AtHoc | Division of BlackBerry

Network-Centric Emergency Mass Notification

Datasheet

Protecting over 75% of U.S. Military and Homeland Security Personnel at 1,500 Locations Worldwide

> "The AtHoc-based system can automate personnel recall and continuity of operations and can manage personnel accountability in emergencies."
>
> *– Ted Kim, USCG Lt. Commander*

Challenge

During emergencies, the ability to quickly and accurately notify all employees of threats, provide instructions and assess the status of personnel in real time is critical. To instantly reach a mass audience as well as targeted individuals and groups, many government, commercial and military organizations rely on one of their most pervasive and reliable assets – the IP network.

Solution overview

AtHoc transforms the IP network into an enterprise-class mass notification system. By deploying AtHoc, large private and public enterprises can rapidly alert thousands of employees in geographically dispersed buildings and facilities during an emergency.

AtHoc provides:

- **Personnel protection:** Mass dissemination of alerts across multiple channels, accelerating threat response
- **Personnel recall:** Rapid communication to off-facility personnel to report back to duty
- **Personnel accountability:** Real-time response tracking reports on the status and safety of personnel
- **Critical communications:** Distribution of important corporate information to employees
- **Regulatory compliance:** Alignment with government and commercial emergency management, disaster recovery and continuity planning requirements, including fire and building safety (e.g., NFPA 72 2010 and DoD UFC 04-021-01)

AtHoc is enterprise-class

AtHoc has been designed as a secure, enterprise-class network-centric mass notification and emergency communication system. Its interoperability, scalability and security measures have led to its selection by highly demanding defense and commercial organizations including the US Air Force, US Army, US Navy, US Coast Guard, US Department of Veterans Affairs, UCLA, Microsoft, Boeing and Raytheon.

AtHoc can:

- **Transform your existing IP network** into an enterprise-class mass notification system for cost-effective pervasive reach and rapid communication
- **Unify all communication channels and devices** via the AtHoc server, into a single system to simplify activation, ensure message consistency and reduce alerting time
- **Manage the notification process across the enterprise** with predefined scenarios, operator access policies, multilocation support, alert activation flow, tracking and reporting
- **Monitor video feeds, physical security/life safety sensors** and external data sources to automatically trigger notification scenarios
- **Ensure accuracy of personnel contact information** by integrating with enterprise directories and supporting end-user self-service updates
- **Improve building safety** by integrating with existing fire alarm and public address (PA) systems
- **Scale to support hundreds of thousands** of personnel worldwide

Features and benefits

AtHoc can manage the emergency notification process across your entire enterprise. Using a web-based console, operators from any location in the organization can activate alerts to virtually any device, track responses and view accountability reports. Automatic notifications can be triggered by physical sensors and data feeds. Notification processes can be defined to support both enterprise- wide and individual department needs.

Unify notifications to all devices

Through a single unified interface, AtHoc allows you to quickly communicate a consistent message across multiple channels and delivery devices (customizable messaging per device) – all integrated using the IP network. The information is sent via multiple and redundant means, including:

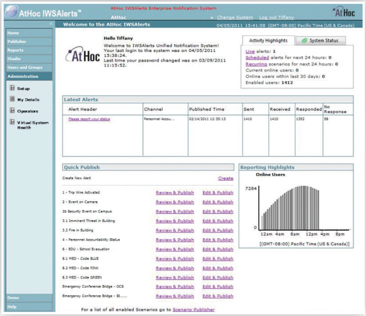
- **Networked computers** – Delivery of audio-visual pop-up notifications to computer desktops connected to the IP network
- **Networked IP phone displays** – 2-way audio-visual (text, video, images) blast alerts to IP phone displays and speakers
- **Telephony** – Delivery of voice telephony alerts to any land, VoIP, mobile phone via on-site or hosted mass dialing services
- **Text messaging** – Delivery of text messages (SMS) to mobile devices and pagers
- **Mobile devices** – Rapid and scalable delivery of notifications to mobile applications, response collection and location tracking
- **Email** – Secure digitally PKI signed email delivery with responses using the organization's email address
- **Social networks** – Distribution of alerts through social networks, including Twitter and Facebook
- **Indoor and outdoor speakers** – Audio notifications to outdoor sirens and indoor public address (PA) systems
- **Cable TV and display boards** – Text, image or video alerts sent to digital displays
- **Radio broadcasts** – Audio broadcasts to local radio stations
- **Land mobile radios (LMRs)** – Alerts to security forces' handheld LMRs
- **Building safety/fire protection** – Integration with existing fire alarm systems
- **XML feeds** – Output standard XML feeds (RSS, Atom and others) integrating with other systems and websites

Provide versatile publishing capabilities

- **Secure PKI digitally signed email delivery with responses** – AtHoc integration with the SMTP delivery infrastructure enables emails to be sent directly using the organization's email address (e.g., .com, .mil, .gov) supporting customer PKI digitally signed emails. Rich content like HTML, videos and links can also be embedded within email alerts.
- **Test alert** – Operators can test an alert on selected personal notification devices before sending out to a larger-scale user base.

Track and report responses for personnel accountability

During an emergency, alert recipients receive multiple response options for acknowledgement and reporting their status on networked channels. Alerts are tracked in real time, giving operators a detailed delivery report for each alert recipient, providing critical personnel accountability status across the enterprise.



Welcome to the AtHoc IWSAlerts 04/05/2011 15:41:58 (GMT-08:00) Pacific Time (US & Canada)

Hello Tiffany
Welcome to IWSAlerts Unified Notification System!
Your last login to the system was on 04/05/2011 15:38:24.
Last time your password changed was on 03/09/2011 11:15:52.

Live alerts: 1
Scheduled alerts for next 24 hours: 0
Recurring scenarios for next 24 hours: 0
Current online users: 0
Online users within last 30 days: 0
Enabled users: 1412

Latest Alerts

Alert Header	Channel	Published Time	Sent	Received	Responded	No Response
Please report your status	Personnel Accou...	02/14/2011 12:35:13	1410	1410	1352	58

Quick Publish

Create New Alert

1 - Trip Wire Activated
2 - Event on Camera
2b Security Event on Campus
3.1 Imminent Threat in Building
3.2 Fire in Building
4 - Personnel Accountability Status
6 - EDU - School Evacuation
8.1 MED - Code BLUE
8.2 MED - Code PINK
8.3 MED - Code GREEN
Emergency Conference Bridge - OCS
Emergency Conference Bridge - St......

For a list of all enabled Scenarios go to Scenario Publisher

Reporting Highlights

Online Users

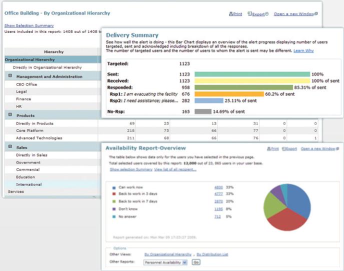
[(GMT-08:00) Pacific Time (US & Canada)]

Web-based console for managing the entire notification process

Child Abduction
Hurricane Approaching
Bomb Threat in the Administration Building
NEW MESSAGES
Attention!
An Emergency Alert has been issued.
Please evacuate all buildings immediately!

Through a single web-based console, launch and manage all communication channels simultaneously. Devices include computers, phones (mobile, landline, VoIP), PDAs, pagers, BlackBerry smartphones, computer kiosks, sirens, TV, radio and PA systems

AtHoc unifies all alerting channels, including triggering alerts to giant voice/PA systems and digital displays



Office Building - By Organizational Hierarchy

Show Selection Summary
Users included in this report: 1408 out of 1408

Directly in Products	69	25	13	31	0	0
Core Platform	218	75	66	77	0	0
Advanced Technologies	211	68	66	76	0	1

Delivery Summary

See how well the alert is doing - this Bar Chart displays an overview of the alert progress displaying number of users targeted, sent and acknowledged including breakdown of all the responses.
The number of targeted users and the number of users to whom the alert is sent may be different. Learn Why

Targeted:	1123	
Sent:	1123	100%
Received:	1123	100% of sent
Responded:	958	85.31% of sent
Rsp1: *I am evacuating the facility*	676	60.2% of sent
Rsp2: *I need assistance; please...*	282	25.11% of sent
No-Rsp:	165	14.69% of sent

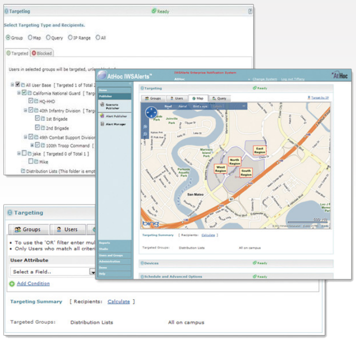
Availability Report-Overview

The table below shows data only for the users you have selected in the previous page.
Total selected users covered by this report: 12,000 out of 23, 865 users in your user base.
Show selection Summary View list of all recipient...

Can work now	4800	33%
Back to work in 3 days	4777	33%
Back to work in 7 days	2870	20%
Don't know	1195	8%
No answer	712	5%

Report generated on: Mon Mar 09 17:03:27 2009.

Real-time response tracking provides accountability and visibility into the safety and status of personnel



Quickly target personnel by organizational hierarchy, geographical maps, named individuals, distribution lists or dynamic queries

Target personnel by organization, geography or individual names

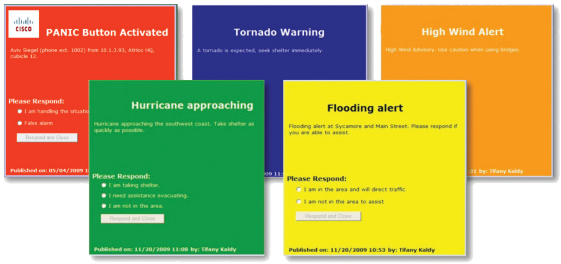
AtHoc can target people based on organizational structure, distribution lists, physical location, individual name or dynamic database query. Personal and mass notification devices (such as sirens and display boards) can be targeted using visual geographic maps, allowing operators to select the buildings, regions or zones to be notified. Dynamic targeting can be accomplished by using a combination of attributes such as individual, role, location or IP address. During the publishing flow, an operator can issue a follow-up alert to users based on the notification response (e.g., targeting those who did not respond to the initial alert) or block or remove individual recipients by name from a targeted distribution list set for notifications.

Automate emergency scenarios and processes

AtHoc automates operating procedures for emergency situations by providing a library of more than 100 out-of-the-box scenarios, including FPCON, INFOCON and warning conditions.

Scenarios include alert content, response options, targeted recipients and delivery devices. Using simple web-based tools, operators can customize their own scenarios and processes or create new ones.

Within the publishing flow, AtHoc allows for a single alert message to be sent to multiple recipients that share the same phone number (e.g., workgroup, department, call center) while automatically consolidating multiple alert messages into one notification that is then sent only once to the shared phone.



PANIC Button Activated

Aviv Siegel (phone ext. 1002) from 10.1.3.93, AtHoc HQ, cubicle 12.

Please Respond:
- ● I am handling the situatio
- ● False alarm

Respond and Close

Published on: 05/04/2009 1

Tornado Warning

A tornado is expected, seek shelter immediately.

High Wind Alert

High Wind Advisory. Use caution when using bridges.

:31 by: Tifany Kaldy

Hurricane approaching

Hurricane approaching the southwest coast. Take shelter as quickly as possible.

Please Respond:
- ● I am taking shelter.
- ● I need assistance evacuating.
- ● I am not in the area.

Respond and Close

Published on: 11/20/2009 11:08 by: Tifany Kaldy

Flooding alert

Flooding alert at Sycamore and Main Street. Please respond if you are able to assist.

Please Respond:
- ○ I am in the area and will direct traffic
- ○ I am not in the area to assist

Respond and Close

Published on: 11/20/2009 10:53 by: Tifany Kaldy

Examples of the 100+ out-of-the-box alert scenarios

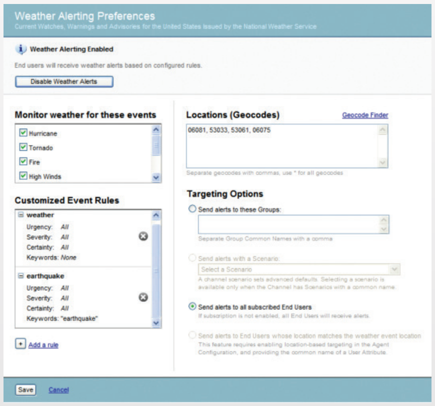
Send real-time alerts to security personnel using the IP phone panic button

Specific keys on IP phones can be configured as Panic or Duress Buttons. By clicking this button, users can send real-time alerts to security officers or emergency operation center (EOC) operators quickly and quietly. The Panic Alert received by the EOC operators identifies the affected individual as well as the location and type of emergency, allowing security operators to take immediate action.

The Panic Button on a Cisco IP phone and resulting pop-up alert sent to security personnel

Enable event monitoring and system interoperability

Emergency alerts are often triggered by physical sensors (e.g., fire alarms, video surveillance and chemical detectors) or external data sources (e.g., National Weather Service content feeds). AtHoc can monitor these events. Using preconfigured business rules, it can automatically activate any emergency scenario. By utilizing Common Alerting Protocol (CAP), XML and web services, AtHoc also enables communication with external systems, such as federal, state and local agencies for information sharing and interoperability.



Weather Alerting Preferences

Current Watches, Warnings and Advisories for the United States Issued by the National Weather Service

Weather Alerting Enabled

End users will receive weather alerts based on configured rules.

Disable Weather Alerts

Monitor weather for these events
- ☑ Hurricane
- ☑ Tornado
- ☑ Fire
- ☑ High Winds

Customized Event Rules

weather
Urgency: *All*
Severity: *All*
Certainty: *All*
Keywords: *None*

earthquake
Urgency: *All*
Severity: *All*
Certainty: *All*
Keywords: "earthquake"

Add a rule

Locations (Geocodes) Geocode Finder

06081, 53033, 53061, 06075

Separate geocodes with commas, use * for all geocodes

Targeting Options
- ○ Send alerts to these Groups:
  Separate Group Common Names with a comma
- ○ Send alerts with a Scenario:
  Select a Scenario
  A channel scenario sets advanced defaults. Selecting a scenario is available only when the Channel has Scenarios with a common name.
- ● Send alerts to all subscribed End Users
  If subscription is not enabled, all End Users will receive alerts.
- ○ Send alerts to End Users whose location matches the weather event location
  This feature requires enabling location-based targeting in the Agent Configuration, and providing the common name of a User Attribute.

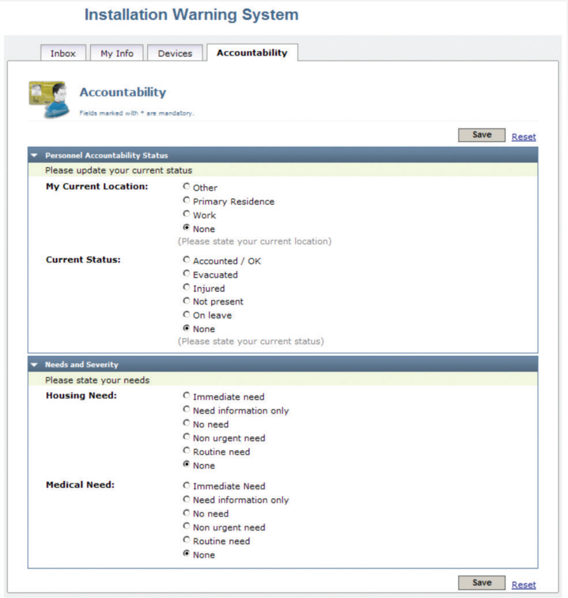
Save Cancel

Monitor external sensors and event sources, including critical weather conditions using the AtHoc Weather Alerts Module

Maintain up-to-date contact information and self-service

Maintaining the accuracy of personnel contact information is crucial for the success of any large-scale emergency notification system. AtHoc addresses this challenge via a four-tiered approach:

- **Integration with organizational repositories** – AtHoc concurrently integrates with multiple enterprise user directories to continuously synchronize personal and organizational information. Supported repositories include Active Directory, LDAPv3, and common HRMS applications.
- **Stale data cleanup** – Operators may also disable and delete end-user accounts and corresponding contact information based on customizable user criteria (e.g., users not logged in for 60 days), enhancing notification accuracy for improved accountability.
- **Operator management** – Local operators can manually update contact information for their local personnel or import personnel rosters in common file formats (e.g., .csv, xls).
- **User self-service** – End users can access and modify their own personal information and device preferences through a web-based, self-service portal, as well as view their personal alert Inbox.



Installation Warning System

Inbox | My Info | Devices | Accountability

Accountability

Fields marked with * are mandatory.

Save Reset

Personnel Accountability Status

Please update your current status

My Current Location:
○ Other
○ Primary Residence
○ Work
● None
(Please state your current location)

Current Status:
○ Accounted / OK
○ Evacuated
○ Injured
○ Not present
○ On leave
● None
(Please state your current status)

Needs and Severity

Please state your needs

Housing Need:
○ Immediate need
○ Need information only
○ No need
○ Non urgent need
○ Routine need
● None

Medical Need:
○ Immediate Need
○ Need information only
○ No need
○ Non urgent need
○ Routine need
● None

Save Reset

The self-service module allows users to update their own contact information, alerting preferences and status

Monitor, supervise and troubleshoot system health

AtHoc provides administrators complete visibility into the health of the system and end devices via visual indications, system and detailed event logs as well as proactive notifications of important system and device status changes that may affect the notification process. Visual indicators within the system give the operator immediate awareness of the status of various capabilities and features (e.g., red, yellow, green). Supervision of the system is achieved across all system components, including network and integrated end devices such as strobes, alarms and displays. Integral troubleshooting tools allow system issues to be resolved quickly.

Predict alert targeting

AtHoc supports (patent pending) device coverage reports post-alert as well as prior to publishing a notification that disclose how many users will be reached when an alert is activated. These reports allow an operator to choose the best method of reaching recipients based on the current contact data in the system.

Scale operations as your needs evolve

AtHoc supports further scaling out of the operation by cascading separate systems for single-action alert activation across organizations. This unique capability can logically interconnect AtHoc implementations for greater recipient reach. The same cascade capability can also be configured internally to the AtHoc system between VPSs to allow common alert activation across VPSs.

Report on cascading

The cascaded delivery summary reports include targeted, sent, received and acknowledged for cascading alerts and will show the sum total of alert activity from sub-virtual systems into original alert.

Enable enterprise-wide operations and multitenancy

With its enterprise capabilities, AtHoc can be deployed centrally using a secure private cloud architecture to support a multisite implementation while accommodating the alerting needs of each individual group, enabling organizational emergency directors to disseminate alerts to the entire user population with visibility across the entire enterprise, while providing each remote site its own “private” alerting system. AtHoc also includes a permissions management system that controls operator access rights to scenarios, contact information and device types. Beyond increased data confidentiality and network security, this centralized (“private cloud”) approach provides a common notification system across the enterprise. Private cloud deployments also reduce infrastructure and maintenance costs and enable organizations to notify and gather responses from hundreds of thousands of personnel in minutes.

AtHoc can support a single site or a multisite organization while accommodating the notification needs of each location. All alerting devices can be triggered either by a local site or centrally by headquarters.

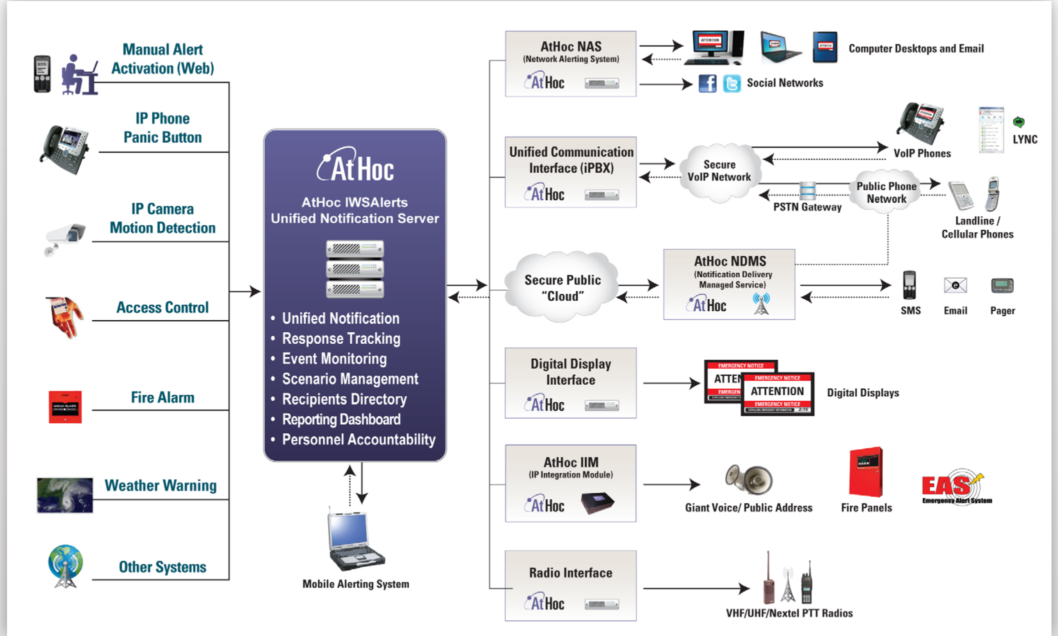
Enterprise-class architecture

AtHoc provides many enterprise capabilities, including:

- **High availability:** Manual and automatic failover; instant, transparent connection to provisioned end devices to multiple gateways in case of critical failure of primary site
- **Security:** Provisions for secure communication, authentication and encryption using industry-standard PKIs
  - Digitally signed email (SMTP) delivery and sending directly using the organization's email address domain
  - The management system supports integration with CAC (Smart Card) and PIV login for operator authentication
- **Scalability:** A load-balanced server farm to support hundreds of thousands of end users
- **User directory integration:** Active Directory, LDAP and other common enterprise directories accessible via API
- **Deployment flexibility:** Multiple delivery options including:
  - On-premise: Entire system deployed behind the firewall leverages secure integration with user directory and internal resources including network, Cisco Unified Communications Manager, Microsoft Lync, public address systems, siren systems and physical security sensors
  - On-premise with telephony alerting via IP-based unified communications: Delivery of alerts as audio messages to any land, mobile or VoIP phone
  - Hosted/Software-as-a-Service (SaaS): Available as a service from a redundant and highly available remote hosting facility, deployment is expedited and the need for on-site hardware is eliminated. AtHoc SaaS service is certified per NIST SP 800-53 Rev3 IA controls at FIPS-199 Moderate classification
  - On-premise with hosted managed notification delivery service: Software installed locally with secure access to remote communication center for mass telephony dialing and text messaging without taxing local telephony resources
  - On-premise with hosted failover: Software installed locally with failover to host facility, assuring redundancy

AtHoc Mobile Alerting System

AtHoc Mobile Alerting System (MAS) includes an AtHoc server instance that is packaged preloaded on a ruggedized or semi-ruggedized laptop computer. MAS can connect to a central alerting site via VPN using wired or wireless transmission. It can also use the local AtHoc server for direct access to the remote communication center, maintaining telephony alerting capabilities in the event of a catastrophic breakdown of local infrastructure. If an evacuation is necessary, AtHoc's MAS is portable and can be carried easily by a single person. Data is synchronized from central site to local site to ensure the local site is always up-to-date. The system allows Internet connectivity through LAN, Wi-Fi, wireless broadband and satellite channels. MAS does not depend on the local infrastructure (e.g., PBX, IP network) to provide full alerting capabilities.


Manual Alert Activation (Web)
IP Phone Panic Button
IP Camera Motion Detection
Access Control
Fire Alarm
Weather Warning
Other Systems
AtHoc
AtHoc IWSAlerts Unified Notification Server
• Unified Notification
• Response Tracking
• Event Monitoring
• Scenario Management
• Recipients Directory
• Reporting Dashboard
• Personnel Accountability
Mobile Alerting System
AtHoc NAS (Network Alerting System)
Computer Desktops and Email
Social Networks
Unified Communication Interface (iPBX)
Secure VoIP Network
VoIP Phones
LYNC
PSTN Gateway
Public Phone Network
Landline / Cellular Phones
Secure Public "Cloud"
AtHoc NDMS (Notification Delivery Managed Service)
SMS
Email
Pager
Digital Display Interface
ATTENTION
Digital Displays
AtHoc IIM (IP Integration Module)
Giant Voice/ Public Address
Fire Panels
EAS Emergency Alert System
Radio Interface
VHF/UHF/Nextel PTT Radios

The above architecture diagram shows the role of AtHoc in monitoring events from multiple sources (on left), delivering alerts to multiple devices and capturing responses from individuals (on right)

Compliance with federal requirements and guidelines

National Fire Alarm and Signaling Code (NFPA 72)

The National Fire Alarm and Signaling Code (NFPA 72) updated its code in 2010 to include Distributed Recipient Mass Notification Systems (DRMNS). The NFPA code provides the blueprint for the implementation of ENS (or, as the code labels it, DRMNS) in facilities nationwide. AtHoc complies with NFPA 72 (2010) DRMNS requirements.

NFPA 1600

Standards on Disaster/Emergency Management and Business Continuity Programs. AtHoc complies with NFPA 1600.

UFC Recommendations for Network-Centric Alerting Systems

The DoD's Unified Facilities Criteria (UFC) 4-021-01 titled "Design and O&M: Mass Notification Systems" provides planning and design of mass notification systems and applies to US military departments and defense agencies. AtHoc complies with the specifications for Network-Centric Alerting Systems (NCAS) incorporated in the UFC.

NIST SP 800-53 Rev3 IA Controls at FIPS-199 Moderate Classification

AtHoc has been certified for its SaaS service per NIST SP 800-53 Rev3 IA controls at FIPS-199 Moderate classification. This process is equivalent to DIACAP (MAC level II) security certification processes done by our government customers. AtHoc is the only vendor to offer such certified SaaS service.

Security and Network Certifications

AtHoc has many DoD security and network certifications and complies with key DoD security requirements, including:

- DIACAP – certified under DoD Information Assurance Certification and Accreditation Process, DISA 8500
- On DISA Approved Product List (APL) under MNWS category, per UCR 2008 Change 3 Requirements
- NIST SP 800-53 IA Control Set – certified under Rev 2 and Rev 3
- Army-wide Certificate of Networthiness (CoN) and ATO
- Navy/Marine Corps Intranet (NMCI) and Navy ONE-NET Certificate to Operate
- Defense Information Systems Agency (DISA) FSO Gold Standard and applicable STIGs
- DoD Common Access Card (CAC) and Federal PIV compliant
- DoD Password Management Policy
- Secure PKI Digitally Signed On-Premise email delivery
- DoD Standard Ports and Protocols compliant

DoD Instructions and Requirements

- DoD Instruction 6055.17 "DoD Installation Emergency Management (IEM) Program": AtHoc is compliant with the Mass Warning and Notification capability.
- Air Force Instruction (AFI) 10-2501 "Emergency Management Program Planning and Operations": AtHoc meets the AFI's network-centric alerting requirements pertaining to installation warning systems.
- AFI 10-218 "Personnel Accountability in Conjunction with Natural Disasters or National Emergencies": AtHoc supports this AFI by proactively querying personnel for status and providing accountability reports to operators.
- Navy Anti-Terrorism Force Protection (ATFP): AtHoc complies with the requirements of the ATFP program responsible for all Navy installations.

Deployable on All Major DoD Networks

AtHoc has been deployed on the following networks:

- NIPRNET (Unclassified but Sensitive Internet Protocol Router Network)
- SIPRNET (Secret Internet Protocol Router Network)
- NMCI (Navy/Marine Corps Intranet)
- JWICS (Joint Worldwide Intelligence Communications System)
- ONE-NET for OCONUS Navy

Federal Continuity Directive 1 (FCD 1)

Federal Executive Branch National Continuity Program and Requirements Agencies should have procedures in place to contact employees in the event of an emergency. Agencies should establish alternative means for employees to contact the agency in the event an emergency causes a disruption to the regular means of communication with the agency.

OMB Memorandum M-05-16: Regulation on Maintaining

A national directive designating OMB with the authority to issue a regulation on certain telecommunications functions under Section 414 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108- 447).

National Communication System (NCS) Directive 3-10

The National Security Presidential Directive 51/Homeland Security Presidential Directive 20 established a comprehensive program designed to ensure survival of our constitutional form of government and the continuation of the performance of National Essential Functions under all conditions.

Section 508 of the Rehabilitation Act

Section 508 requires federal departments and agencies to ensure that personnel with disabilities have fair access to and use of IT systems. AtHoc Desktop Notifier™ (the desktop component of AtHoc) software passed the Department of Commerce test for Section 508 compliance.

HEA and Clery Act Compliance

Amendments to the Higher Education Act and Clery Act require universities to: Develop and implement communication systems for emergencies and develop procedures or notify their community about emergency situations.

ISO 22320: Emergency management

AtHoc is compliant with requirements for incident response.

Your organization deserves the leader in networked crisis communication.
Go to AtHoc.com or call 650-685-3000