identified and branded as the enemy. In comparison, the terrorist strikes against New York City and the Pentagon, and the failed attack against a target in Washington D.C. were conducted by members of an international Islamic terrorist organization. The perpetrators were operating freely in the United States during the preparation and training phase of their attack. Failure to detect the presence of the terrorist cells was partly assured by the laws that prevented law enforcement and intelligence agencies from

sharing information, even on matters involving terrorism. No system was in place to enable the sharing of information among the government agencies that had the responsibility for protecting the American people.

Additionally, the nature of the current war on terrorism being conducted is different then the nature of the Second World War against Japan. Given that the September 11, 2001 attack was carried out by a non-state entity that is much more difficult to isolate and identify as the enemy, or to locate for retaliation and destruction, the prosecution of this war requires a completely different strategy. Years of liberal entry and immigration policies have allowed terrorists to easily infiltrate and establish themselves within the nation. Intelligence analysts warn that future terrorist attacks on the scale of those that occurred against the Pentagon and the World Trade Center are inevitable. There exists a clear and present danger of future terrorist attack, and the necessity for heightened vigilance remains paramount.

Given this scenario, every effort must be made now to provide all government agencies that safeguard the American people with the capabilities that they need to effectively combat terrorism. For this reason, the Department of Homeland Security (DHS) was created, resulting in the largest restructuring of the federal government in history. The DHS has taken significant steps to ensure that the people and assets of the United States are protected, however, a significant vulnerability still remains that requires immediate attention: there are no common standards or systems in place that will provide the capabilities necessary to perform installation security effectively.

Installation Security Requirements Defined

At the national level, conducting the missions of Homeland security and Homeland defense are daunting tasks. One fundamental piece of the Homeland security puzzle that this paper will address involves installation security. Installation security ensures, among other things, that government agencies, their assets, personnel, and property are protected against any threat to include terrorism. Installation security applies to agencies at the federal, state, and local level. There are a number of capabilities that are vital to an effective installation security plan. The foremost requirement is that an automated installation security system, commonly referred to as a Decision Support System (DSS), provides the following capabilities:

(1) Instantaneous inter- and intra-agency communication. Two essential requirements for any installation security system involve compatibility and accessibility. The ability for different federal, state, and local government agencies to share relevant information across compatible systems in real-time is absolutely critical for installation security operations, whether at the national level when the security of the country is concerned, or at a regional level where individual installations and their surrounding areas are concerned. Additionally, any DSS employed for the purposes of installation security must be accessible to all agencies that have a need to coordinate efforts. The requirements for compatibility and accessibility were validated during the Federal Emergency Management Agency (FEMA) Region IV's Consequence Management Exercises conducted at Fort Gordon in 2002 and 2003. During both exercises, the requirement was validated for the Fort Gordon Installation Operation Center (IOC) to share information with a number of other organizations and agencies to include the Fort

Gordon Eisenhower Army Medical Center,[1] Georgia Public Health Region VI, Columbia and Richmond County Emergency Operation Centers (EOCs), FEMA Region IV, US Army South-East Regional Installation Management Agency (IMA), Medical College of Georgia, Georgia Army National Guard EOC, and others. While not all of these agencies were tied together using one common DSS, enough were to show that this capability requires a substantial degree of effort.

Given the immense amount of information that must be shared, processed, and analyzed, simply maintaining open lines of communication over the telephone network is wholly inadequate. Each organization requires access to a common DSS that queries parallel and distributed information sources. Using these information sources, the DSS then provides a Common Operational Picture (COP) that is updated in real-time.

Typically, each organization operates on its own network; each has its own separate requirements for network security, and each has separate budgets for purchasing computer systems and networking equipment. Having an installation security DSS that is flexible enough so that every required organization or agency is able to gain access to relevant information, was viewed to be a paramount requirement for any Homeland security operation to be successful. Metcalf's Law states that as the number of nodes on a network grows, the corresponding value to the user of the networked system grows exponentially. His theory holds true in this case. Flexibility is gained by employing a system that is web-based (as opposed to application-based) and that uses a federated, distributed, peer-to-peer model. Agencies that have the resources to purchase and maintain their own DSS can do so. Other pertinent and authorized organizations, which

[1] The Fort Gordon Eisenhower Army Medical Center and Fort Gordon are both Army organizations; however, each falls under a different and unrelated command structure.

do not have the money or resources to maintain a DSS, may gain access to all of the relevant information maintained by a given system through a web browser that is used to access a DSS server. All that is needed to allow the client to access the DSS server is an account on the server and prior coordination through the network administrator on whose network the DSS server resides.

Using common applications like the web browser, and open source protocols like HTML and XML, inter- and intra-agency communications can be revolutionized. There is no need for different, expensive, application-based, and resource-heavy systems for every organization to administer. The ubiquitous nature of the Internet and other DoD networks makes it possible to leverage this common architecture to provide an inter-agency communications capability.

(2) Access to a Common Operational Picture (COP). A real-time tailorable COP that includes all relevant and actionable information that is geo-referenced to a set of computerized maps must be accessible to every agency that is responding to missions of Homeland and Installation security. The necessity for a COP is a fundamental and undisputed requirement for the conduct of warfare. According to the US Joint Forces Command (USJFCOM) Glossary[1], a COP is a single identical display of relevant information shared by more than one organization. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness. While the nature of the war against terrorism is different than the nature of conventional war, many requirements remain similar. To facilitate a coordinated response to a given situation, everyone must have access to the visual display of the same relevant information. Thus,

any automated installation security DSS must display a COP that is maintained in real-time and is customizable to the agency or organization that is viewing it.

(3) Remote monitoring of alarm or sensor systems (chemical, biological, radiological, and nuclear). The ability to remotely monitor alarms and sensors that detect the presence of chemical and biological agents and radioactive isotopes is a critical component of installation security. An installation security system's ability to monitor fire, HVAC, intrusion detection, and other sensors is also an important requirement because the sensors serve as the eyes and ears for an automated installation security system.

(4) Location tracking of assets in real time. The ability to track assets and display this information within the COP on the DSS is important for personnel who manage installation security. A need exists to track the location of first responders, emergency response personnel and vehicles, and other mobile assets, and to provide this information to every organization or agency that requires it. In the same way that a commander must understand where his forces are located on the battlefield, emergency response managers must understand where first responders and emergency support teams are located during a crisis.

(5) Automated public alert and recall or notification of essential and key personnel. Any automated system used for the purposes of installation security must have the ability to notify and recall key personnel. It must also have the ability to either serve as, or trigger a public alert system in order to warn the public in times of emergency. Finally, an installation security DSS must also have the ability to notify and

alert higher headquarters and adjacent organizations and agencies, and be capable of receiving notifications and alerts from both.

(6) Tie-in to law enforcement criminal background check systems. The ability to access law enforcement criminal background checking systems is a capability that while not critical, may serve to enhance a DSS designed for Homeland and Installation Security. This capability would enable installation security personnel to identify known criminals and terrorists for the purpose of apprehension.

(7) Integrated Decision Support System (DSS). The combination of the capabilities described in the preceding paragraphs, for the purposes of providing an automated installation and homeland security system, is described as a Decision Support System (DSS) in the context of this paper.

What has been done to date to develop a DSS?

At the time of this writing, there are at least four systems that perform some or all of the requirements outlined in the previous paragraphs. The four systems are Joint Protection Enterprise Network (JPEN), Joint Warning and Reporting Network (JWARN), Area Security Operations Command and Control (ASOCC), and Protect, Respond, Inform, Secure, and Monitor (PRISM). A description, overview, and summary of each system's capabilities follow.

(1) Joint Protection Enterprise Network (JPEN). According to documentation released by the Joint Staff C4 Systems Directorate, the purpose of JPEN is to create an integrated, cross-domain / inter-agency, information sharing program for force protection and threat related events that potentially impact the security of DoD installations within the United States. The program is intended to permit essential information sharing

among military, law enforcement, and intelligence organizations that, as part of their mission, collect and disseminate information in an effort to identify and combat possible threats. JPEN can document, refer, track, monitor, and evaluate suspected criminal activity that threatens the interests, property, and/or personnel on a DoD installation.[2]

JPEN was created by CellExchange in Jacksonville, Florida. The JPEN system manager is the Joint Staff C4 Systems Directorate. Records maintained in the JPEN system include investigative information supporting known or suspected suspicious activity and incidents at DoD installations. JPEN essentially serves as a law enforcement database that can be accessed by DoD and non-DoD agencies.[3] JPEN is a government-off-the-shelf (GOTS) product. It was previously known as "Protect America".

Unfortunately, JPEN does not provide the capabilities necessary for it to be used as an installation security decision support tool, because it only addresses one of the capabilities previously listed as critical for an installation security DSS.

(2) Joint Warning and Reporting Network (JWARN). The purpose of JWARN is to accelerate the warfighter's response to an enemy chemical, biological, radiological, or nuclear (CBRN) attack by providing the joint forces with the capability to report, analyze, and disseminate CBRN detection, identification, location and warning information. JWARN consists of software and hardware components that link CBRN detectors to tactical communications for CBRN warning, reporting, and battlefield management.[4] The U.S. Marine Corps is the program lead. The JWARN Program will replace the manual service-specific systems currently in use. At full capability, it will automate the transfer of data between CBRN detectors/sensors and C4I systems that will facilitate the military's decision-making process. Quicker response with accurate and

current information will minimize the effects of hostile attack, accidents or incidents. JWARN will be compatible with and integrated into the Joint Service C4I2 systems, and will be located in C2 centers once fielded.[4] This system is a combination of commercial off the shelf (COTS) and GOTS products. A significant shortcoming of JWARN is that it only addresses a limited set of installation security requirements, as it provides only CBRN threat warning and mitigation capability.

(**3) Area Security Operations Command and Control (ASOCC).** The purpose of ASOCC is to serve as a DSS for installation security operations. The ASOCC software originally was called the Coalition Rear Area Security Operations Command and Control System. It was developed for C2 applications by Science Applications International Corporation (SAIC) for the US Pacific Command (PACOM) before being modified for Homeland security and installation security purposes.[5] ASOCC has three main functional areas: *information management, situation management,* and *collaboration*.

ASOCC is a package of COTS and GOTS products integrated by the Defense Information System Agency (DISA) and accredited for secure and non-secure government networks. One core component of ASOCC is the *Defense Collaborative Tool Suite* (DCTS). DCTS itself is a Joint Program that provides a COTS-based suite of applications that enables a voice-over-whiteboard collaboration capability. DCTS uses Microsoft's Internet Information Server (IIS) suite of software products, including Netmeeting as a client. ASOCC is currently in operation in the US Pacific Command (PACOM) and in the Capital Area Defense Information Initiative (CADII). ASOCC

provides commanders with the capability to plan, coordinate, integrate and manage anti-terrorism and force protection operations.[6] Other ASOCC components include:

ExPanel – A real-time alerting and status visualization system.

KnowledgeBoard – Portal that pushes web-based information.

Java Imagery and Video Exploitation (JIVE) - Multiple formats of geo-spatial imagery with overlays and text capabilities.

eXtensible Information Systems (XIS) – Provides open standards information management support.

Deployment Visualization Toolkit (DVT) - Provides read-only access to the Joint Operational Planning Execution System (JOPES) database.

ASOCC is a fully developed solution for Homeland security and installation security operations. It provides several of the capabilities outlined earlier with the exception of the automated public alert and recall capability, and criminal background checking capability. ASOCC has limited CBRN capability integration. ASOCC's largest drawback is limited accessibility due to high cost. Every location that uses ASOCC must have a copy of DCTS, which costs approximately $600,000 per system installation. Additionally, ASOCC is not web-based which precludes accessibility for all non-DoD and DoD agencies that do not have the resources necessary to purchase such an expensive system. Given that accessibility is a critical requirement for an installation security system, ASOCC is not the best choice for many agencies.

(4) PRISM – Protect, Respond, Inform, Secure, and Monitor. PRISM is a Homeland security Command and Control (C2) decision support system. PRISM is composed of two primary components: *Contora* and *ESRI ArcIMS*. Additional and optional components include *Message 911, Ensco Sentry*, and *Lunar Eye*. These components have been tightly integrated into a single end-user application that provides a

messaging, alerting, geo-referenced mapping, asset tracking, CBRN sensing, and public warning system. The core PRISM package which includes sensor and asset tracking integration costs approximately $80,000 per installation with a 50-client license. A brief explanation of the COTS components that make up the integrated PRISM system follows:

Messaging and alerting capability: The component of PRISM that provides messaging and alerting capabilities is called Contora. Contora, with its embedded Transsend Enterprise Messaging Service software, is the COTS component that is the core of PRISM. It provides enterprise messaging to every agency or organization that is equipped with a PRISM server or that has a web-based account on the server. The Contora engine is seamlessly integrated into PRISM, operates in a distributed client-server model, and is accessible from any web browser. It provides an incident reporting and tracking capability and a tasking and facility reporting capability.

Georeferenced mapping capability: The PRISM component that provides this capability is called ArcIMS. ArcIMS is also seamlessly integrated into PRISM through Contora. ArcIMS is a component of the COTS ArcGIS mapping software suite that will replace the Joint Mapping Toolkit (JMTK). ArcIMS provides web-based geographical maps onto which Contora plots geo-referenced incident reports, asset tracking, and Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) events tracking and reporting. ArcIMS is the industry standard Geo-referenced Information System (GIS) mapping software.

Integrated sensor capability: Ensco Sentry is a COTS component that provides sensor integration capabilities to tie together a deployed suite of Chemical, Biological, Radiological, and Nuclear (CBRN) sensors. Sentry is tightly integrated with PRISM to provide immediate notification of CBRN events that can then be plotted to the ESRI ArcIMS enabled mapping display. Ensco Sentry can also integrate other types of sensors and alarms to include facility and boundary intrusion alert, and facility emergency alert (fire, HVAC, etc.). The Ensco Sentry system is capable of generating downwind hazard plume information and passing this information off to Message 911 for geo-referenced reverse lookup message alerting.

Automated public alert and recall capability: Message 911 is a COTS web-based voice notification system that can be configured to call, automatically or on command, all of the telephones in a geographic area. It can also be set up to call, automatically or on command, all of the telephone numbers in a predefined group or set of groups. Message 911 is capable of sending alerts via pager, mobile trunked radios, and e-mail. This system has a text-to-speech capability that enables computer-generated voice messages to be generated from text. ArcIMS mapping is seamlessly integrated into the notification system providing a geo-referenced reverse look-up capability. Message 911 is also integrated with the Ensco Sentry Sensor suite of products so that it is able to receive a CBRN plume and then notify all residents within the affected area.

Asset tracking capability: LunarEye is a COTS hardware / subscription service that is tightly integrated into PRISM. LunarEye provides an asset tracking capability based on GPS position data and cellular telephone network information transmission.

Any asset with a LunarEye asset-tracking device installed will report its location back to the PRISM server. This feature provides an invaluable command and control, and situational awareness capability for tracking and monitoring the location and movement of emergency response units and first responders such as fire-rescue units, police, HAZMAT, and EMS teams. The asset tracking system information is passed over the cellular telephone control channels, so that user saturation of the network will not prevent the information from reaching its destination.

Comparative summary of competing decision support systems

Based on the requirements in the TRADOC Force Protection Operational and Organizational (O&O) document, and on the criteria outlined in the previous paragraphs, PRISM provides the largest set of capabilities in comparison to the other installation security systems outlined in this paper. Both JPEN and JWARN, while providing valuable capabilities that fulfill a portion of the requirements, do not provide the depth of capabilities necessary to be considered installation security decision support systems. ASOCC is a robust system that provides many of the required capabilities outlined in the TRADOC Force Protection O&O Plan. However, ASOCC does not meet the level of accessibility necessary for many organizations and agencies due to its high cost and application-based nature. PRISM's web-based design and relative low cost provides the greatest level of accessibility. It is ideally suited for deployment in federal, state, and local government agency Installation Operation Centers (IOCs), Emergency Operation Centers (EOCs), and Crisis Management Centers (CMCs). PRISM uses the XML open standard protocol to pass information across the network and can be easily configured for

compatibility with other HTML or XML open standard DSS systems. PRISM provides a "Common Operational Picture" across agency, organizational, and installation boundaries. PRISM is highly scalable: every PRISM server and client can be associated vertically and horizontally with other PRISM servers. None of the other installation security decision support systems provide the comprehensive set of capabilities offered by PRISM, while also being highly accessible and cost affordable. PRISM is a complete package that has already seen limited deployment.

In summary, the most important benefit of PRISM is its accessibility, in that it provides a web-based, distributed solution that does not require significant investment by every organization that requires access to the force protection information provided by a DSS.

Conclusion

The acquisition, development, and fielding of the four installation security systems detailed in the previous paragraphs are each being undertaken by different Department of Defense organizations and agencies in parallel efforts without any coordination among the programs. Parallel efforts, when the goal is testing and evaluation, are typically a good thing because it allows best-of-breed technologies to be developed and identified. Under other circumstances, such as when national security is at stake, parallel effort without central coordination is not a good thing because incompatibility and duplication are the byproduct. This is the situation that is occurring today.

There is no coordinated effort or central control by any agency or organization within the Department of Defense or the Department of Homeland Security to ensure that compatible and interoperable, installation security DSSs are being acquired and fielded. Further, no effort is being made to ensure that the DSSs currently being identified as solutions will provide the level of accessibility necessary to adequately assure Homeland and installation security. One agency must be delegated responsibility for ensuring that all installation security DSS solutions are compatible, interoperable, and accessible. The security of the United States will remain at risk until these measures are taken.

Bibliography

[1] **USJFCOM Glossary**. http://www.jfcom.mil/about/glossary.htm 12 March 2004

[2] DoD Joint Staff, Combat Support Directorate, notices. http://www.defenselink.mil/privacy/notices/js/JS008CSD.html, 8 March 2004

[3] **Federal Register** / Vol. 68, No. 187 / Friday, September 26, 2003 / Notices, http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-24358.pdf, 12 March 2004

[4] SBCCOM Online. JWARN Program Description. http://www.sbccom.apgea.army.mil/products/jwarn.htm. 5 March 2004

[5] Capt. Phil East, Norfolk (Va.) Fire/Rescue Department, **Testing Technology against Terrorism**. Homeland Security ATD Organization. http://www.homelandsecurityactd.org/downloads/ACTDArticle.pdf 8 March 2004

[6] Maj. Gen. Whelden, Craig B. Deputy Commander, U.S. Army, Pacific Command, **Defend America**, http://www.defendamerica.mil/articles/jul2002/a071902a.html, 13 March 2004