



INSTITUTE FOR DEFENSE ANALYSES

A Survey of Mass Warning and Notification Systems

Serena Chan, *Project Leader*

John W. Bailey
Ronald A. Enlow
Elisabeth A. Ferland

March 21, 2017

Approved for public release;
distribution is unlimited.

IDA Document
D-8388

Log: H 2017-000170
Copy

INSTITUTE FOR DEFENSE
ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882



The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task ET-5-4155, "DoD First Responder Communications Interoperability," for Director, C4 Resilience & Mission Assurance. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Gregory N. Larsen

For more information:

Serena Chan, Project Leader
schan@ida.org, 703-933-6563

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

© 2017 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-8388

**A Survey of Mass Warning
and Notification Systems**

Serena Chan, *Project Leader*

John W. Bailey
Ronald A. Enlow
Elisabeth A. Ferland

Executive Summary

This document reports on work the Institute for Defense Analyses (IDA) did for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO).

The objective of the project is to assess the current state of communications interoperability between DoD public safety and emergency management (PS/EM) and United States (U.S.) civilian PS/EM entities, and how that is likely to change as the next generation of public safety information systems is implemented across the nation. Specifically, IDA was asked to “execute a survey of the major DoD systems that participate in the national public safety communications backbone to identify approaches that could be leveraged to achieve a high degree of harmonization and integration.” This paper discusses only the major mass warning and notification systems employed by the civilian sector and DoD to alert individuals. It contains relevant system descriptions, discussions regarding interoperability potential, observations, and conclusions. Subsequent white papers will survey other types of systems (e.g., Computer Aided Dispatch).

Conclusions

This project highlighted one critical obstacle to the realization of a unified DoD system capable of interfacing seamlessly with civilian systems. That obstacle is the lack of a formal requirement approved by DoD and the Services. The difficulty that the absence of a requirement causes was clearly seen in the system descriptions and assessment of current interoperability and the potential for future interoperability. However, U.S. Northern Command (USNORTHCOM) J34 (Homeland Defense and Protection Division) has issued a draft, U.S. Northern Command Enterprise Mass Warning and Notification Concept of Operations (CONOPS), which, when approved, will provide a necessary step forward.

This paper illuminates the heterogeneous state of current mass warning and notification systems. They are a mix of government off-the-shelf (GOTS), multi-Service, Department systems, and commercial systems. They are:

- GOTS:
 - Alert!,
 - IP2;
- U.S. Navy and U.S. Marine Corps:
 - C4I Suite;
- U.S. Army:
 - Keystone:
- Department of Homeland Security:
 - IPAWS;
- Commercial:
 - AtHoc,
 - Everbridge.

We point this out, not as a criticism but simply to illuminate the challenges of achieving a unified DoD system moving forward. The intent is to be unified through interoperability, not by replacing existing solutions with a single solution.

Fortunately, interoperability may not be as big a technical problem as was anticipated. This document includes an example of incident management/mass warning systems that interoperate (Rave Alert and Web-based Emergency Operations Center (WebEOC)) without having experienced significant technical problems. This paper also includes an example of a dedicated interoperability bridge (Keystone), which has successfully demonstrated interoperability across multiple disparate systems. From a purely technical perspective, the interoperability “problem” is eminently tractable given the existence of a requirement. The following table summarizes the interoperability potential of the systems that the IDA team examined.

Interoperability Summary

System	(1) Like-to-Like Interoperability	(2) Interoperability through a Bridge	(3) Direct Interoperability
Alert!	Yes	TBD	Planned with WebEOC
AtHoc	Yes	Yes	TBD
C4I Suite	TBD	Yes	TBD
Desktop Alert	TBD	TBD	TBD
Everbridge	Yes	Yes	Yes
IP2	TBD	Yes	TBD
IPAWS	N/A	N/A	N/A
Keystone	N/A	Yes	N/A
Rapid Notify	TBD	Yes	TBD
Rave Mobile Safety	Yes, through WebEOC	Yes	Yes, through WebEOC
WebEOC	N/A	Yes	Yes

The recent spate of terrorist attacks, shootings, and bombings provides ample incentives for DoD PS/EM to implement the interoperability needed to save lives and property. The DoD CIO has an opportunity to lead a mission-driven force protection effort to provide an integrated capability with the national public safety community.

Contents

1.	Introduction	1-1
A.	Background	1-1
B.	Scope and Approach.....	1-1
2.	System Descriptions	2-1
A.	Alert!	2-1
	System Description.....	2-1
B.	AtHoc	2-3
	System Description.....	2-3
C.	Command, Control, Communications, and Computers and Intelligence (C4I) Suite.....	2-10
	System Description.....	2-10
D.	Desktop Alert	2-11
	System Description.....	2-11
E.	Everbridge	2-12
	System Description.....	2-12
F.	Installation Protection Integration Platform	2-16
	System Description.....	2-16
G.	Integrated Public Alert and Warning System.....	2-17
	System Description.....	2-17
H.	Mission Assurance, Threat Alert, Disaster Resiliency, and Response	2-18
	System Description.....	2-18
I.	Rapid Notify	2-19
	System Description.....	2-19
J.	Rave Mobile Safety	2-21
	System Description.....	2-21
K.	WebEOC	2-22
	System Description.....	2-22
3.	Interoperability	3-1
	1. Alert! Interoperability.....	3-1
	2. AtHoc Interoperability	3-2
	3. C4I Suite Interoperability	3-4
	4. Desktop Alert Interoperability.....	3-5
	5. Everbridge Interoperability	3-5
	6. IP 2 Interoperability Potential/Constraints	3-5
	7. IPAWS Interoperability.....	3-5
	8. MATADRR Interoperability	3-6

9. Rapid Notify Interoperability	3-6
10. Rave Mobile Safety Interoperability	3-6
11. WebEOC Interoperability	3-7
4. Observations and Conclusions	4-1
Acronyms and Abbreviations	AA-1

Figures

Figure 1. The Alert! Notification Dashboard and Alert Notification Example	2-2
Figure 2. Geographic Alerting Capability for Alert, Warning, and Notify	2-3
Figure 3. AtHoc Management Home Page	2-5
Figure 4. AtHoc Alert Template	2-6
Figure 5. AtHoc Accountability.....	2-7
Figure 6. AtHoc DoD Customers.....	2-9
Figure 7. AtHoc Communications System Architecture	2-9
Figure 8. AtHoc Cloud Architecture.....	2-10
Figure 9. Everbridge Customer Base	2-12
Figure 10. Everbridge Function: Assess	2-14
Figure 11. Everbridge Function: Locate	2-15
Figure 12. Everbridge Function: Communicate.....	2-16
Figure 13. WebEOC Example Board.....	2-24
Figure 14. WebEOC Program/Project Management Board.....	2-25
Figure 15. WebEOC COOP Control Panel.....	2-26
Figure 16. WebEOC Severe Weather Notification Board	2-26
Figure 17. AtHoc Technical Interoperability.....	3-3
Figure 18. AtHoc Interoperability – Legacy or Non-IP Integration	3-4
Figure 19. WebEOC Functions.....	3-7

Tables

Table 1. Interoperability Summary	4-1
---	-----

1. Introduction

A. Background

This document reports on work the Institute for Defense Analyses (IDA) did for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO). Both offices (PM-ISE and DoD CIO) are working with the law enforcement, public safety, homeland security, intelligence, defense, and foreign affairs communities to improve the management, discovery, and sharing of counterterrorism, homeland security, and weapons of mass destruction information. They are facilitating responsible information sharing by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices.

The objective of this project is to assess the current state of communications interoperability between DoD public safety and emergency management (PS/EM) entities and United States (U.S.) civilian PS/EM entities, and how that is likely to change as the next generation of public safety information systems is implemented across the nation. Specifically, IDA was asked to “execute a survey of the major DOD systems that participate in the national public safety communications backbone to identify approaches that could be leveraged to achieve a high degree of harmonization and integration.”

This paper discusses the major mass warning and notification systems employed by the civilian sector and DoD to alert individuals. It contains relevant system descriptions, discussions regarding interoperability potential, observations, and conclusions.

B. Scope and Approach

The IDA team reviewed the available literature, including the March 2014 Gartner report “Magic Quadrant for U.S. Emergency/Mass Notification Services,” and concluded that there were no applicable “major DoD systems” in the strict sense of the term.¹ Rather, DoD writ large uses a spectrum of systems, some proprietary and some public. So, in the interest of being inclusive, the team identified 11 systems for assessment:

¹ Roberta Witty, John Girard, and Catherine Goldstein, “Magic Quadrant for U.S. Emergency/Mass Notification Services,” *Gartner Research Note*, 31 March 2014.

Alert!, AtHoc, C4I Suite, Desktop Alert, Everbridge, IP2, IPAWS, Keystone, Rave Mobile Safety, Rapid Notify, and Web-based Emergency Operations Center (WebEOC). The list includes incident management software (e.g., WebEOC), mass warning software (e.g., AtHoc), and interoperability-oriented middleware (e.g., Keystone). IDA contacted the companies that produce the 11 systems above and received responses from or held technical interchanges with Rave, AtHoc, Alert, Keystone, WebEOC, and Everbridge. Information on the remaining systems was extracted from open sources.

Our approach was first to obtain sufficient information to describe each system at a high level and then to assess its potential for interoperability with other PS/EM communications systems (see Chapter 2).

The scope of the descriptions excludes incident detection. Consequently, the descriptions depend upon data supplied by the providing companies, augmented by technical interchanges and face-to-face discussions.

As defined by DoD, “interoperability” is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.² This definition is used throughout this paper.

The interoperability assessment, Chapter 3, comprises two phases: documenting existing (demonstrated) interoperability with any of the other systems, and then, qualitatively discussing the potential for future interoperability with other civilian and DoD systems. In particular, the IDA team looked for instances of: (1) like-to-like interoperability (e.g., AtHoc to AtHoc); (2) interoperability through a bridge (e.g., AtHoc to Keystone to C4I Suite); and (3) direct interoperability (e.g., AtHoc to Everbridge). In addition, instances in which systems have demonstrated interoperability with legacy systems or non-IP systems were noted. This paper concludes with some general observations and conclusions for future approaches to a unified DoD mass warning and notification system.

² Department of Defense, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” DoD Instruction Number 8330.01, 21 May 2014, p. 39.

2. System Descriptions

This chapter describes each of the following systems at a high level and then assesses its potential for interoperability with other mass warning and notification systems:

- Alert!,
- AtHoc,
- C4I Suite,
- Desktop Alert,
- Everbridge,
- IP2,
- IPAWS,
- Keystone,
- Rapid Notify,
- Rave Mobile Safety,
- WebEOC.

A. Alert!

System Description

The Alert! system was a research and development (R&D) project funded by the Naval Facilities Engineering Command (NAVFAC) in response to the high cost of the commercial off-the-shelf (COTS) solutions being implemented at the time. Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific (SSC PAC) produced the first government off-the-shelf (GOTS) prototype.³ In 2014, U.S. Army Tank-automotive and Armaments Command (TACOM) began limited deployments of Alert! on Army sites, and in 2015, the U.S. Air Force Materiel Command (AFMC) and

³ David Franing and Chris Rattray, “Alert! Briefing for the DoD Public Safety Communications Working Group (PSCWG),” PowerPoint Presentation, September 2015.

SSC PAC came to an agreement to deploy Alert! on 10 continental U.S. air bases.⁴ The U.S. Army (G-34) is the current Product Owner, replacing NAVFAC. Alert! is managed in partnership by TACOM Life Cycle Management Command (LCMC) Integrated Logistics Support Center (ILSC) and U.S. Army Armament Research Development and Engineering Center (ARDEC).

The application comprises three major components:

- Web Interface – used by emergency managers to configure the system and send alerts,
- Desktop Client – gives end users the ability to receive alerts and maintain contact information, and
- Web Service – supports real-time client/server communication.

The Alert! system supports desktops alerts, phone messages, Short Message Service (SMS) texts, email, indoor beacons, and Giant Voice.⁵ Because it is a GOTS product, required features are implemented according to DoD specifications and there are no licensing fees. The only cost is for technical support, sustainment, hosting, and telephony services. The notifications are received by clients with the software on their systems. An administrator can use the web application to manage alerts, input templates, and coordinate clients needing notification. Figure 1 illustrates an example notification dashboard and alert notification of the Alert! system.



Figure 1. The Alert! Notification Dashboard and Alert Notification Example⁶

The Alert! system technology can prioritize use of system resources based on the severity of the alerts being sent. Any alert with a higher severity will have higher-priority access to system resources. Another feature of the application is the ability to cancel an

⁴ Ibid.

⁵ ARDEC, “N2C2 Enterprise Mass Warning Notification System Demonstration,” PowerPoint Presentation, 2 February 2017.

⁶ David Franing and Chris Rattray, “Alert! Briefing for the DoD Public Safety Communications Working Group (PSCWG),” PowerPoint Presentation, September 2015.

alert early on in the process. This ceases all communications regarding the specific alert and reduces the potential for false alarms. The infrastructure is built to support new DoD deployments without the need for any local server installations, and the Defense Enterprise Computing Center (DECC) architecture is designed to support a total population numbering into the millions. The Alert! system also supports a geographic alerting capability as depicted in Figure 2.

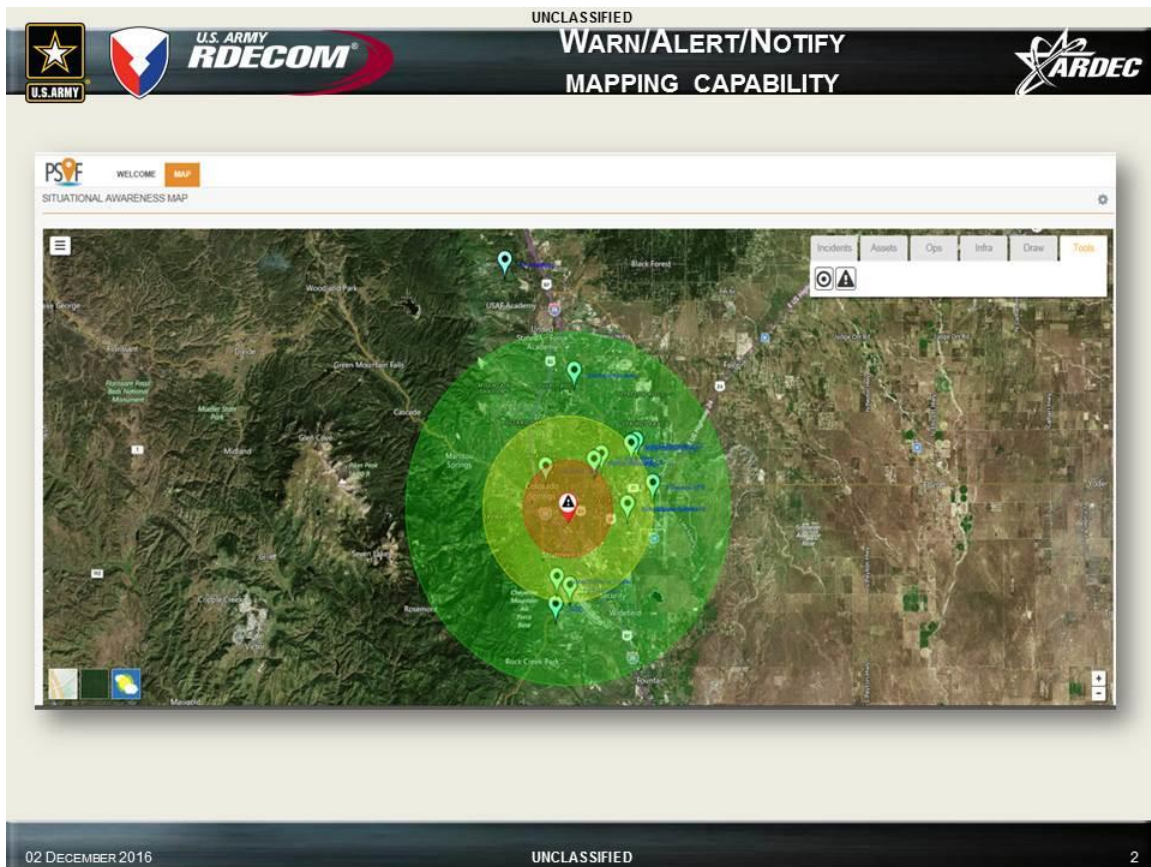


Figure 2. Geographic Alerting Capability for Alert, Warning, and Notify⁷

B. AtHoc

System Description

AtHoc is a Division of the Blackberry Corporation. The AtHoc Crisis Communication technology is a COTS bi-directional⁸ mass notification and networked

⁷ ARDEC, "N2C2 Enterprise Mass Warning Notification System Demonstration," PowerPoint Presentation, 2 February 2017.

⁸ Notifications can be sent to users and user responses can be sent back through the system.

crisis communication system that can be customized for military, government, health care, higher education, and commercial organizations. Notifications can be delivered through a variety of methods, modalities, and devices. The technology is deployed and fully operational within all three Services, the Joint Staff, and the National Guard, in addition to dozens of Federal agencies and multiple universities. Specifically, the AtHoc system has been adopted by a number of civilian companies, including Eastman Chemical; USS-POSCO Industries; Baylor Scott & White Health; the University of California, Los Angeles; and the Department of Homeland Security (DHS).

The AtHoc software is proprietary. The software suite is organized into four components: Alert, Collect, Account, and Connect.

The AtHoc Alert component is designed to allow notifications to be sent to tens of thousands of users securely through a single permissions-based operator interface. Operators can configure the notifications to be delivered through a variety of communication modalities such as text messages, e-mail, automated telephone calls, radio, television, and public address (PA) systems. Each operator can also customize which events trigger the notifications and which can be integrated to monitor physical sensors and with external data sources, such as weather alerts, to automatically trigger notifications.

The standard, XML-based Common Alerting Protocol (CAP) format along with Web Services allows the capability to be easily extended to use new alerting mechanisms. The AtHoc IP Integration Module (IIM) interface allows the software to adapt to new detection and notification systems. The software works with Microsoft operating system's Active Directory—the Lightweight Directory Access Protocol (LDAP)—and it provides a Solution Developer Kit (SDK) interface to integrate with other primary sources of user data, thus making it easier for an administrator to synchronize an organization's users with the technology.

As shown in Figure 3, the management home page for administrators displays the latest alerts, aggregates statistics on system activity, tracks the number of live alerts, highlights the number of online users within the past few hours, contains canned alerts that can be quickly tailored and sent, and provides a navigation panel.

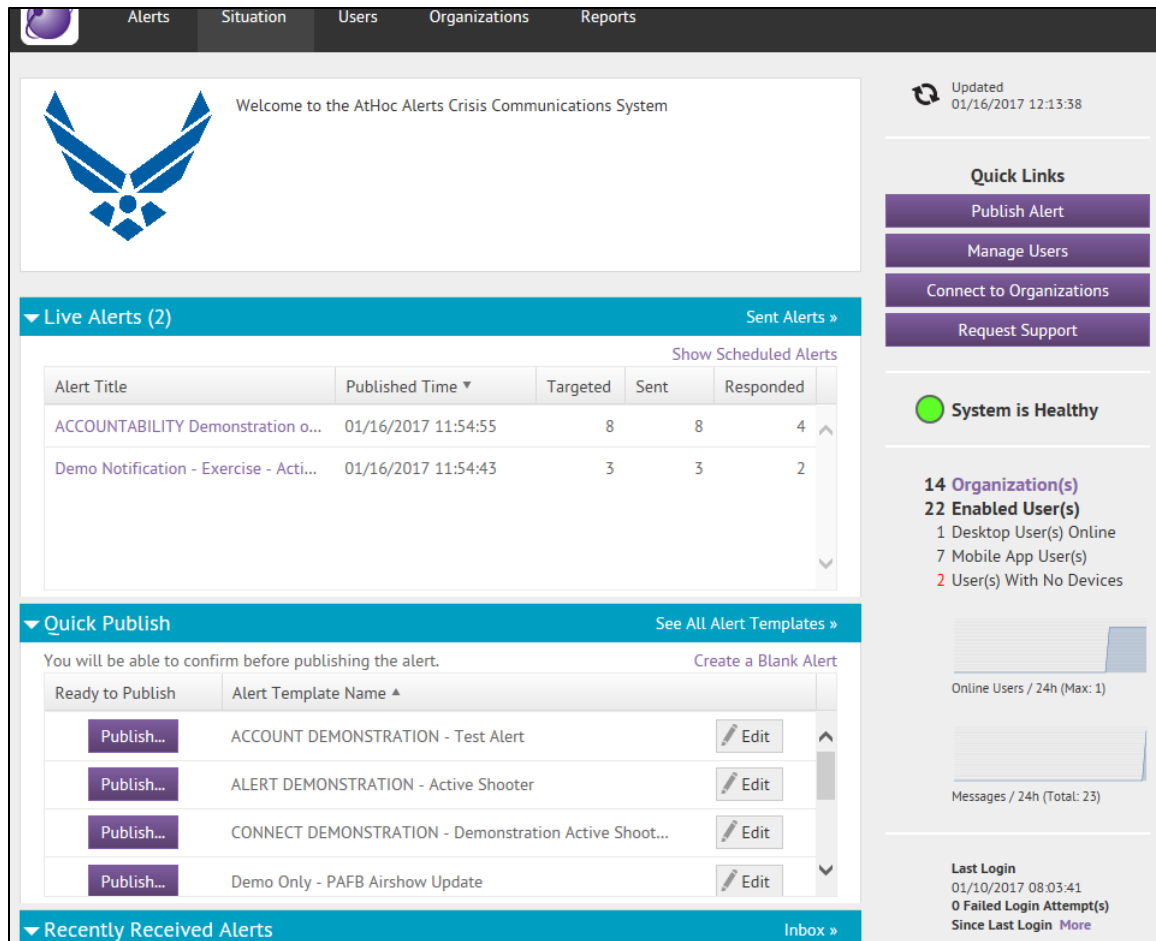


Figure 3. AtHoc Management Home Page⁹

To set up an alert template for rapid publishing, the administrator initiates the creation of the alert template and fills out a preset screen, as shown in Figure 4. A type and severity can be designated for each alert template. Next, a title and body are entered as the default text of the alert template. The targeted recipients are selected via multiple methodologies, including organization hierarchy, customer-defined attributes, and geo-targeting. Then, the types of devices are selected to maximize the effectiveness of the alert. The delivery order (priority) is also set for multiple contacts of the same type according to operator preference. Once all necessary information has been entered, the alert template can be saved and later referenced and customized for rapid alert dissemination.

⁹ Mike Brown, Pete Frasco, and Matt Moore, "AtHoc Crisis Communications Discussion and Demonstration for IDA," Blackberry demonstration given at the Institute for Defense Analyses on 10 January 2017.

Alert Templates > **ALERT DEMONSTRATION - Active Shooter** Cancel Settings Save

Severity High **Type** Safety English (US)

Title * Demo Notification - Exercise - Active Shooter - Lockdown - Lockdown - Lockdown +

Body Demo only, no action needed. A Simulated Active Shooter has been identified near the Demonstration Air Force Base Main Headquarters, building 201. Lockdown, Lockdown, Lockdown. All personnel are directed to lockdown until further notice. Additional information will be provided shortly. This is a Demo only. NO ACTION NEEDED! +

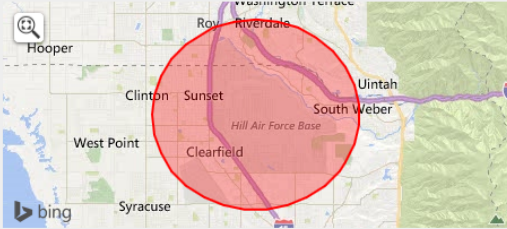
Response Options Custom Response Options

1	Acknowledge - I am locking down +	☐ Call Bridge -
2	I need assistance +	☐ Call Bridge -
3	I am not on the installation +	☐ Call Bridge -

[Add Response Option](#)

More Info Link Test URL

Location



Edit
Remove

Figure 4. AtHoc Alert Template¹⁰

As shown in Figure 5, the AtHoc software also allows operators to track information once an alert has been sent, such as how many alerts have been sent and how many were successfully delivered to the recipients. If an alert does not reach some of the intended recipients, that could indicate a problem with specific delivery devices or a backlog due to high traffic volume on cellular towers. Because alerts can be set up to request recipients to respond, those results can also be tracked, and users who have not responded to an alert can be easily re-targeted for additional alerting and accountability.

¹⁰ Ibid.

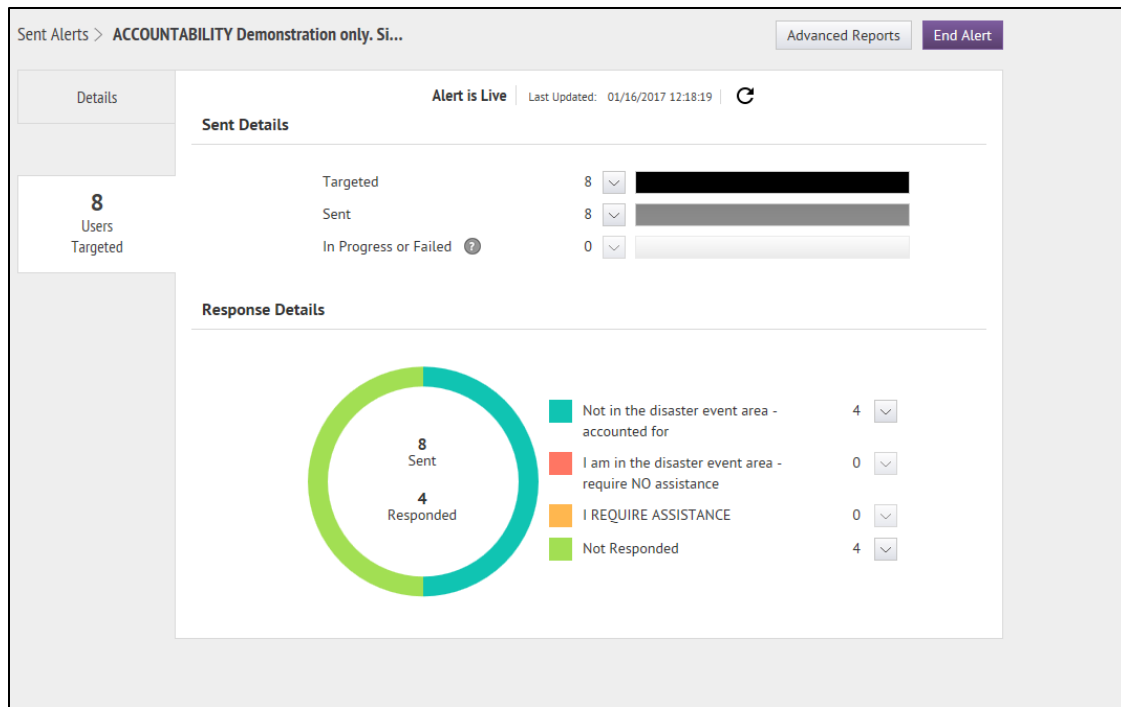


Figure 5. AtHoc Accountability¹¹

Similar to requesting responses from recipients of either text messages or e-mail, individuals who subscribe to the telephony notification subscription services can respond to an alert in real time or receive alert notifications with a callback number. If a recipient listens to the message and responds, then the activity is recorded and can be tracked in a report. Reports can be used by operators and administrators to view statistics and to determine which methods of delivery are the most efficient for their user community.

The AtHoc Collect component is a mobile device application-based capability that allows the organization to gain greater awareness and make better decisions by enabling field personnel to be the eyes and ears of the Emergency Operations Center (EOC). The application is available commercially at the iOS and Android Application Stores, providing personnel in the field the ability to report events with geo-tagged media reports, plus a one-click “duress” button to report emergent situations for rapid response. The operations center can see what is happening at any incident scene, enabling rapid mobilization for a more effective response.

The AtHoc Account component enables real-time visibility into personnel location and status for crisis handling and response. An EOC or the organizational leadership uses Account to request status from select groups or the entire populace. Organizations can

¹¹ Ibid.

account for people after emergencies, recall personnel, and conduct daily mustering. Emergency and organizational management are provided an accurate summary view or detailed delivery report of each alert recipient across the enterprise. Users can also provide unsolicited reports of their current status and location via multiple modalities, including mobile devices.

The AtHoc Connect component enables organizations to create their own secure permission-based networks, establishing interoperable communication with organizations in their hierarchical infrastructure and local area. It allows organizations to discover and invite other organizations to be part of their network and accept invitations to join the networks of others. The invite step ensures that only those organizations receiving permission through an authenticated process are allowed to receive an interoperable notification from the sender. Further, because each organization has a distinct account, the receiving organization always controls how an interoperable notification is targeted to its own users. By leveraging the existing AtHoc Alert component, organizations are able to execute interoperable notification of an event from a single notification input, while ensuring all data is protected with the highest level of security driven by their Information Assurance requirements. To date, 215 DoD organizations, as shown in Figure 6, have established organizational connections. The Communications System Architecture enabling these capabilities is depicted in Figure 7 and Figure 8, which were provided by AtHoc.

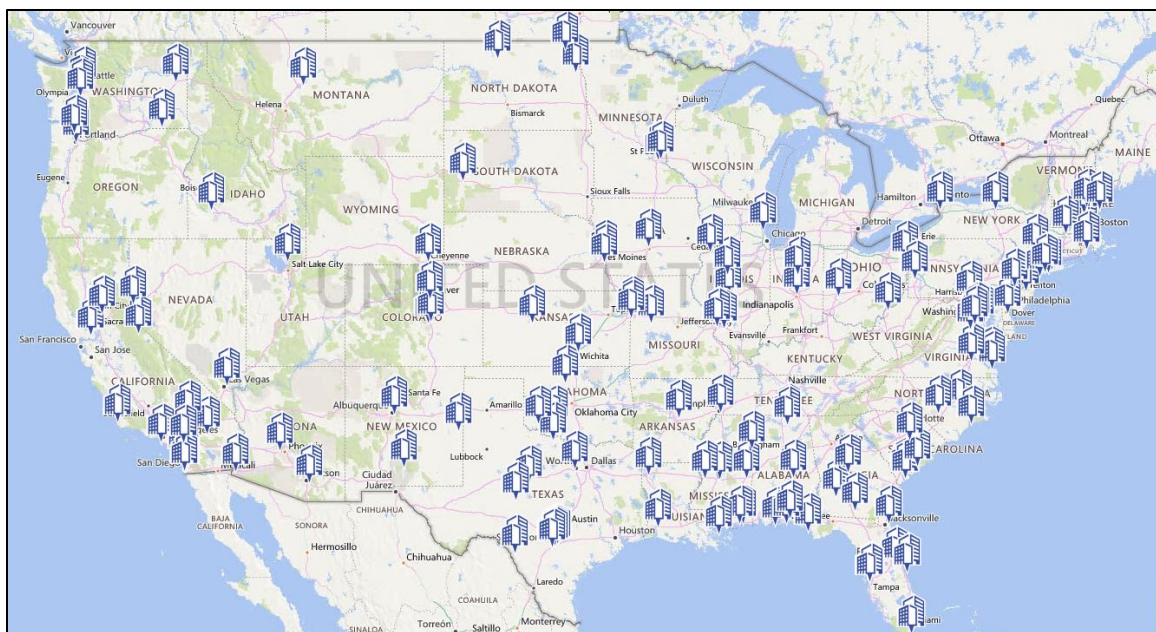


Figure 6. AtHoc DoD Customers¹²

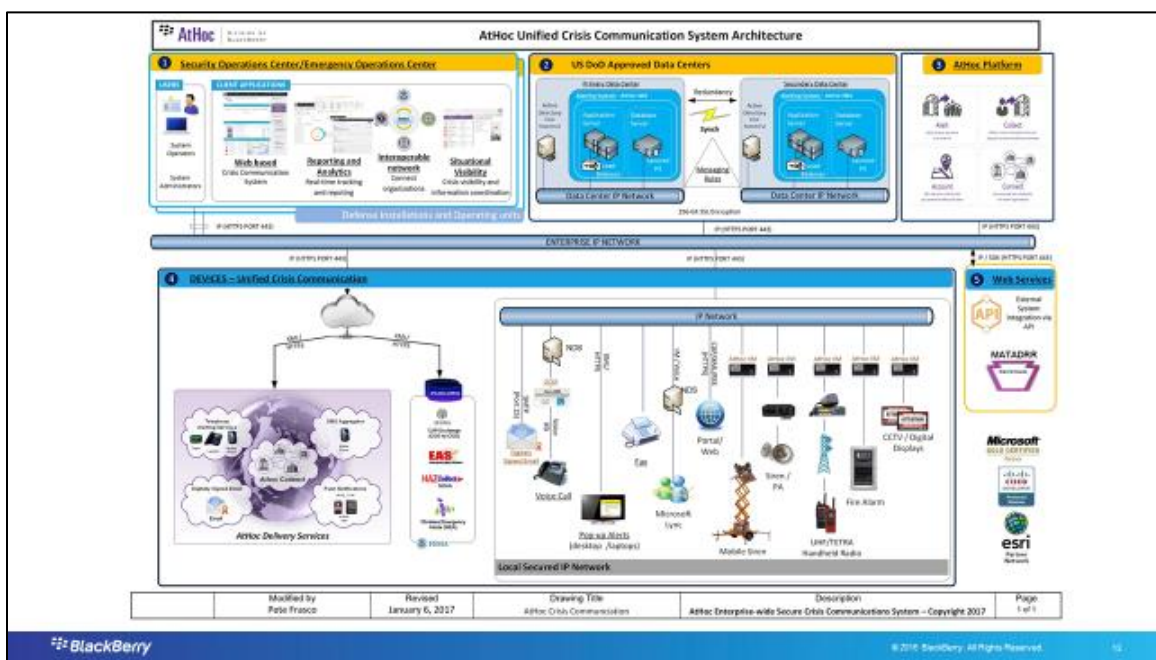


Figure 7. AtHoc Communications System Architecture¹³

¹² Ibid.

¹³ Ibid.

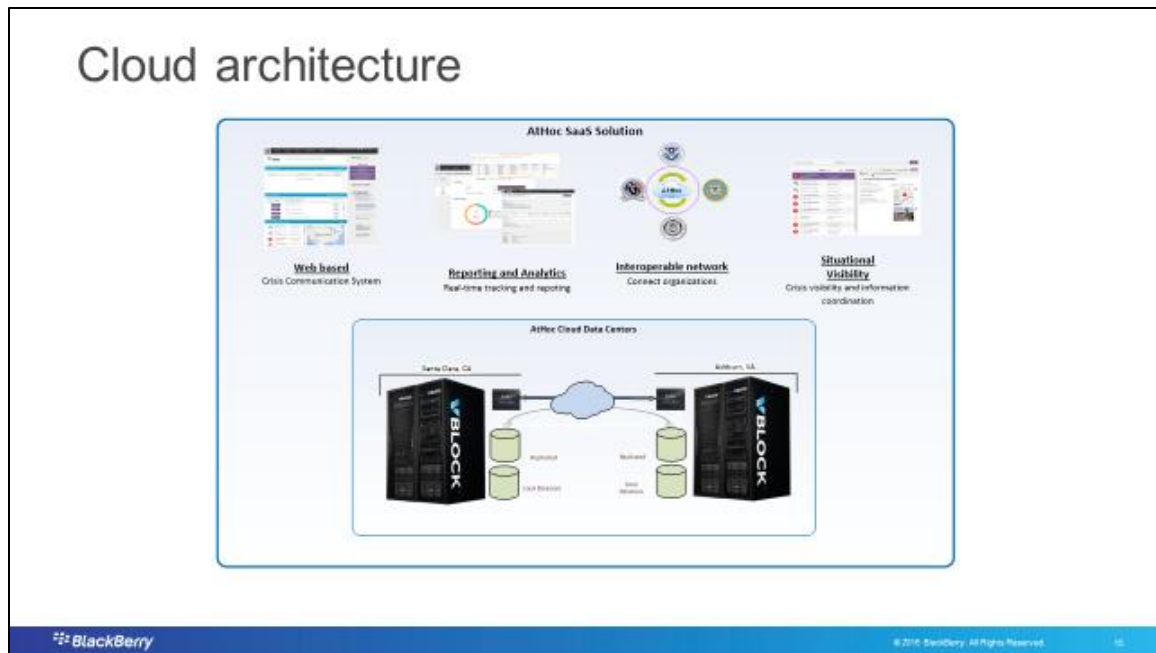


Figure 8. AtHoc Cloud Architecture¹⁴

C. Command, Control, Communications, and Computers and Intelligence (C4I) Suite

System Description

The C4I Suite is a combined U.S. Navy (USN) and U.S. Marine Corps (USMC) capability deployed after the 2009 Fort Hood shooting. It is intended to fill the gaps in DoD's ability to communicate unclassified real-time information across the enterprise. The C4I Suite provides core services for fusing and filtering information from multiple Anti-Terrorism/Force Protection (AT/FP) systems and sensors to provide more complete and actionable information to AT/FP and Emergency Management watch-standers and decision makers. C4I Suite's SharePoint web-based "One Clear Picture" page facilitates installation status reporting on Force Protection Conditions, asset availability, major operations, etc., and it provides system alerts, weather alerts, an electronic Daily Logbook, links to map viewers, and reference materials. SharePoint's discussion board and document-sharing capabilities facilitate real-time user collaboration. The C4I Suite can also integrate 2-D and 3-D geospatial views with a Common Operating Picture (COP), real-time alerts, and events of interest. The three main functions are chat (all levels of the chain of command), dissemination of notices (routine and urgent), and operational status.

¹⁴ Ibid.

Individual C4I Suite accounts are required for participation. Account holders include managers and staffs in the areas of operations, mission assurance, force protection, law enforcement, security and emergency services, and EOC, as well as crisis action team members, and operations center watch-standers. Also included are intelligence personnel working in support of mission assurance, law enforcement, and emergency management personnel.

Regional Operations Centers (ROC) were established to manage operational activities through any operational conditions such as weather, power, and network outages. The four capability areas handled by the ROCs include gathering of regional information, gaining situational awareness, exercising control of forces, and interacting with other government agencies. The ROCs are co-located with the regional commands to provide the capability to oversee and respond to any incident, and they can display and operate in classified, sensitive-but-unclassified, and unclassified modes.

The EOCs were established to manage operational activities through all operational conditions such as weather, power, and network outages. The five functional areas handled by the EOCs include Secure/Non-Secure Communications, the EOC Video Display System, C4I Suite web-based capabilities, Equipment Rack with Vital Power (uninterruptable power supply), and Federal Emergency Management Agency (FEMA) radios. The EOCs provide local commanders the capability to oversee and respond to all incidents and can display and operate in classified, sensitive-but-unclassified, and unclassified modes.

D. Desktop Alert

System Description

Desktop Alert is an IP-based alert technology that shares communications and commands using standard protocols. Desktop Alert, Inc., is a worldwide firm providing enterprise-class, network-centric emergency mass notification systems to private, industrial, military, government, and commercial organizations. Desktop Alert has numerous strategic relationships and partnerships with industry re-sellers. By partnering with Desktop Alert, an organization can rapidly augment critical information delivery.

Desktop Alert already has clients across all branches of the military. The enterprise-class unified alerts management includes the capability to initiate emergency alerts to any warning device via a single web-based interface; integrate user data from disparate data sources; manage a single repository of emergency scenarios; manage permission-based access for operators; enable real-time tracking and reporting; manage integration with multiple delivery devices; manage real-time reports, communications, and video surveillance; and manage DoD Approved Extensible Message and Presence Protocol

(XMPP) Live Instant Messaging. Desktop Alert did not respond to the IDA team’s request for further information.

E. Everbridge

System Description

Everbridge (formerly known as 3n Global and the National Notification Network) is a global provider of Software-as-a-Service (SaaS)-based critical communications and provides, “enterprise software applications to automate the delivery of critical information to help keep people safe and businesses running.”¹⁵ Everbridge began operations in 2002 and is based in Boston and Los Angeles, with additional offices in San Francisco, Beijing, and London.

The Everbridge customer base grew from 867 customers at the end of 2011 to more than 3,000 customers by July 31, 2016. Details about their customer base are depicted in Figure 9, which was provided by Everbridge.



Figure 9. Everbridge Customer Base¹⁶

¹⁵ SaaS is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as “on-demand software.” SaaS is typically accessed by users using a thin client via a web browser.

Everbridge, “Everbridge Overview: Introduction,” PowerPoint Presentation, 25 January 2017.

¹⁶ Everbridge, “Everbridge Overview: Introduction,” PowerPoint Presentation, 25 January 2017.

Everbridge has sold its Unified Critical Communications Suite (UCCS) technology to more than 2,500 private and government clients. These include the Department of Commerce, Department of Veterans Affairs, Department of Defense, U.S. Coast Guard, the U.S. Army (Picatinny Arsenal, New Jersey), and the California National Guard. The technology has also been deployed to several universities, including the University of New Haven and Virginia Polytechnic Institute and State University (Virginia Tech). The UCCS was used during Hurricanes Katrina, Irene, and Sandy, and during the Boston Marathon bombings and manhunt.

Everbridge applications received designation under the Support Anti-Terrorism by Fostering Effective Technology Act of 2002, or SAFETY ACT, and certification by DHS. Everbridge applications are also accredited under the Federal Information Security Management Act of 2002 (FISMA). Accreditation under the Federal Risk and Authorization Management Program (FedRAMP) is expected in 2017.

The UCCS is a bi-directional, SaaS-based, mass emergency notification and communications system. The UCCS is designed to facilitate communication among first responders, emergency managers, and constituents, such as residents in a given city or town, during emergency situations, including terrorist attacks, and non-emergency situations, such as interruptions to a customer's information technology infrastructure.

UCCS customers can transmit mass notifications via pagers, land lines, mobile phones, and e-mail. Notifications can be initiated by the customer via an Internet-connected device or by calling customer support, who will issue the notification on behalf of the customer. The UCCS consists of four integrated modules that are offered in combination or on the basis of customer requirements. The company's critical communications and enterprise safety applications include Mass Notification, Incident Management, IT Alerting™, Safety Connection™, Community Engagement™, Secure Messaging, and Internet of Things.

The Everbridge approach is fourfold, allowing organizations to assess events and determine whether there is a threat, locate the people affected or needed for a response, automate the process of activating procedures and protocols, and communicate instructions to stakeholders in an event. It does this through the series of applications mentioned in the previous paragraph.

a. Assess

As shown in Figure 10, Everbridge aggregates data from several disparate input sources, including front line sensors, people in the field, crime and incident data, social media trends, and weather inputs, among others. The software then uses customer-defined thresholds to trigger any necessary actions.

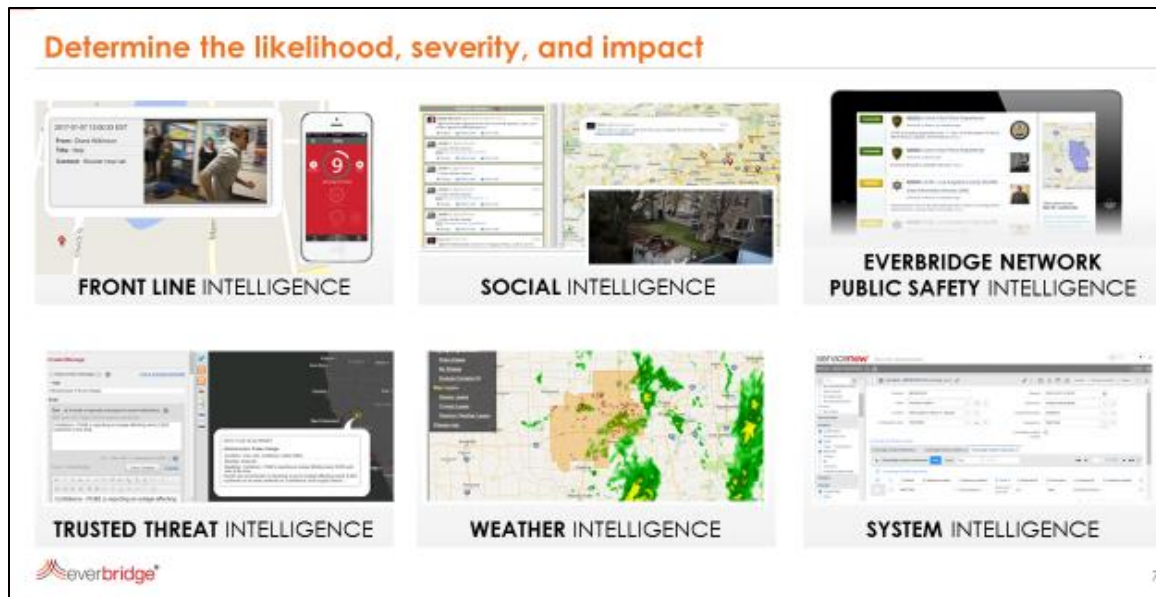


Figure 10. Everbridge Function: Assess¹⁷

b. Locate

Everbridge takes location information far beyond the typical static location information. See Figure 11. Through dynamic location, people can be located based upon several addresses entered into the system, an expected location, the building they last gained access to by swiping their badge, or the Wi-Fi hotspot they last connected to. Everbridge can also locate people by skill. For example, if there is a medical emergency at a school, Everbridge can be used to find and contact all those in the vicinity with a cardiopulmonary resuscitation (CPR) certification. See Figure 11 below for an example of Everbridge's Locate service view.

c. Automate

Most active shooter incidents are over within six minutes or less, so time matters with regard to emergency notification. By outlining a detailed set of standard operating procedures when subscribing, Everbridge customers can set automatic triggers to cut down on time and, hopefully, save lives.

¹⁷ Ibid.

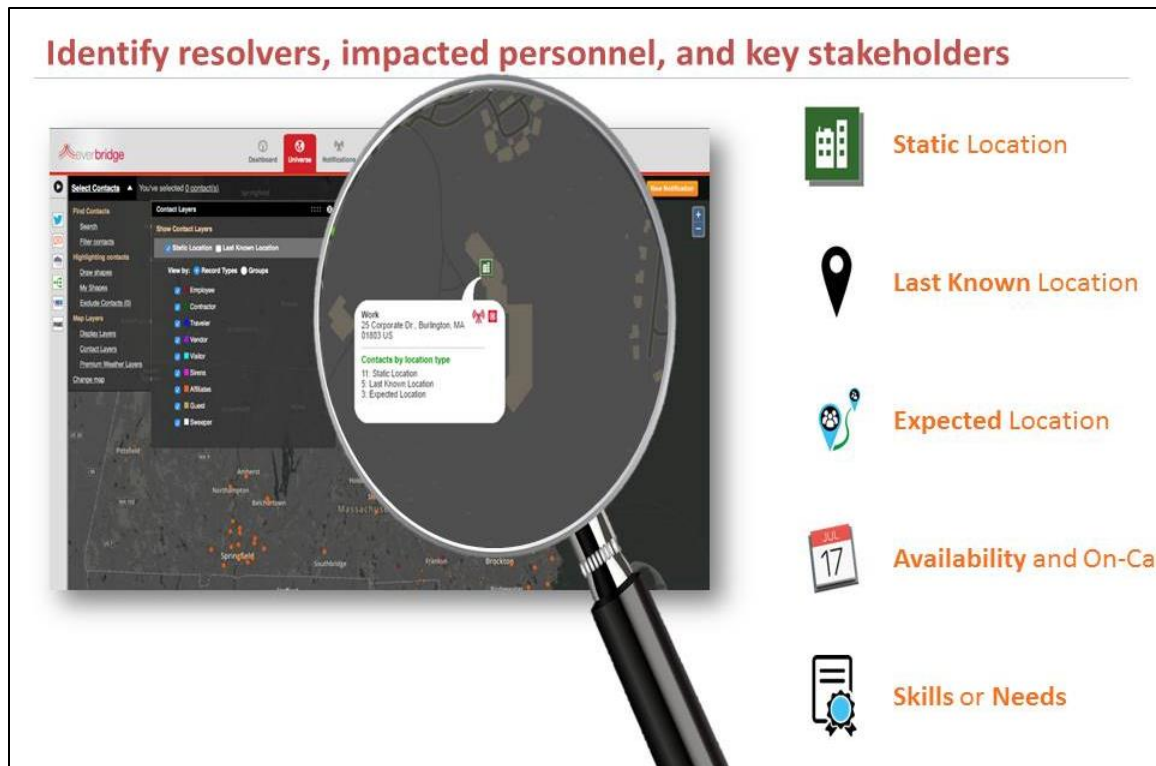


Figure 11. Everbridge Function: Locate¹⁸

d. Communicate

Communication can be initiated in one of two ways, by the organization or by an individual in distress. The communication can become two-way if information needs to be shared or updated or instructions need to be given, see Figure 12.

The Everbridge system was used in 2012 to send over 10 million messages to residents during Hurricane Sandy. During the Boston Marathon bombings in April 2013, the city of Boston used Everbridge for its critical communications. Everbridge relayed information to business operators, employees, firefighters, hospital staff, police, and residents after the explosions and during the lockdown of Boston, Watertown, Waltham, and surrounding areas.

The company's platform sent over 1 billion messages in 2015.¹⁹ It offers the ability to reach more than 200 countries and territories, with secure delivery to over 100 different types of devices.²⁰

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Ibid.



Figure 12. Everbridge Function: Communicate²¹

F. Installation Protection Integration Platform

System Description

The Installation Protection Integration Platform (IP2) system is an emergency response and information management system focused on the incident-command-post-to-emergency-operations-center interface. The platform facilitates interoperability and provides a COP that enables situational awareness for on-scene response and off-scene support personnel during all phases of incident management. The primary operators of the system are DoD civilians, including installation emergency management personnel, decision makers, and first responders. From a procurement standpoint, the system is in sustainment.

The system is Government-owned and supports CAP messaging. The system is compatible with DHS's Public Alert and Warning System, enabling communication and information sharing with local entities. Users include the Reserve Components, National Guard Bureau, USN, USMC, U.S. Coast Guard, U.S. Army, and U.S. Air Force. A Keystone application program interface has been written and demonstrated as a means to

²¹ Ibid.

implement interoperability with other systems, specifically: AtHoc, C4I Suite, NIPR-SAGE, and WebEOC.

G. Integrated Public Alert and Warning System

System Description

The Integrated Public Alert and Warning System (IPAWS) program launched in 2006 in response to Presidential Executive Order 13407, which required that the United States have “an effective, reliable, integrated, flexible and comprehensive system to alert and warn the American people in situations of natural disasters, terrorist attack, or other man-made disasters or threats to public safety.” The Homeland Security Act of 2002 was amended by the Integrated Public Alert and Warning System Modernization Act of 2015, Public Law 114-143, April 11, 2016, by adding Section 526, Integrated Public Alert and Warning System Modernization.

Residing under DHS and managed by FEMA, the purpose of the IPAWS is to create a fully integrated, multi-modal system of systems for warning citizens and to focus on modernizing and enhancing the aging Emergency Alert System (EAS). The program’s primary responsibility is ensuring that the president can speak to the American public during a critical national event, but it also aims to provide the power of a national system to local authorities for use during situations of localized imminent threats and AMBER²² Alerts.

A major obstacle to creating an integrated alert and warning system has been the lack of standards across various warning devices. The new Emergency Data Exchange Language Common Alerting Protocol (EDXL-CAP) Version 1.2 was approved by Organization for the Advancement of Structured Information Standards (OASIS) in August 2010. The clock on an industry implementation timeline started when FEMA formally adopted this protocol. With CAP, any user interface capable of creating CAP-compliant messages can activate any warning device capable of receiving CAP-compliant messages. This includes EAS hardware designed to interrupt broadcast programming for radio, television, and cable for the purpose of issuing an audio (and now text) emergency message. Vendors building these standards into their products open the door to interoperability among a wide spectrum of warning systems.

Another important technological accomplishment within the IPAWS program is the Commercial Mobile Alert System (CMAS), which allows for sending text-based alerts to mobile devices in targeted geographic areas without requiring opt-in subscriptions from

²² AMBER = America’s Missing: Broadcast Emergency Response.

recipients. CMAAS operates by sending alerts through the cellular carrier and transmitting over cell towers only within the targeted area to everyone within range. In most cases, the message is not a traditional text message (a one-to-one method that, with sufficient volume, can cause major bottlenecks within the carrier network). Instead, the messages are cell-broadcast messages (a one-to-many approach). Cell broadcasts “ride” along the carrier’s administrative channel, which is required for the mobile device to remain connected to the cellular network, and are transmitted to everyone active on a given cell tower at once, eliminating bottlenecks.

Another concept associated with IPAWS is the Primary Entry Point (PEP) station, which is a radio station designated to provide public information before, during, and after an emergency, whether national or local. PEP stations will also serve as the daisy chain for station-to-station broadcasts of EAS alerts. These stations are equipped with designated circuits and an emergency generator to ensure broadcasts continue even if power is lost. FEMA helps station owners and operators maintain and restore these facilities.

A final advancement of interest is the Geo-Targeted Alerting System (GTAS), a joint development effort between the U.S. Department of Commerce’s National Oceanic and Atmospheric Administration (NOAA) and the IPAWS program. The map-based GTAS application taps into the administration’s atmospheric condition data to help determine the population impact of a toxic substance release or severe weather event. The GTAS models more than 500 types of hazardous substances and creates notification boundaries based on the results. Once an affected area is defined, alerts and warnings can be issued using CAP through whatever means are available.

H. Mission Assurance, Threat Alert, Disaster Resiliency, and Response

System Description

Mission Assurance, Threat Alert, Disaster Resiliency, and Response (MATADRR) is a USNORTHCOM joint program to establish information-sharing interfaces across unclassified emergency management/force protection applications. The MATADRR program has developed a middleware software capability named Keystone. Keystone is standards-based middleware that receives, translates, and transmits incident-related data between linked disparate systems. It is not clear that the Keystone Application Program Interfaces (API) satisfy the DoD definition of interoperability, which requires information to flow both ways. The Keystone architecture consists of two main web-based services: the DoD Core and the software adapters, more commonly referred to as APIs.

As of September 2015 (the latest documentation available), APIs have been written and validated for AtHoc; Installation Protection Integration Platform (IP2); Command, Control, Communications, Computers and Intelligence Suite (C4IS); NIPR-SAGE; GeoByte (German, Austria, and Luxembourg) system; Physical Security Integration Framework (PSIF); and WebEOC.

The Keystone DoD Core supports three levels of service: infrastructure, domain, and external. The services rely on existing standards such as the National Information Exchange Model (NIEM) and OASIS. Each Core is configured to include the capability to incorporate existing, developing, and future standards. The architecture is scalable, that is, Keystone Core can be linked to another Core, as shown at the Technology Demonstration at Fort Belvoir, Virginia, on June 25, 2013.

Communication via Keystone is not full duplex, i.e., a call for data exchange does not automatically generate an acknowledge message when the data is received. Either the receiving system must acknowledge receipt or another call must be generated. Another solution is for the receiving system to publish all received messages. During a technical interchange, WebEOC was described as publishing a unique identifier to confirm message receipt.

I. Rapid Notify

System Description

Headquartered in Irvine, California, Rapid Notify, Inc., has locations across North America, including New York, Massachusetts, Colorado, and Nevada. Rapid Notify has been in the mass notification industry for almost 30 years. Formerly known as Community Alert Network (CAN), which was acquired by American Emergency Notifications (AEN), the company became Rapid Notify in 2008. The system is a hosted and managed notification system for which no additional hardware is required. The system provides a secure, online dashboard for access to notification tools from any location with Internet connection.

Rapid Notify is a comprehensive suite of emergency notification, mass notification, and incident management services. It is a web-based emergency notification system that enables effective, real-time, two-way communication via telephone, email, and Short Message Service (SMS) text messaging. The services provided are “ideal for government agencies, municipalities, educational institutions, non-profit organizations, first-responders and businesses.”²³ In the event of an emergency, it allows users to alert their

²³ Rapid Notify, <<http://www.rapidnotify.com/about.html>>. Accessed March 2017.

employees and other people in the affected area, as well as communicate with first-responders. It uses geographic information system (GIS) data to exactly pinpoint a desired audience.

System Capabilities:²⁴

- Fully Hosted – There is no hardware to purchase; the services are fully hosted and secured with Firewall Security, SSL Certificate, and 256-Bit Data Encryption.
- Simple Controls – The secure online dashboard allows for access to client tools from any location. Multiple operator levels with different access increase data confidentiality and security. Live customer service support is available 24/7.
- Data Management – The user can create and store unlimited contact lists and messages, with up to three phone numbers per contact in addition to the SMS text number and the email address. A Master/Sub-Account structure allows for multiple locations of a business or department to ensure message consistency and reduce the time to alert.
- Reporting – The dashboard allows delivery and status reports to be downloaded for each alert recipient for complete tracking and auditing.
- Targeted Communications – An unlimited number of distribution lists may be created for targeted communications. Contacts can be kept up to date via manual importing and editing or with the embedded Self-Registration Portal directly in the website.
- Delivery Options – Instant and reusable scenario alerts allow the user to respond to immediate situations. Scheduled delivery enables the user to plan notifications in advance. Repeat alerts on an hourly, daily or monthly schedule. Customize caller ID and email reply-to address.
- Inbound calling – A Dedicated Inbound 800 Number allows users to record messages as often as they need. This helps manage inquiries and reduces the overall call volume and strain on internal resources.
- Internal Communications – An optional Communications Desk allows for real-time email and SMS text conversations with the team.

²⁴ Rapid Notify, “Rapid Notify: Emergency Notification Without Equal,” *Rapid Notify, Inc.* <http://rapidnotify.com/downloads/Rapid_Notify_Business_Continuity.pdf>. Accessed March 2017.

J. Rave Mobile Safety

System Description

Rave Mobile Safety provides several products to ensure better preparedness, faster response, and more effective communication capabilities before, during, and after an emergency.²⁵ Their products are:

- Rave Alert – This provides the ability to send emergency notifications to all channels of communication from a computer, smart phone, or tablet. The pre-set templates allow for an accelerated send and notification process. The infrastructure ensures performance and notification delivery through geo-redundant data centers, multiple carriers, carrier networks, and aggregators.
- Rave Panic Button – Authorized personnel can use the panic button to communicate within seconds an emergency to 9-1-1, staff in the affected area, and first responders. This improves collaboration between the 9-1-1 call taker and those on scene or responding to the scene by allowing for communication between all parties involved in the response. When the button is pressed, the 9-1-1 call taker can immediately see the location of the emergency and any building floor plans or facility information.
- Rave 911 Suite – This is primarily a tool for first responders to use to gain faster and better situational awareness of an emergency. This is done through a command view, two-way SMS communication capabilities, facility data, caller information, etc.
- Smart911 – This provides additional caller data during a 9-1-1 call. It gives the Public Safety Answering Points (PSAPs)²⁶ and first responders access to the caller's Safety Profile. This contains information such as family members, photos, medical conditions, disabilities, and exact address, allowing dispatch to make informed decisions in an emergency.
- Rave Guardian – The campus safety application creates a real-time virtual safety sub-network within a safety network. These sub-networks can be defined by the operators and can include family, friends, and campus safety personnel.

²⁵ Rave Mobile Safety, "Products," <<https://www.ravemobilesafety.com/products/>>. Accessed March 2017.

²⁶ A primary PSAP is defined as a PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office, such as, a selective router or 9-1-1 tandem. A secondary PSAP is defined as a PSAP to which 9-1-1 calls are transferred from a primary PSAP.

- Rave Eyewitness – Eyewitness is a two-way text-based application for the submission of tips by the public. This allows the general public to help law enforcement by providing a confidential and anonymous avenue for members of the community to submit tips.
- Rave Prepare – This product allows emergency managers to understand the needs of the community and effectively prepare to meet those needs in an emergency.

Rave Mobile Safety's platform is built with Public Safety Grade Technology that needs to perform best when conditions are the worst: during storms, power outages, etc. Rave's services are run out of geo-diverse Tier 4 data centers that provide redundant networks and have power and cooling capabilities. They also employ technologies and processes, and are subject to regular audits by third parties.²⁷

K. WebEOC

System Description

WebEOC is owned by ESi Acquisition, Inc., a wholly owned subsidiary of Intermedix Corporation. WebEOC has been deployed across 66 Army, 12 Air Force, and 7 USMC installations, 15 Departments, and 48 Agencies within the Federal Government; 42 states and territories, including more than 70 state-level agencies; and over 200 local government agencies.

WebEOC is a web-enabled information management application that is geared toward the information management requirements of Emergency Management. WebEOC is accessed by the user through a web browser and does not require any client-side application or plug-in. The web server utilized by WebEOC is Microsoft's Internet Information Server, and it is connected to a Microsoft SQL Server database on the backend. Although WebEOC and its product suite provide specialized tools for managing crisis information and emergency response, it can also be used to manage other events.

WebEOC includes a default set of boards and plugins that enable an agency to begin using it almost immediately. An agency can use any or all of the boards as is, or build an unlimited number of boards and forms tailored to local requirements. Within the context of WebEOC, a board is an electronic display that allows transmission and sharing of information in real time with other WebEOC users. WebEOC boards are the equivalent of the large, chronological, or topical paper-based boards that, for years, were extensively

²⁷ Rave Mobile Safety, "Public Safety Grade Technology," <https://www.ravemobilesafety.com/technology-3/>. Accessed March 2017.

used by Emergency Operations Centers (EOC) and command centers around the world. Initially introduced in 1997, WebEOC was the first web-based, COTS Critical Incident Management System (CIMS) system used for emergency management. See Figures 13–16.

WebEOC as a “board” manager is essentially an electronic version of the legacy grease pencil status board used to manage emergency responses in real time. The WebEOC board is provided as a URL that can be reached from any browser. The primary advantages of WebEOC status boards over the legacy grease pencil status boards are visibility of information by people not physically present in the EOC, data is stored in the database (instead of erasing and updating a grease pencil status board) and is timestamped, and the user name of the individual entering the information is captured. This affords the opportunity to analyze the information available throughout an event for after-action analysis, investigations, and litigation. It has primarily civilian users, as compared to the AtHoc footprint within DoD.

Of the 50 State Emergency Management Agencies, 44 of the 50 use WebEOC to manage their centers. The WebEOC is also used (partial list) by FEMA, the Transportation Security Administration, Customs and Border Protection, Immigration and Customs Enforcement, and the Department of Energy.

WebEOC Enterprise has all the features and capabilities of WebEOC Professional, but it is geared toward large agencies or organizations that also have sub-agencies or organizations with full emergency management responsibilities. The main differences in this case between WebEOC Professional and WebEOC Enterprise are their administrative features. WebEOC Enterprise provides the ability to delegate administrative functions to these sub-agencies or organizations instead of maintaining centralized administration at the primary agency or organization. WebEOC Enterprise is also bundled with some other WebEOC Plug-ins and add-ons, such as a Dashboard module and Data Manager, which streamlines the process of importing and exporting data, and other add-on modules. WebEOC Fusion is, for the most part, a message switch that is specifically designed for WebEOC. It facilitates the exchange of information between separate WebEOC systems with store-and-forward capabilities when network connectivity between the WebEOC Fusion server and the WebEOC server is down.

An example of the utilization of a WebEOC Fusion server is in the National Capital Region (NCR). The Virginia and Maryland counties that surround Washington, D.C., along with the D.C. Emergency Management Agency, all have their own WebEOC Professional systems. So that they can all share and exchange information during an event that is affecting the region, they are tied together through a WebEOC Fusion server. This allows each agency to operate within its own WebEOC system, following its own processes and business practices, yet share information it deems relevant to the other agencies and see information the other agencies feel is relevant to all. It also allows

agencies to share unique status boards through a publish/subscribe method that precludes the need to develop each status board separately on each system.

WebEOC is developing rapidly within the space, and adding a vulnerability assessment capability (cameras, metal detectors, exits, glass, and tenants).

Training - 2012										
PWC Corrective Action Tracking										
New Entry		Filter By: Show All Completed In Progress Not Started No Action Required								
Title	Date AAR Finalized	Primary Agency	Primary POC	Supporting Agency	Capability Element	Anticipated Corrective Action Completion Date	Corrective Action	Progress	Status	View Details
Title 2	03/07/2012	Andrea Miller	John	PWC Temp User	Training	03/08/2012	Nothing now		In Progress	Edit View
Title 1		Joan E. Koss		Andrea Miller					Completed	Edit View

Figure 13. WebEOC Example Board²⁸

²⁸ ManTech International Corporation, "Supported Specialty WebEOC Boards: Corrective Tracking Board," Version 1.0x, 3 June 2016, p. 9.2, <<http://www.ncrwebeoc.com/wp-content/uploads/Supported%20Speciality%20WebEOC%20Boards/Catalog-Corrective-Tracking-Board.pdf>>. Accessed March 2017.

Program/Project Management (Version 2.1) *Incident Dependent*

Description: This board captures information for individuals or offices to track their projects/programs and track status activity.

Views: There is one main list view for this board.

List View – This view lists the Programs and Projects and associated high-level information.

Daily Log Print to PDF



Program and Project Management

New Record Search Sort By: All

Record #	Importance	Project / Program	Type	Lead	Timeframe:	Date Due:	Status	Action
26	High	CEMP-IT update	Project		2013 - Q1	01/23/2013 12:28:07	In Progress	Details Edit
25	Low	Table top exercise	Project		2013 - Q1	02/28/2013 12:27:13	Future Project	Details Edit
24	Low	AEM Certification for Regina	Project		2013 - Q2	04/30/2013 12:25:21	Future Project	Details Edit
5	Low	POD Plan Update	Project		2013 - Q1	01/11/2013 16:32:31	Waiting	Details Edit
22	Low	Webeoc AAR	Program		2013 - Q1	01/31/2013 13:18:18	Future Project	Details Edit
21	Moderate	CERT Monthly Drill	-Select One-		2013 - Q1	01/16/2013 13:13:54	Complete	Details Edit
19	Low	OEM Wants list in WebEOC	Project		2013 - Q1	01/31/2013 13:12:22	In Progress	Details Edit
18	Moderate	Flu Flyer	Project		2013 - Q1	01/16/2013 11:23:55	In Progress	Details Edit
13	Low	Plan Inventory / Status Report	Project		2013 - Q1	01/11/2013 12:18:03	Complete	Details Edit
9	Moderate	CERT Graduation article	Project		2013 - Q1	01/09/2013 16:59:29	Complete	Details Edit
11	Moderate	KinderCare Plan Review	Project		2013 - Q1	01/09/2013 17:00:00	Complete	Details Edit
8	Moderate	Cert article for Sandy	Project		2013 - Q1	01/09/2013 16:58:17	Complete	Details Edit
1	Low	Grant Inventory List	Project		2013 - Q1	01/14/2013 15:29:03	Complete	Details Edit

Figure 14. WebEOC Program/Project Management Board²⁹

²⁹ ManTech International Corporation, “Supported Specialty WebEOC Boards: Corrective Tracking Board,” Version 1.0x, 3 June 2016, p. 29.1, <<http://www.ncrwebeoc.com/wp-content/uploads/Supported%20Speciality%20WebEOC%20Boards/Catalog-Corrective-Tracking-Board.pdf>>. Accessed March 2017.

List View – COOP Department Control Panel – Each identified Department will have a Department Control Panel with buttons on the left to access the identified data. Descriptions are on the right. Each button opens a display view and each display view has an associated input view as appropriate.

The current leader and facility address for Continuity of Operations in support of the following objectives within 12 hours of activation:

1. Ensure continuous performance of essential functions
2. Reduce loss of life/minimize damage
3. Ensure succession to office of key leadership
4. Reduce/mitigate disruptions to operations
5. Protect essential assets
6. Achieve timely recovery/reconstitution
7. Maintains Tests, Training and Exercises program for validation

Orders of succession are provisions for the assumption of senior departmental leadership positions during an emergency when the incumbents are unable or unavailable to execute their legal duties. Delegations of Authority specify who is authorized to make decisions or act on behalf of the department head and other key officials for specific purposes during COOP emergencies to include, making personnel management decisions, approving commitment of resources and signing contracts.

Mission Essential Functions are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public and sustain the industrial and economic base.

Locations, other than the normal facility, used to carry out essential functions in a COOP situation.

The COOP Program Managers serve as the department COOP coordinator and is responsible for all activities that enable the department to perform essential functions in any situation that would otherwise disrupt normal operations.

Human capital management is having the right people (Emergency Response Group) in the right jobs to perform essential functions, ensures that all employees have a clear understanding of what to do in an emergency, and includes protocols for identifying/assisting special-needs employees. It considers alternate assignments for nonemergency employees.

A vendor is an entity that provides information, data, services, etc. to your department/unit. A customer is an entity to whom your department/unit provides information, data, services, etc. Vendors and customers may be internal to the County government (i.e., another County department or agency) or external to the County government (i.e., another jurisdiction, the State, private sector company, the public, etc.)

Vital records are electronic and hardcopy documents, references, and records needed to support essential functions during a COOP situation. The two basic categories of vital records are emergency operating records, and legal and financial records.

Communications, IT, and other support equipment that provides the capability to perform essential functions, in conjunction with other organizations, until normal operations can be resumed.

Special reports to include COOP Program Manager contact list, Alternate Facility locations, orders of succession list, and a COOP Departmental Quick Reference Guide

Figure 15. WebEOC COOP Control Panel³⁰

Record ID	For Date	Status of Government	Name	Last Update	Action
52	03/25/2016	Open with Unscheduled Leave		04/05/2016 12:57:52	Edit Edit Notifications Details
1	03/25/2016	Closed		03/25/2016 15:34:03	Edit Edit Notifications Details
13	03/25/2016	Open with Unscheduled Leave		03/25/2016 15:07:53	Edit Edit Notifications Details

Figure 16. WebEOC Severe Weather Notification Board³¹

³⁰ ManTech International Corporation, “Supported Specialty WebEOC Boards, COOP Board,” Version 1.0, 3 March 2017, p. 6.1, <<http://www.ncrwebeoc.com/wp-content/uploads/Supported%20Speciality%20WebEOC%20Boards/Catalog-COOP-Board.pdf>>. Accessed March 2017.

³¹ ManTech International Corporation, “Supported Specialty WebEOC Boards, COOP Board,” Version 1.0, 3 March 2017, p. 76.1, <<http://www.ncrwebeoc.com/wp-content/uploads/Supported%20Speciality%20WebEOC%20Boards/Catalog-COOP-Board.pdf>>. Accessed March 2017.

3. Interoperability

Interoperability was measured according to three criteria; Like-to-like interoperability, Direct interoperability, and Interoperability through a bridge.

- **Like-to-like interoperability** is the ability of one instance of a system being interoperable with other instances of the same system. For example, if a county buys an AtHoc license to do their mass, warning and notification, would this version of AtHoc be able to communicate with the next county's different license of AtHoc?
- **Direct interoperability** is the capability for two different mass, warning, and notification systems to interact with each other without a middleware solution. This is accomplished with an API developed by one or both of the systems. The APIs are generally built upon request and not in anticipation, because funding needs to be established before development. Therefore, lack of an established connection, does not preclude one existing in the future.
- **Interoperability through a bridge** allows for the use of middleware enabling two disparate systems to communicate during a developing incident or emergency situation. This paper examined WebEOC (incident management platform) and Keystone. These middleware systems already have the capability to "talk" with several emergency notification systems.

Below is a summary of each system's ability to be interoperable. Where a system does not currently have that capability, future capabilities for interoperation via various means are discussed.

1. Alert! Interoperability

The Alert! system software includes a service-oriented architecture (SOA), meets OASIS standard specifications for data, and is CAP-compliant. The interoperability of the Alert! system is as follows: (1) interoperability with other Alert! systems, was established during technical interchange; (2) interoperability through a bridge has not yet been demonstrated—however, an API for Keystone is a possibility; (3) direct interoperability with WebEOC is under consideration in 2017.

2. AtHoc Interoperability

AtHoc Interactive Warning System (IWS) Alerts is an IP-based COTS software system. Many legacy systems (e.g., Giant Voice, local radio stations, and facility fire and life safety systems) are not IP-based or certified for customer network access, and the AtHoc IIM is used to operate these systems. The IIM is a PC-based appliance that connects to the local network and supports the CAP or XML protocols to communicate with the AtHoc IWS Alerts server. The IIM connects to the legacy systems over the various interfaces types, including serial interfaces (RS-232, RS-485), audio-out, and dual-tone multi-frequency. The IIM usually connects to the external system's central control unit via one of the interfaces described above. Multiple IIM units may be used at a single site. The IIM can also interface with the local, state, or national EAS and translates the IP-based CAP message into the appropriate format of the EAS Encoder/Decoder (ENDEC). Typically, the IIM polls AtHoc IWS Alerts using the CAP protocol. Once an alert has been initiated, AtHoc IWS Alerts posts a CAP message, which is then retrieved by the IIM. The IIM parses the message and activates the relevant system accordingly. Requests to cancel messages may also be sent. See Figure 17 for details.

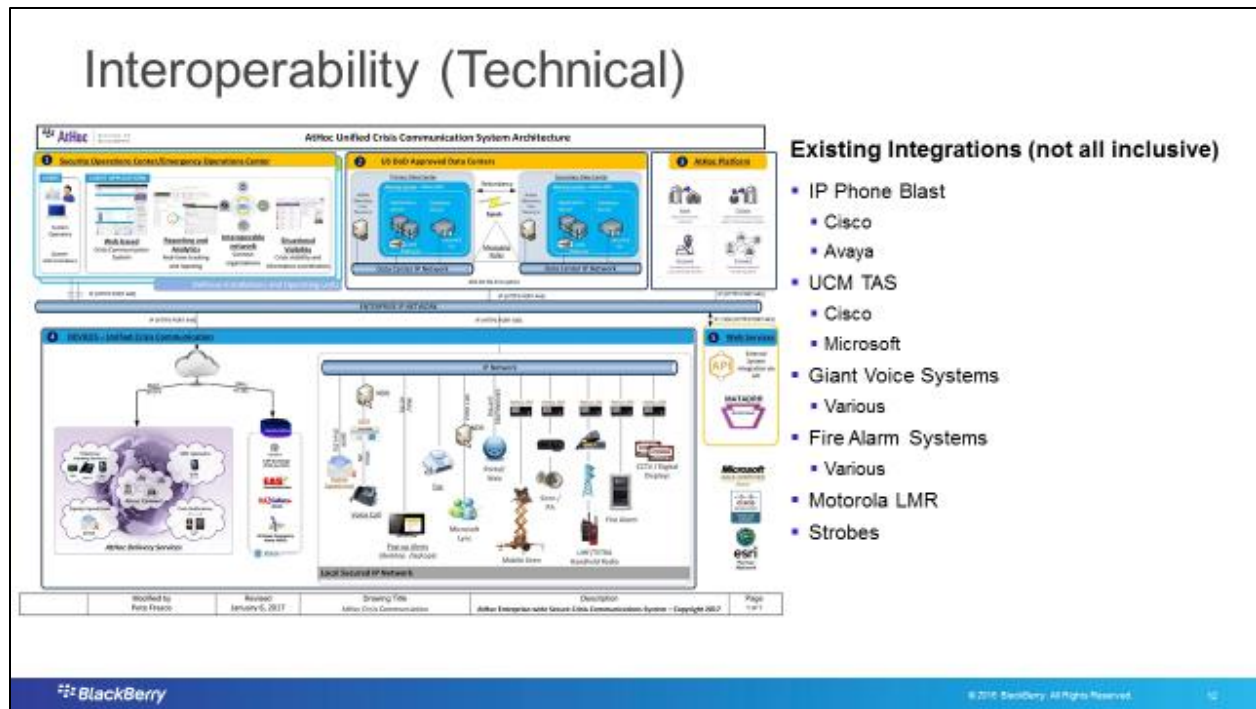


Figure 17. AtHoc Technical Interoperability³²

One of the most significant interoperability accomplishments was the integration of AtHoc IWS Alerts with the Land Mobile Radio (LMR), as described in Figure 18. Voice messages can be generated by the IIM from a text message using text-to-speech conversion or from a pre-recorded message that resides in the AtHoc IWS Alerts system. The physical interface to the LMR base-station radio is via a push-to-talk adaptor and an audio-in cable.

³² Mike Brown, Pete Frasco, and Matt Moore, “AtHoc Crisis Communications Discussion and Demonstration for IDA,” Blackberry demonstration given at the Institute for Defense Analyses on 10 January 2017.

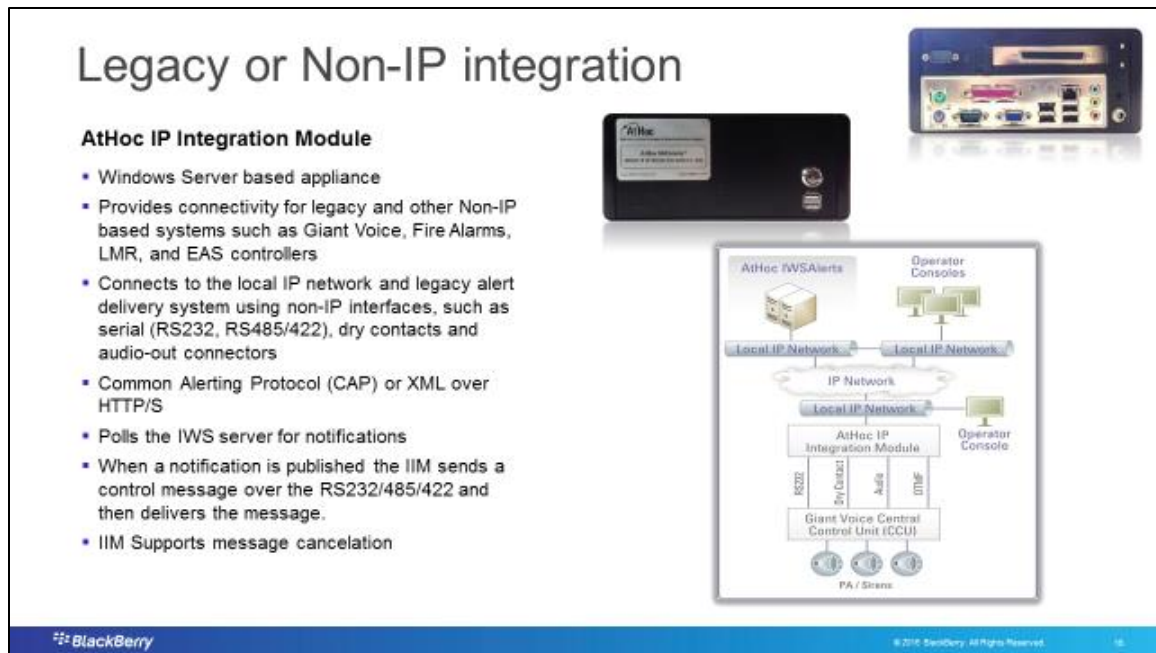


Figure 18. AtHoc Interoperability – Legacy or Non-IP Integration³³

Interoperability between AtHoc systems (1) is not a problem based on a technical interchange. Interoperability using a bridge (2), i.e., the Keystone, an application program interface (see description below), has been written and demonstrated as a means to implement At Hoc interoperability with other systems, specifically C4I Suite, IP2, Non-Secure Internet Protocol Router-Situational Awareness Geospatial Enterprise (NIPR-SAGE), and WebEOC. Within the U.S. European Command (EUCOM), interoperability was demonstrated (again using Keystone) with the German system GeoByte and WebEOC, PSIF, and NIPR-SAGE. At the present time, direct interoperability (3) of AtHoc with other systems has not been determined.

3. C4I Suite Interoperability

Because C4I Suite was developed as a USN-USMC program, it should be interoperable between these two Services. Interoperability with the U.S. Army and U.S. Air Force is unknown at this time. Interoperability between C4I Suites (1) should certainly be possible (although undocumented at this time) due to its SharePoint basis. Interoperability using a bridge (2) has been demonstrated using Keystone. An application program interface has been written and demonstrated as a means to implement interoperability with other systems, specifically with AtHoc, iP2, NIPR-SAGE, and

³³ Ibid.

WebEOC. Direct interoperability (3) between disparate systems has not yet been determined.

4. Desktop Alert Interoperability

Desktop Alert is an IP-Based alert technology that provides integration with enterprise-class federated environments and shares communications and commands using standardized protocols such as XML and HTML. Desktop Alert is the largest United States IP-Based Mass Notification deployment in the United States. Desktop Alert now serves U.S. Army locations in 54 U.S. states, territories, and locations and in Afghanistan. Desktop Alert is the leading provider of net-centric mass notification systems to the U.S. Army worldwide. Desktop Alert did not respond to a request for information by the IDA team, so determination of interoperability has not been made at this time.

5. Everbridge Interoperability

Everbridge has an existing set of APIs that can be used for integrating with or connecting to third-party data sources. Given that APIs already are incorporated into Everbridge, the potential interoperability with like and other systems (interoperability 1, 2, and 3) should not be a problem.

6. IP 2 Interoperability Potential/Constraints

The IP2 system did not respond to a request for information by the IDA team, so determination of interoperability (1) and (3) has not been made at this time. Interoperability through a bridge (2) has been demonstrated.

7. IPAWS Interoperability

Standardized alerts can be received from many sources, and users can configure their applications to process and respond to the alerts as desired. Alerts from DHS, the Department of the Interior's United States Geological Survey, NOAA, and state and local government agencies can all be received in the same format, by the same application. That application can, for example, sound different alarms based on the information received.

The IPAWS program provides an Internet-based capability for Federal, state, territorial, tribal, and local authorities to use to issue critical public alerts and warnings from a single portal to multiple communication pathways such as EAS and CMAS.

Although IPAWS must be accessed through specific software, such as Rapid Notify, that meets IPAWS system requirements, there is no additional cost to send

messages through IPAWS. As a bearer network, the three categories of interoperability adopted by this paper do not directly apply.

8. MATADRR Interoperability

Since this is middleware, it is designed to be interoperable with other systems as long as an appropriate two-way API can be written.

In addition to the technology demonstration (referenced above), an Independent Verification Test was conducted at SPAWAR Systems Center Pacific, San Diego, California, on March 14, 2014, which included two Cores and five of the APIs listed above. A Final Transition Demonstration was conducted March 17–20, 2014, at the same site. Keystone software was again successfully demonstrated during the March 2015 U.S. Army Garrison Quarterly Exercise (Stuttgart, Germany) and the September 15 EUCOM Operational Demonstration as part of the Stallion Shake Exercise (Stuttgart, Germany). Keystone conforms to the NIEM version 2 and the XML protocols.

Based on the documentation available and because MATADRR is middleware, two-way interoperability has not been verified. There are no apparent technical reasons why the Keystone Core should not be adopted by civilian agencies/companies/departments. Interoperability (1) does not apply. Interoperability through a bridge (2) obviously is satisfied. Interoperability (3) does not apply.

9. Rapid Notify Interoperability

Rapid Notify is becoming an IPAWS-Open Developer. This means Rapid Notify will implement a Memorandum of Agreement with FEMA for the purpose of gaining access to the IPAWS–Open Platform for Emergency Networks (OPEN) Test Environment to support interoperable software development.³⁴ Interoperability categories (1) and (3) have yet to be determined. Conceptually, if one considers IPAWS a bridge, then Rapid Notify satisfies interoperability category (2).

10. Rave Mobile Safety Interoperability

Rave Mobile Safety and WebEOC recently announced a partnership, creating a Rave Alert Extension, which integrates Rave Alert and WebEOC.³⁵ This solution is bringing together crisis management and mass warning to improve the agencies' ability

³⁴ Federal Emergency Management Agency, “Integrated Public Alert Warning Systems (IPAWS) OPEN Developers,” <<https://www.fema.gov/media-library/assets/documents/25916>>. Accessed March 2017.

³⁵ Rave Mobile Safety, “Rave Alert Extension for WebEOC,” Rave Alert Product Brief, <https://www.ravemobilesafety.com/downloads/2017/alert_webeoc_2017_web.pdf>. Accessed March 2017.

to mitigate, prevent, prepare for, respond to, and recover from an emergency event. Together they will provide end-to-end incident response management and communication. Interoperability (1) and (3) are accomplished through WebEOC, which in this case can act as a bridge or through the use of Keystone. Interoperability (2) is accomplished.

11. WebEOC Interoperability

As described above in Section J, Rave Mobile Safety and WebEOC have recently announced a partnership, creating a Rave Alert Extension that integrates crisis management and alerting/mass warning. Assuming that the integration goes as planned, WebEOC will have demonstrated its ability to interoperate with at least one disparate system, interoperability (3). Interoperability with additional systems seems a reasonable possibility as need arises. For example, the MATADRR program office offered the ability to interface between WebEOC and other systems via Keystone, in particular with AtHoc, as shown in Figure 19. Interoperability (1) and (2) do not apply.

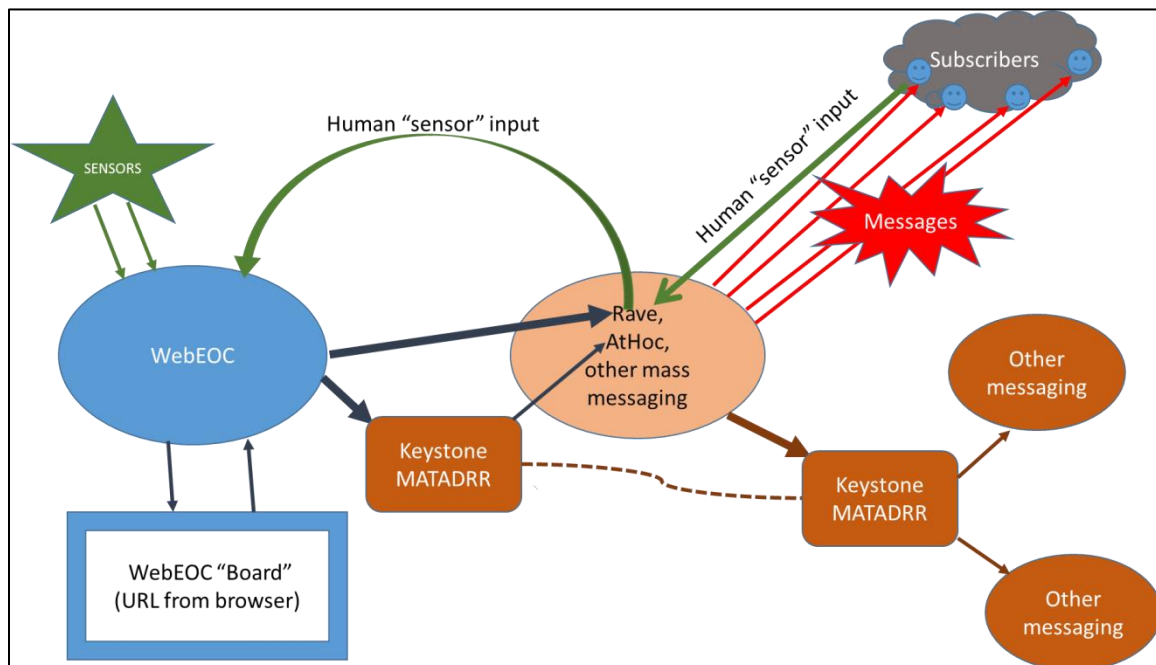


Figure 19. WebEOC Functions

4. Observations and Conclusions

The survey revealed the heterogeneous state of current systems. They are a mix of GOTS, multi-Service DoD systems, and commercial systems—Alert! and IP2 (GOTS), C4I Suite (USN and USMC), Keystone (U.S. Army), IPAWS (DHS), AtHoc and Everbridge (commercial). We point this out, not as a criticism but simply to illuminate the challenges of achieving a unified DoD system moving forward. The intent is be unified through interoperability, not by replacing existing solutions with a single solution.

Fortunately, interoperability may not be as big a technical problem as was anticipated. The survey identified an example of incident management/mass warning systems that interoperate (Rave, Alert! and WebEOC) without having experienced significant technical problems. The survey also identified an example of a dedicated interoperability bridge (Keystone), which has successfully demonstrated interoperability across multiple disparate systems. From a purely technical perspective, then, the interoperability “problem” is eminently tractable given the existence of a requirement.

Table 1. Interoperability Summary

System	(1) Like-to-Like Interoperability	(2) Interoperability through a Bridge	(3) Direct Interoperability
Alert!	Yes	TBD	Planned with WebEOC
AtHoc	Yes	Yes	TBD
C4I Suite	TBD	Yes	TBD
Desktop Alert	TBD	TBD	TBD
Everbridge	Yes	Yes	Yes
IP2	TBD	Yes	TBD
IPAWS	N/A	N/A	N/A
Keystone	N/A	Yes	N/A
Rapid Notify	TBD	Yes	TBD
Rave Mobile Safety	Yes, through WebEOC	Yes	Yes, through WebEOC
WebEOC	N/A	Yes	Yes

Interoperability may not be technically difficult to because the pieces are set. Jurisdictions, bases, and facilities do not dynamically relocate or change mission (within short time periods), as is the case with military systems. If the requirement to interoperate

is identified and the resources to do so are available, there will be ample time to implement the necessary interoperability. Having the time and the requirements to define the problem is key.

The systems in this paper have, with five exceptions (C4I Suite, IPAWS, IP2, Alert!, and Keystone), been developed by for-profit corporations. And, there are other commercial systems outside the scope of this paper. This situation has pluses and minuses. On the plus side, the profit motive is very powerful. On the minus side, proprietary capabilities are necessarily shared very carefully; thus, defining the interoperability interfaces cannot be expected to be anything other than a deliberate process. Table 1 summarizes the systems' interoperability.

The recent spate of terrorist attacks, shootings, and bombings provides ample incentives for DoD and civilian public safety organizations to implement the interoperability needed to save lives and property. The DoD CIO has an opportunity to lead a mission-driven force protection effort to provide an integrated capability with the national public safety community.

Acronyms and Abbreviations

AEN	American Emergency Notifications
AFMC	Air Force Materiel Command
API	Application Program Interface
ARDEC	Armament Research Development and Engineering Center
AT/FP	Anti-Terrorism/Force Protection
C4&IIC	Command, Control, Communications and Computers and Information Infrastructure Capabilities
C4I	Command, Control, Communications, Computers and Intelligence
C4IS	Command, Control, Communications, Computers and Intelligence Suite
CAD	Computer Aided Dispatch
CAN	Community Alert Network
CAP	Common Alerting Protocol
CIMS	Critical Incident Management System
CIO	Chief Information Officer
CMAS	Commercial Mobile Alert System
CONOPS	Concept of Operations
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf
CPR	Cardiopulmonary Resuscitation
DCIO	Deputy Chief Information Officer
DECC	Defense Enterprise Computing Center
DHS	Department of Homeland Security
DoD	Department of Defense
EAS	Emergency Alert System
EDXL-CAP	Emergency Data Exchange Language-Common Alerting Protocol

ENDEC	Encoder/Decoder
EOC	Emergency Operations Center
EUCOM	U.S. European Command
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act of 2002
GIS	Geographic Information System
GOTS	Government Off-The-Shelf
GTAS	Geo-Targeted Alerting System
GTAS	Geo-Targeted Alerting System
IDA	Institute for Defense Analyses
ILSC	Integrated Logistics Support Center
IP	Internet Protocol
IP2	Installation Protection Integration Platform
IPAWS	Integrated Public Alert and Warning System
IP IIM	IP Integration Module
IWS	Interactive Warning System
LCMC	Life Cycle Management Command
LDAP	Lightweight Directory Access Protocol
LMR	Land Mobile Radio
NAVFAC	Naval Facilities Engineering Command
NIEM	National Information Exchange Model
NIPR-SAGE	Non-Secure Internet Protocol Router-Situational Awareness Geospatial Enterprise
NOAA	National Oceanic and Atmospheric Administration
OASIS	Organization for the Advancement of Structured Information Standards
OPEN	Open Platform for Emergency Networks
PA	Public Address
PEP	Primary Entry Point

PM-ISE	Office of the Program Manager, Information Sharing Environment
PSAPs	Public Safety Answering Points
PS/EM	Public Safety and Emergency Management
PSIF	Physical Security Integration Framework
R&D	Research & Development
ROC	Regional Operations Centers
SaaS	Software-as-a-Service
SAFETY ACT	Support Anti-Terrorism by Fostering Effective Technology Act of 2002
SDK	Solution Developer Kit
SMS	Short Message Service
SOA	Service-Oriented Architecture
SPAWAR	Space and Naval Warfare Systems Command
SSC PAC	SPAWAR Systems Center Pacific
TACOM	Tank-automotive and Armaments Command
UCCS	Unified Critical Communications Suite
URL	Uniform Resource Locator
U.S.	United States
USMC	U.S. Marine Corps
USNORTHCOM	U.S. Northern Command
WebEOC	Web-based Emergency Operations Center
XML	eXtensible Markup Language
XMPP	Extensible Message and Presence Protocol

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YY) 21-03-17		2. REPORT TYPE Final		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE A Survey of Mass Warning and Notification Systems				5a. CONTRACT NUMBER HQ0034-14-D-0001	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Serena Chan, John W. Bailey, Ronald A. Enlow, Elisabeth A. Ferland				5d. PROJECT NUMBER ET-5-4155	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882				8. PERFORMING ORGANIZATION REPORT NUMBER D-8388 H 2017-000170	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Joseph M. Wassel Director, C4 Resilience & Mission Assurance DoD CIO 6000 Defense Pentagon, Arlington, VA 20301				10. SPONSOR'S / MONITOR'S ACRONYM DOD CIO	
				11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES Project Leader: Serena Chan					
14. ABSTRACT This document reports on work done by the Institute for Defense Analyses (IDA) for the Office of the Program Manager, Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, and for the Office of the Deputy Chief Information Officer (DCIO) for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (C4&IIC), Department of Defense (DoD) Chief Information Officer (CIO). The objective of this project is to assess the current state of communications interoperability between DoD Public Safety and Emergency Management (PS/EM) entities and United States (US) civilian PS/EM entities and how that is likely to change as the next generation of public safety information systems is implemented across the nation. Specifically, IDA was asked to “execute a survey of the major DoD systems that participate in the national public safety communications backbone to identify approaches that could be leveraged to achieve a high degree of harmonization and integration.” This survey paper discusses only the major mass warning and notification systems employed by the civilian sector and DoD to alert individuals. It contains relevant system descriptions, discussions regarding interoperability potential, observations, and conclusions. Subsequent white papers will survey other types of systems (e.g., Computer Aided Dispatch).					
15. SUBJECT TERMS Public Safety and Emergency Management Communications; Mass Warning and Notification Systems					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER OF PAGES 48	19a. NAME OF RESPONSIBLE PERSON Joseph M. Wassel
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include Area Code) 703-901-7360

