



INCIDENT MANAGEMENT SYSTEM TECHNOLOGIES

WHITE PAPER

25 October 2004

Prepared By:

CACI Technologies Incorporated

745 Hope Road

Eatontown, NJ 07724

Phone: (732) 578-5200

Fax: (732) 578-5201

<http://www.caci.com/>

This White Paper includes CACI International proprietary data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this technological approach. This restriction does not limit the recipient’s rights to use information contained in this data if it is obtained from another source without restrictions. The data subject to this restriction is contained on sheets marked “Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.”

TABLE OF CONTENTS

1.0 Understanding the Challenge..... 3

1.1 Background 3

2.0 IMS INDUSTRY BEST PRACTICES 5

2.1 History of IMS..... 5

2.2 Unified Command Concept..... 6

2.3 The Incident Management Lifecycle 8

2.4 Emergency Operations Centers 9

3.0 CACI IMS SOLUTION: ARCHITECTURE, PROCESSES AND TECHNOLOGY 11

3.1 IMS Architecture..... 11

3.2 Process Identification and Automation..... 12

3.3 Candidate Technologies 12

3.3.1 Command and Control (C2) Software..... 13

3.3.2 Sensors 16

3.3.3 Communications..... 17

4.0 ABOUT CACI TECHNOLOGIES 18

4.1 CACI Corporate Overview 18

1.0 UNDERSTANDING THE CHALLENGE

1.1 Background

Emergency Operations Center/ Incident Management System (EOC/IMS) programs represent comprehensive efforts by governments and corporations to ensure the safety and security of the public, critical facilities, employees, visitors, vendors, and business operations. IMS architectures are developed for the purposes of Security Systems Monitoring and Response, Emergency Management (EM) and Continuity of Operations (COOP). EOC/IMS implementation can be accomplished by leveraging an architecture that leverages Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) technologies in a “System of Systems” Enterprise Architecture. This White Paper presents an architecture solution based on a multi-tiered, network-centric source of information sharing to assure a Common Operational Picture (COP) and improved Situational Awareness (SA) between those charged with EM operations and various operating organizations and locations.

Typically, the EOC serves as a key location for the operation of the IMS. The EOC will support emergency management operations at the Headquarters (HQ) level, across multiple operating agencies, and across multiple external agencies involved in planning and response to incidents and emergencies within the client’s organization’s various locations.

The goals for an EOC/IMS initiative typically include, but are not limited to:

- Ensuring the EOC has the ability to monitor input from multiple, geographically distributed locations in real time and can facilitate response operations as required
- Providing a global monitoring capability and data display, implementing incident management standards and easy information management
- Leveraging existing data systems within the company or organization
- Implementing a highly scalable system that allows incremental expansion
- Providing complete lifecycle support services, including development, fielding, integration, and training
- Establishing Standard Operating Procedures (SOP’s) for end user reference and implementation
- Integrating SOP’s into the EM environment
- Incorporating Information Security best practices to safeguard proprietary organizational information. The IMS must handle critical and sensitive information that needs to be safeguarded and protected from compromise or unauthorized access.

CACI Technologies can assume complete responsibility for planning, designing, and implementing IMS system architectures. CACI offers a comprehensive systems engineering and acquisition approach that will also include a sustainment model for training and maintenance.

In close coordination with the client organization security and technical support staff, CACI typically provides the following major services to successfully plan, design, and implement an organization's IMS/EOC systems:

- Project management oversight
- Detailed requirements analysis
- An analysis of technical alternatives to meet system requirements
- Develop an operational, system, and technical architecture design based on requirements analysis, alternatives analysis, and coordination with the client organization technical staff
- Procure (or assist in the procurement) of system components
- Configure, install and test all system components
- Document all configuration information
- Support training, on-going operation, sustainment and maintenance of the system.

In the balance of this White Paper, CACI will demonstrate its understanding of the nature and scope of an EOC/IMS project, an intimate familiarity with the concepts, best practices and enabling technologies supporting IMS, an Enterprise-level architecture for a comprehensive EOC/IMS system, and a discussion of the requisite components that comprise the EOC/IMS architecture.

2.0 IMS INDUSTRY BEST PRACTICES

In this section, CACI offers a brief overview of Incident Management System best practices. Starting with the genesis of IMS as a concept, we will illustrate how IMS concepts and operations can be supported by comprehensive technology architecture. When this architecture is reviewed against a client organization's specific operational requirements, a system design composed of an integrated hardware and software product suite can be developed and implemented.

2.1 History of IMS

In the 1970's, California resources were severely taxed by major wildfire outbreaks. These incidents required the cooperation of multiple agencies that were not used to working together. Many agencies competed for supplies and equipment in a resource scarce environment. The California experience revealed several key findings:

1. There was no clearly identified leader or incident manager
2. There was no basic organizational structure for chain of command and span of control
3. There was no common terminology
4. There was no communications system
5. There was no system for allocating resources.

A system was subsequently developed that could resolve the major issues of coordination and resource allocation in a wildfire or disaster event. The resulting product, the Incident Command System (ICS), evolved into today's Incident Management System (IMS.) IMS provides a management boilerplate for diverse agencies to work together. IMS includes a core set of concepts, principles, and terminology for incident command, multi-agency coordination, management of resources and incident reporting.

IMS exists for a very specific set of purposes:

1. Ensure the safety of people (public, responders, staff, visitors, vendors, customers, neighbors)
2. Ensure the protection and continued viability of critical infrastructure, public utilities, and corporate facilities
3. Ensure the continuity of government or business operations, i.e., the government agencies' ability to continue to provide public services, or a corporation's ability to continue to generate revenue.

IMS is based on five basic elements. There is an incident manager (with a management staff) that coordinates operations, logistics, planning and administration. The system is diagrammed in Figure 1.

- The Incident Manager is responsible and accountable for all aspects of the incident or events, and is directly responsible for all sectors not delegated.

- The Operations Element coordinates the tactics and/or tasks needed to accomplish assigned objectives.
- The Logistics Element supports of all elements in the IMS, such as equipment, supplies, communications, food/water, and facilities.
- The Planning Element devises long and short term plans, maintains status boards, and tracks resources.
- The Administration/Finance Element records workers' compensation, personnel records, payroll and finance records. Nobody appreciates administration until it's time to get paid or get reimbursed.

**The National Incident Management System (NIMS)
Organizational Response to Emergencies**

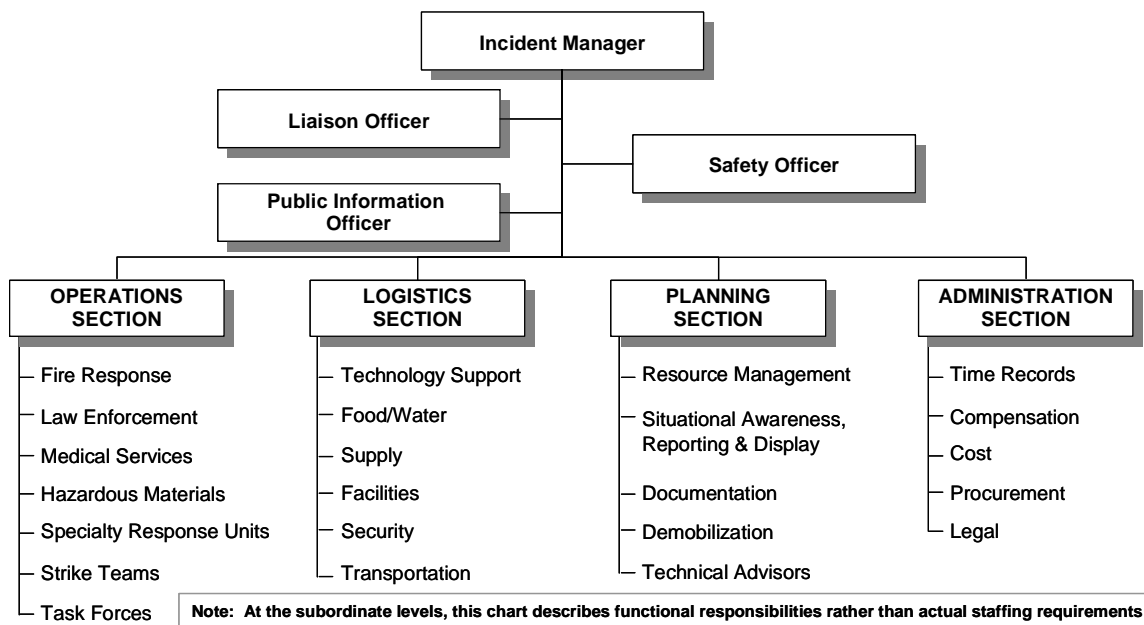


Figure 1—National Incident Management System

In the wake of the events of 9/11/01, President George Bush issued Homeland Security Presidential Directive Five (HSPD-5), which directs the incorporation of a single, comprehensive approach to domestic incident management, which is the IMS described above. IMS is applicable to terrorist attacks, major disasters and other emergencies. IMS fosters coordination across all levels of government and promotes partnership with the private sector. Obviously, any private sector entity developing an Emergency Management operation would be well served in incorporating the same Incident Management System that would be used by government organizations and agencies responding to an incident involving a corporate property.

2.2 Unified Command Concept

Although a single Incident Commander normally handles the command function, an ICS organization may be expanded into a Unified Command (UC). The UC is a structure that brings together the "Incident Commanders" of all major organizations involved in the incident in order

to coordinate an effective response while at the same time carrying out their own jurisdictional responsibilities. The UC may be used whenever multiple jurisdictions are involved in a response effort. These jurisdictions could be represented by geographic boundaries, governmental levels, functional responsibilities, statutory responsibilities, or some combination of the above. When it becomes necessary to establish a UC, the UC replaces the Incident Commander function and becomes an essential component of an ICS. The UC links the organizations responding to the incident and provides a forum for these entities to make consensus decisions. Under the UC, the various jurisdictions and/or agencies and non-government responders may blend together throughout the operation to create an integrated response team. The UC is responsible for overall management of the incident. The UC directs incident activities, including development and implementation of overall objectives and strategies, and approves ordering and releasing of resources. Members of the UC work together to develop a common set of incident objectives and strategies, share information, maximize the use of available resources, and enhance the efficiency of the individual response organizations.

The ICS/UC maintains its modular organizational structure, so that none of the advantages of the ICS are lost by the introduction of a UC. (See Figure 2)

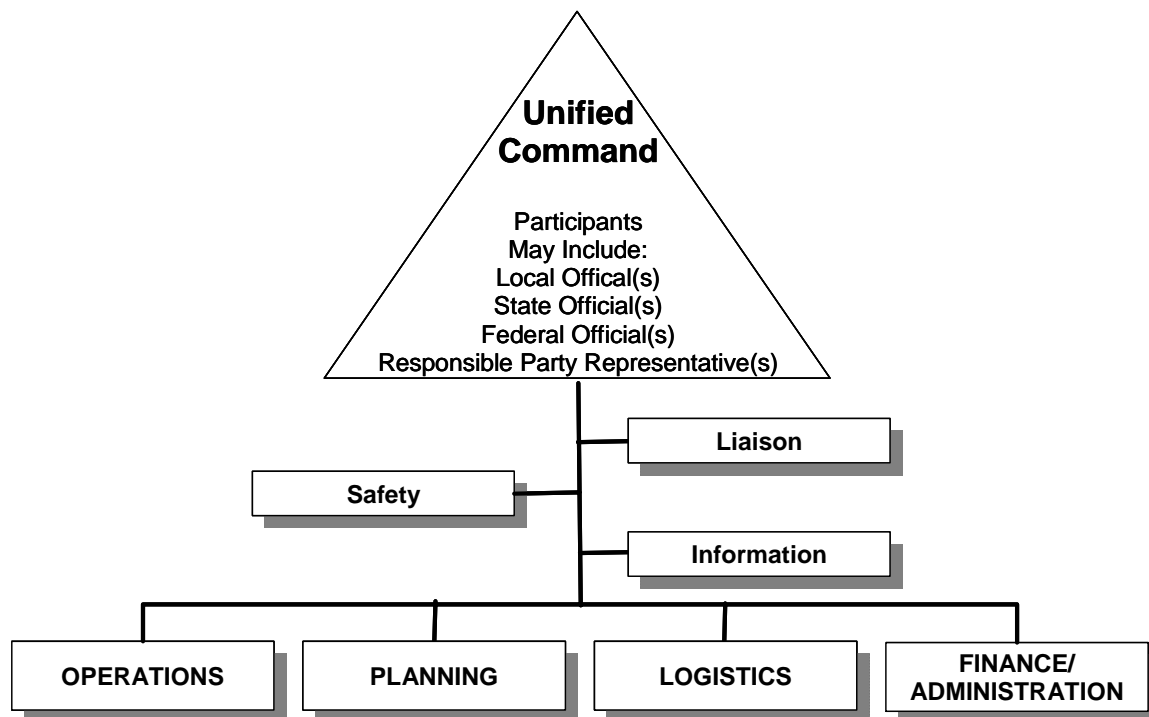


Figure 2—Relationship Between ICS and UC

2.3 The Incident Management Lifecycle

Under the National Blueprint for Homeland Security, there are a series of domains associated with an Incident Management Lifecycle that guides the activities of those charged with managing domestic emergencies. As outlined in Figure 3, those tenets are to Prevent, Protect, Respond, and Recover. Figure 3 also shows how key technology systems and products can be integrated to support operations throughout the Incident Management lifecycle.

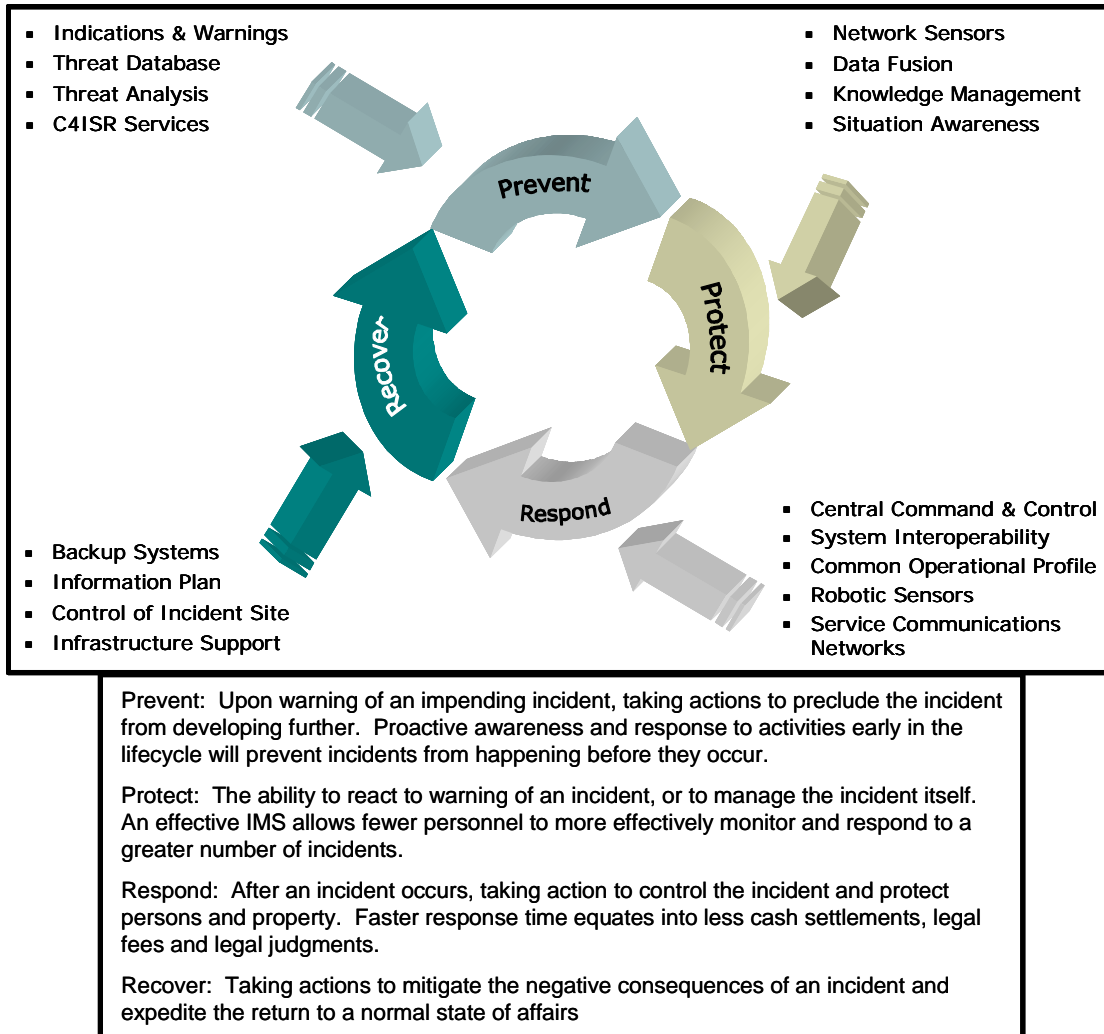


Figure 3—National Blueprint for Homeland Security

When the lifecycle is examined as a timeline, (Figure 4) a series of events unfolds that shows how an infrastructure must be established to maintain situational awareness, develop a common operational picture, react to unfolding events, and assess the efficacy of actions. Organizations then have the option to introduce a variety of systems and technologies to support their emergency management efforts. These systems can range from very unsophisticated (e.g., pen and paper, 3 ring binders, whiteboards, telephones and radios) to very sophisticated (e.g. networked based command and control systems, automated analysis and decision support tools, large screen audio/visual display systems, online collaborative tools and digital handheld devices).

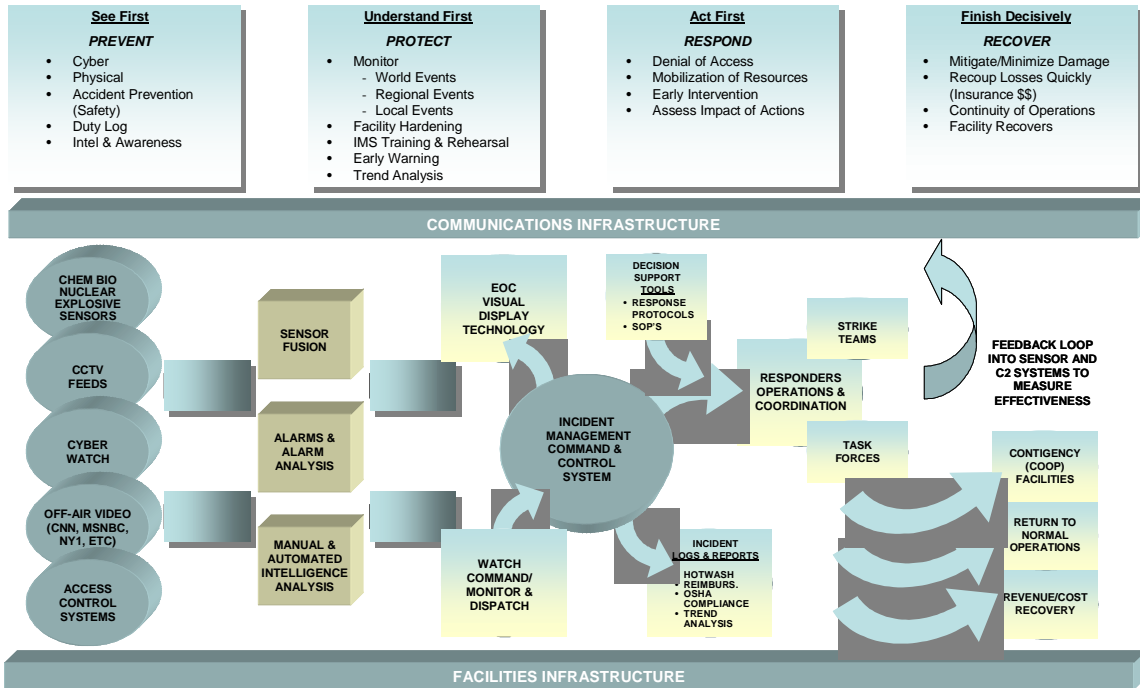


Figure 4—Incident Management Lifecycle

2.4 Emergency Operations Centers

The EOC (Figure 5) serves as a key location for the operation of the IMS. The EOC/IMS support emergency management operations at the HQ level, across multiple operating agencies, and across multiple external agencies involved in planning and response to incidents and emergencies at various locations.

The EOC is usually constructed with the appropriate IT hardware, software, networking, large screen displays, and ancillary support technologies so that it will be able to perform emergency management functions. The main function of this center is to monitor, control, manage and coordinate emergency incident response, provide crisis management and expert advice and logistical services to involved agencies and organizations.

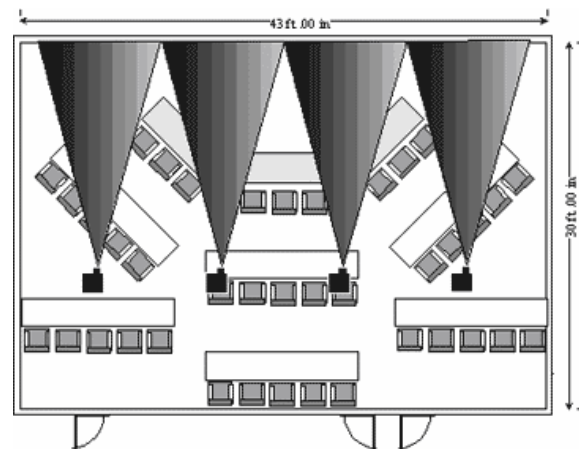


Figure 5—Notional EOC Configuration

Located within the EOC will be staff, facilities and technologies, which may include dispatchers, supervisors, Incident Management System staff, telecommunications facilities, data communications, Incident Management System systems, direct links to other emergency services, numerous video feeds, alarm circuits, recording equipment, Geographical Information Systems (GIS), Computer Aided Dispatch (CAD) and other services. The data processing equipment housed in this facility will provide Internet access,

office automation support, E-mail and all other automated services. The entire emergency management and data center operation must be made fail-safe by implementing a remote emergency operations center and data co-location facility.

The facility, as defined, would be the building and building support systems enabling the Incident Management System architecture. These systems include power and lighting, environmental control, mechanical systems, plumbing, architectural layouts, furniture, information technology centers, and special physical hardening systems to enable a certain degree of protection from man-made or naturally occurring disasters. Also supporting this facility are administrative offices and conference rooms that enable the EM function. Finally, a mobile command post provides a field-ready, deployable IMS capability.

To assure uninterrupted continuity of operations (COOP) for the EM function, the primary site is configured with system level redundancies. If the nature of hazards associated with locating the EOC in a prime target area, (e.g., a corporate HQ in NYC), emergency managers also consider a backup/redundant location where the activities of the EOC and IMS can be carried out should continued operations in the main EOC become untenable. In the event the primary IMS Center is removed from service (planned or otherwise), emergency management organizations should also define a secondary location that can operate in a fully functional mode, replicating all the services and support elements of the primary facility. This capability could be provided by a fully functional “Hot Site” which could be used immediately, with minimal work required to transfer operation to this site. Alternatively, it could be incorporated into a backup EOC established at a subordinate organization’s facility. In the design and operation of the Incident Management System architecture there can be no dependencies between various locations that would impair operations should one of the sites become unavailable. All communications and data processing would be available at multiple locations.

CACI recognizes that control of security and EM EOC/IMS initiatives at many organizations, whether government or corporate, is undergoing a paradigm shift from locally based security control to a centralized, global awareness approach. Operating divisions frequently span multiple operating regions, creating a complex, geographically distributed enterprise organization. Previously, each operating unit or division was responsible individually for incident management and notification of a centralized authority was inconsistent and often limited to email or fax, if at all.

There is a strong analogy here to the migration of core enterprise Information Technology (IT) assets (e.g., email systems) from an operating unit-centric model to a centralized corporate IT infrastructure. As an IT Systems Integrator, CACI is well suited to the challenges of centralization of corporate infrastructure and can assist with this program through the demonstration of benefits to the operating units from participation and cooperation with global IMS initiatives. The IMS can demonstrate significant cost benefits resulting from centralization of emergency management operations. The benefits of a global security structure need to be strategically “sold” to the various operating units, resulting in the need to phase in the system incrementally.

The IMS must also provide operating divisions with cost impact analysis for security issues, assessing impact and issues by region, so appropriate budget resources can be focused against most pressing issues. The IMS must collect and report on a yet-to-be-defined set of security performance metrics.

3.0 CACI IMS SOLUTION: ARCHITECTURE, PROCESSES AND TECHNOLOGY

3.1 IMS Architecture

In a very complex organization with a large area of responsibility (AOR), there is a greater need for an integrated, seamless, intuitive, and easy to use IMS architecture. CACI Technologies has developed a broad reaching architecture for Incident Management support that encompasses the various functional and system elements demanded by an Emergency Management operation and allows us to assess candidate technologies for insertion into the model. This architecture is presented in Figure 5.

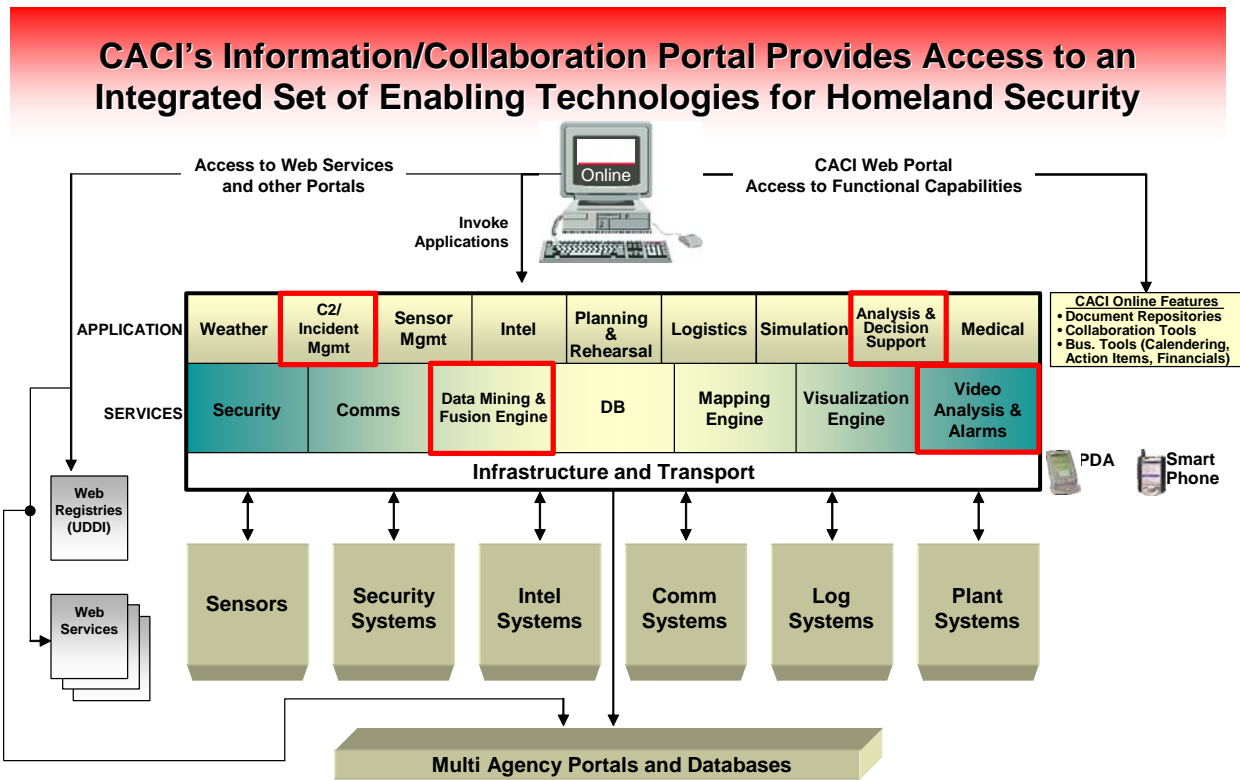


Figure 6—CACI Incident Management System Architecture

CACI has found that vendors have invested a great deal of development effort to bring products to market to support IMS. While many vendors claim to provide comprehensive Incident or Emergency Management solutions, CACI has found that each product actually fits into a niche in the overall architecture. CACI's expert ability as a Systems Integration company allows CACI to assess each products strengths and weaknesses and categorize them into the appropriate functional niche in our architecture. CACI further leverages its ability in web-portal and software development to allow us to integrate the individual products into a holistic Emergency Management environment required by its customers. For a potential client organization, CACI would perform a detailed requirements analysis, analyze alternative technologies, and further define the boundaries within our EM architecture that will best support the client organization IMS requirements.

3.2 Process Identification and Automation

For the IMS architecture modeling, CACI can use the Popkin System Architect V9 tool. This tool facilitates business process modeling, relational data modeling, and the development of SOP's to map business models to object-oriented software component models. In concert with System Architect, CACI employs the System Level Automation Tool for Engineers (SLATE), which allows for the capture and management of performance documents that are a living by-product of the design process, and facilitates trace ability of system, subsystem, and training requirements down through test plans and procedures for acceptance testing. These requirements are linked with the IMS architecture, which allows reconciliation of any differences. Using System Architect, CACI has developed various views of the system "enterprise" (this term is used since the IMS is a part of larger entity in terms of distributed communications networks, hierarchical procedures and directives, and the collection of various forms of information. The following aspects or views of the architecture are modeled:

- Operational Requirements: These requirements address the actions of staff, standard operating procedures, and information exchange requirements across platforms within the system as well with other systems.
- Functional Requirements: A key element of an IMS will be the response SOP's or the Operations Playbook, which is directly linked to the model described above. CACI develops the playbook, which defines the procedures used by system operators, and the doctrine they employ when conducting IMS operations.

In summary, the use of System Architect and SLATE present an efficient automated approach to implement the IMS framework and to view the larger picture of the enterprise the IMS must operate within. In addition, the tools facilitate a straightforward way of translating requirements into software design, where in this case, SOP development is a key activity in the project and one that represents significant risk. The use of Popkin Software and the SLATE tool reduces this risk and improves collaboration among the design team participants.

3.3 Candidate Technologies

CACI Technologies offers exceptional depth of capabilities in assessing, selecting and integrating any of a series of products into an architecture that automates required functions. Some requirements CACI imposes on its candidate technologies includes:

- Real time integration and processing of intelligence data
- Automatic feed of info into IMS system (no faxing/retyping/cut and paste from email)
- Scalable while being non-disruptive to current operations
- Expert systems – Smart, Knowledge Management based
- Automation of SOPS
- Web-enabled interface

CACI will complete a requirements analysis documenting the baseline information technology system, including hardware and software on hand and that programmed for acquisition. CACI will identify functional requirements of the system as defined by the client organization. The results of this subtask will be a requirements summary and baseline design for coordination with the client. CACI will perform the following specific activities to define and coordinate system requirements:

Intimate awareness of product offerings in the Homeland Security/Emergency Management marketplace is an integral part of CACI's ongoing business efforts, as well as an organic part of CACI's proposed approach for this project. Under the "Analysis of Alternatives" portion of our approach, and for each of the key goals associated with this initiative, CACI will compare, select, develop and integrate best-of-breed products into a tightly integrated "system of systems" within the budgetary framework defined by the client organization.

CACI maintains overall product neutrality and will act as an honest broker of technology for the client organization. Due to CACI's position as a leading IT Systems Integrator, we are able to leverage that role and enter into agreements as Value Added Partners with several premier products in the Emergency Management venue, and will bring these agreements and relationships to bear for the client organization. These relationships result in very attractive pricing models and ready access to vendor's technical support resources. In addition, CACI's extensive presence in the Federal market allows us to integrate dual-purpose, transferable government technology from the Department of Defense and other federal agencies.

CACI's awareness of the market keeps it abreast of industry analyses, such as the National Institute of Justice' CIMS Software Product Analysis. Since completed in October, 2002, CACI has leveraged this study and updated much of the product research to stay at the front of the IMS product market awareness

3.3.1 Command and Control (C2) Software

The Command and Control (C2) software module is the key engine that drives the EOC/IMS solution. The C2 component will enable the client organization to respond quickly to any crisis situation and deliver coordinated responses based on real-time and historical information. The C2 module will allow users to share a common operational picture by providing real-time access to standardized incident summaries, reports, requests, notifications, directives, annotated maps and resource tracking. The C2 solutions will allow incident participants to post information to, and retrieve information from a commonly accessible operational picture. The C2 tools will be browser-based, easy to use, easy to learn and easily scalable. The information stored and managed by the C2 tool provides access to real-time information that can be simultaneously shared among emergency response teams, decision makers, and organizations during the planning, response and recovery phase of an emergency. The key objectives in the selection of the C2 component is that it meets system requirements as defined elsewhere in CACI's approach, as well as to meet the following key objectives:

- Ensure the EOC staff has the ability to monitor input from various locations real time and to facilitate response operations as required

- Provide robust monitoring capability and data display, implement incident management standards and ease information management
- Implement a highly scalable system that allows incremental expansion
- Provides complete lifecycle support services, including development, fielding, integration, and training.

A host of C2 products exist for integration into EOCs and IMS systems. They span all levels of sophistication, technical complexity, supportability and cost. While all products summarily reviewed by CACI will contribute to the successful EOC/IMS architecture, CACI views the C2 module as the core, driving engine enabling the entire IMS suite.

<u>Candidate C2 Technology Profile</u>	<u>ETeam</u>
	<p>ETeam is structured to support operations along the organizational roles defined by the Incident Command (Management) System. It can be used to implement ICS processes and methodologies. Organization charts, staffing charts and position checklists can be set up and configured to support ICS roles and their implementation on an ongoing or per-activation basis. Workflow associated with situation reports, resource ordering and fulfillment, action planning and public information reports can be configured to support the different functional roles defined by ICS. ETeam also provides organizations with tools that help them standardize their terminology and practices, which are the cornerstone of any successful ICS implementation.</p> <p><u>Incident and Event Database:</u> The ETeam incident and event database provides a complete incident management capability. The Event report is used as a super-incident report, and all incidents related to that event are grouped or sorted by the event. ETeam allows managers to monitor the status of incidents as they are updated, and as new incident reports are created. The incident report form captures critical information such as location, name, status, and time of the incident. The incident report also provides the most recent updates of the incident and logs all modifications or updates made to the report.</p> <p><u>Full GIS and Mapping Functionality:</u> ETeam provides full GIS and mapping functionality, using ESRI's ArcIMS Geographical Information System (GIS). Users can display maps detailing the location, type, and status of events, incidents, resources, facilities, hospitals, shelters, road closures, etc. using dynamic icons. Users can click on an icon to bring up the ETeam report associated with that icon. When viewing the map, a user can pan, scroll, and zoom from the highest level down to detailed street layers.</p> <p><u>Operations:</u> ETeam provides the full spectrum of forms, views, reports, and connectivity necessary to manage the collection, recording, collating, consolidation, and distribution of information. These forms and reports include message logs, incident reports, event reports, alert bulletins, utility reports, road closures, facility and other infrastructure reports, situation reports, public information reports and duty logs.</p> <p><u>Planning and Intelligence:</u> The capabilities mentioned above for Operations ensure that Planning and Intel staff has easy, sorted, and prioritized access to the information they need to do their job. ETeam also gives them the tools needed to manage the analysis of information, assess the results, and provide advice on further action.</p> <p><u>Logistics:</u> ETeam provides robust modules for both resource ordering and resource tracking. These modules help logistics staff manage and coordinate the allocation and distribution of resources. The Resource Request module allows agencies and jurisdictions to order resources, route requests to the appropriate agency or jurisdiction, approve requests and deployments, split requests among available providers, track the status of fulfilling the request, and track the costs associated with the response effort.</p> <p><u>Management/Director:</u> The capabilities mentioned above for Operations ensure that the Incident Managers have easy, sorted, and prioritized access to the information needed to do their job. ETeam also gives them the tools needed to oversee EOC operations, coordinate activity in their area, authorize public information and situational report distribution, and advise the next higher jurisdictional levels. High-level summary views show the big picture for their area, while giving them the ability to quickly find and drill down to detailed information.</p> <p><u>Administration:</u> ETeam also gives Administration staff tools needed to perform the tasks involved in collecting, processing, and disseminating information, and supporting the smooth functioning of the EOC. Various reports allow Administrative staff to track the costs of the response effort.</p>

3.3.1.1 Data Mining and Fusion Engine

The products to be used in this module allow an organization to leverage existing data systems within the company, and to automate existing processes and procedures into IMS SOPs. Products in this module gather information from multiple sources, identify and monitor trend and patterns in data, and provide users a composite view of activity. Candidate products to incorporate this functionality into an EOC IMS are Metatomix Integrated Product Suite and Instaknow, Inc.’s Instaknow-ACE product.

<u>Candidate Data Mining/Fusion Engine Technology Profile</u>	<u>Metatomix</u>
<p>Metatomix’ Surveillance, Monitoring, and Real-Time Events (SMARTE) solution combines real-time integration with semantic web technology. This framework is designed to gather information from multiple sources, identify, and monitor trends and patterns in the data architecture instantly providing users with a composite view of all monitored activity. The SMARTE suite is comprised of three main components that will contribute to the client’s real-time incident management system.</p> <ul style="list-style-type: none"> • The Interchange Platform is a 100% Java-based connectivity layer with an embedded rules engine. It serves as the initial access layer for gathering data from both structured and unstructured data sources. Because of its unique architecture, the Interchange Platform is capable of accepting data in its native format and performing all transformations, translations or intelligent processing functions without requiring modification of the data sources itself (“non-invasive integration”). • The Hologram Store combines the power of semantic web technology with the real-time integration functionality of the Interchange Platform. The Hologram Store advances upon traditional data storage techniques through its use of advanced indexing, schema less data storage, and real-time trend and pattern identification techniques. • The Visibility Dashboard has been developed as a real-time, web-based comprehensive view for effectively monitoring, evaluating, and communicating activity being monitored by the command center. 	

<u>Candidate Data Mining/Fusion Engine Technology Profile</u>	<u>Instaknow</u>
<p>Instaknow-ACE integrates information across silos of disparate data, and creates real time collaboration among people, information systems, and business operations across the Enterprise. Instaknow-ACE implements a client’s custom business rules (logic) without writing additional programming code. Instaknow-ACE automates complex business processes interact with diverse applications, information sources, and groups of people across the enterprise and with partners on the Internet on a real-time basis. Automation and integration is achieved by visually configuring solutions with point-and-click wizards.</p>	

3.3.1.2 Decision Support Tools

In the IMS suite of products, Decision Support Tools automate an organization’s operational playbook by pre-programming Concept of Operations and Response SOP’s into an expert system that directs a “best set of actions” for a particular situation based on the specifics of the occurrence, locations and environmental conditions. Pre-stored knowledge bases are quickly assessed and an action set is generated. Decision Support Tools help establish Standard Operating Procedures (SOP’s) for end user reference and implementation and will integrate SOP’s into the client organization’s environment; consisting of both in-sourced and outsourced security providers. Candidate products for this function will be Critical Situation Management (CSM)’s 4Command product and Instaknow.com Inc.’s Instaknow-ACE software platform.

3.3.1.3 Collaboration Tools

Collaboration tools allow EOC personnel in dispersed locations to interact on-line and real-time to planning and operations. They will ensure the EOC has the ability to monitor input from global locations real time and to facilitate response operations as required. They will assist with global monitoring capability and data display, be part of the IMS toolkit and will ease information management and flow among participants.

Utilization of Collaboration Tool Suites (CTS) begins to address the collaboration and video management requirements of a comprehensive emergency management system. The CTS can provide standards-based services via COTS applications while supporting government off-the-shelf (GOTS) extensions needed to meet DoD or other federal Command/Service/Agency or team unique requirements. CACI integrates CTS as a flexible, integrated set of applications providing interoperable, synchronous, and asynchronous collaboration capability that translates easily to the Emergency Management community while supporting vertical collaborative integration with the well established defense community. US Northern Command (US NORTHCOM) has approved and endorsed CACI's proposal for the use of the Defense Collaborative Tool Suite (DCTS) for use at the local, regional and state level.

For a very low per seat price, DCTS offers a web-based knowledge portal, Situational Assessment Maps for tactical Situational Awareness, and a collaboration monitor providing VTC, virtual whiteboard and chat capabilities. DCTS offers voice and video conferencing, document and application sharing, instant messaging and whiteboard functionality to support response planning. The suite enables two or more distributed operational users to simultaneously participate in the mission planning process without the need to be co-located. With DCTS, emergency managers enjoy the capability to link various command, control, communications, computers and intelligence (C4I) and mission planning systems together through a common interface to share data, conduct collaborative planning and collaboratively consult on information and data at various locations within a region or around the world.

DCTS has demonstrated interoperability and compliance with the DoD collaboration interoperability criteria and has passed interoperability testing at the Joint Interoperability Testing Command (JITC). DCTS is an evolving set of open standards within which compliant products can interoperate. The DCTS program identifies, fields, and sustains a dynamic set of evolving standard collaboration tools that bridge between elements of that community. These Windows-based tools enhance simultaneous, ad hoc crisis and deliberate continuous operational action planning (vertically and horizontally) across echelons of government and other domains that provide operational units and incident managers with simultaneous access to real-time operational, tactical, and administrative information.

3.3.2 Sensors

3.3.2.1 Video Analysis and Alarm

A primary source of sensor data for an EOC/IMS may be CCTV security video from a large number of monitoring points. Video Analysis and Alarm tools will allow the client organization to automatically analyze common behaviors that can indicate a security breach: moving target detection, perimeter/zone violation, suspicious object detection and tower surveillance. This is a

considerable advance over manual monitoring of a multiplicity of displays by security personnel. More effective video screening leads to fewer guards monitoring a greater number of cameras. Proactive alarms will prevent incidents from happening before they occur. Faster response time equates into less cash settlements, legal fees and legal judgments. This capability will enable a capability within the EOC to monitor input from global locations real time and to facilitate response operations as required. Candidate tools for this function are Sarnoff Corporations VisionAlert Suite and Cernium Inc.'s Perceptrak software.

Sarnoff Corporation VisionAlert Suite

VisionAlert transforms conventional security video tools into vision-based, intelligent tools that enhance the awareness of security and EOC personnel and enable more effective responses to threats. VisionAlert analyzes common behaviors that can indicate a security breach: moving target detection, perimeter/zone violation, suspicious object detection and tower surveillance. VisionAlert eliminates false alarms associated with camera sway, snow, rain, vegetation or sensor noise.

Cernium Inc. Perceptrak

Cernium Perceptrak is a CCTV camera screening system and digital recorder that filters out mundane video and detects specific activities or behaviors. It can detect single of multiple persons, fast-moving and converging people, a fallen person, lurking or erratic behavior, single or multiple vehicles, and fast or sudden stopping vehicles.

3.3.3 Communications

3.3.3.1 Information Assurance Tools

It is important the IMS incorporate Information Security best practices to safeguard an EOC's proprietary information. The IMS may handle critical and sensitive information, which needs to be safeguarded and protected from compromise or unauthorized access. In addition to organic information assurance features found in most networked software environments (encryption, passwords, role-based access) a candidate product for more advanced information security would be the VizorNet CryptSec product. CryptSec protects against insider data theft and compromise, illegal cross handling of data among authorized employees, secures Electronic Data Interchange (EDI) with suppliers and protects staff when logging in from remote locations. The user maintains a crypto key with the crypto key server inaccessible to all but authorized network administrators.

4.0 ABOUT CACI TECHNOLOGIES

4.1 CACI Corporate Overview

CACI is an international Information Technology (IT) products and services company now in its 41st year in business. The company delivers client solutions for systems integration, system development, reengineering, simulation services and products, electronic commerce, intelligent document and knowledge management, product data management, web integration services, and information security.

CACI has grown from a two-person software development firm to a diversified corporation with approximately 7,000 employees. CACI headquarters is located in Arlington, Virginia, a suburb of Washington, D.C. The company currently has 92 offices supporting clients across the United States, Canada, and Western Europe. CACI is a financially strong and stable company with no long-term debt. The company has grown steadily to revenues of more than \$850 million in fiscal year 2003.

CACI has delivered billions of dollars' worth of system programs and support to the Federal and commercial sectors. CACI's capabilities span the entire system life cycle, from requirements analysis through design, to implementation and turnkey delivery. CACI IT specialists design, develop, integrate, operate, and maintain a full range of management information systems, automated document management systems, and integrated engineering support systems. We provide value-added, custom-built software. We also reengineer software for migration to new platforms and Web-based configurations.

CACI's credentials in the IT field have been recognized by numerous external organizations, including the following:

- Ranked for the past 4 years as one of the Top 25 Federal Systems Integrators by Federal Computer Week.
- Rated as the largest Washington-based software developer by Washington Business Journal
- Ranked as #43 among Washington Technology's Top 100 Federal Prime Contractors
- Ranked as the Number One systems integrator/reseller in management capabilities and past performance by Federal Computer Week.

For the past 7 years, CACI has worked closely with the Software Engineering Institute (SEI) to continue to improve its management processes for all software-related projects. During that time, an independent company, Technical Assessments, Inc, evaluated us on several projects. On sixteen (16) programs, CACI Federal Systems was rated as functioning at Level 3 of the SEI Capability Maturity Model (CMM). This certification puts CACI in a "best in class" category of companies around the world.

CACI Offers homeland security solutions for knowledge management and information sharing, network services and information assurance, systems integration and development, and intelligence and engineering support. We serve law enforcement agencies such as the Department of Justice and US Customs Service, design and prototype systems that collect

intelligence information, and manage and secure the networks that carry that information. Our technologies include knowledge management tools, sensor systems for airport and border security, web-based security solutions, and simulation tools for counter-terrorism and search and rescue operations.

CACI is currently supporting one of its key client's (US Army) initiatives to leverage proven Defense technologies to improve the "prevent, detect and respond" tenets of HLS for major metropolitan areas and agencies such as the New York City Metropolitan Transit Authority, Port Authority of NY/NJ, Camden County, NJ, and the Delaware River Port Authority. The Camden County program is of direct relevance to IMS goals: we are beginning the development of a county-level incident management system which will include automated SOPs, geospatial mapping tools, and collaboration software that facilitates coordination with NYPD organizations.