



DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET SW, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

CNICINST 2000.3
N3
NOV 1 2010

CNIC INSTRUCTION 2000.3

From: Commander, Navy Installations Command (CNIC)

Subj: CNIC WIDE AREA ALERT NETWORK (WAAN)

Ref: (a) DoDI 6055.17, DoD Installation Emergency Management
(IEM) Program, 13 January, 2009
(b) OPNAVINST 3440.17
(c) CNICINST 3440.17

Encl: (1) CNIC Wide Area Alert Network Concept of Operations
(CONOPS)

1. Purpose. To execute policy delineated in references (a) and (b), and to provide guidance, operational structure, functional requirements, and assignment of responsibilities for implementation of the Commander, Navy Installations Command (CNIC) Wide Area Alert Network (WAAN).

2. Scope and Applicability

a. Scope. This instruction defines the responsibilities of region and installation commanders to develop capabilities to rapidly warn and notify personnel in the event of an emergency per reference (a). Region and installation commanders, as well as tenant commanders and commanding officers are also directed to ensure assigned personnel are participating in WAAN enrollment.

b. Definition. For the purpose of this instruction, the term "installation" may refer to a single installation or multiple installations under a single commanding officer or officer-in-charge.

c. Applicability. This instruction applies to all Navy region and installation commanders within the United States (U.S.), within its territories and possessions, and overseas in peacetime and wartime conditions. This instruction is applicable to Navy personnel including Active and Reserve

Enclosure (1)

NOV 1 2010

components, Navy civilians, Navy families, Navy and non-Navy tenants on Navy installations, transient military or U.S. Government personnel, contractor personnel, visitors and guests, host-nation personnel, and third-country national personnel, as assigned.

d. Interoperability. The CNIC WAAN shall comply with and be consistent with applicable Federal laws, Executive Orders, and Department of Defense (DoD), Joint, and Department of Navy (DON) policies as defined in reference (b).

3. Background. Mass notification provides real-time information and instructions to personnel in buildings and surrounding areas on board installations using intelligible voice communications along with visible signals, text, and graphics, and possibly including tactile or other communication methods. The purpose of mass notification is to protect life by indicating the existence of an emergency situation and instructing people of the necessary and appropriate response and action.

4. Responsibilities. CNIC will provide administrative control over the WAAN.

a. CNIC Headquarters (HQ), region commanders and staff, and installation commanders and staff shall use this instruction and enclosure (1) when planning for and implementing WAAN.

(1) CNIC HQ Operations (N3) shall:

(a) Establish WAAN requirements and serve as lead coordinator for WAAN consolidation and standardization.

(b) Coordinate WAAN manpower requirements with N1.

(c) Coordinate WAAN facilities requirements, selection, and configuration with N4.

(d) Coordinate WAAN information technology requirements and implementation with N6.

(e) Coordinate WAAN training requirements with N7.

(f) Coordinate WAAN resource acquisition with N8.

(g) Ensure enclosure (1) is reviewed and updated annually.

(2) CNIC HQ Total Force Manpower (N1) shall:

(a) Develop manpower requirements for WAAN as required.

(b) Document WAAN Total Force Requirements in the Total Force Manpower Management System, in coordination with N3.

(3) CNIC HQ Facilities and Environment (N4) shall:

(a) Validate N3 WAAN facility requirements.

(b) In coordination with Navy Facilities Command (NAVFAC), develop Military Construction and/or Facility Sustainment, Restoration, and Modernization projects to establish WAAN capabilities in facilities.

(4) CNIC HQ Information Technology Services (N6) shall:

(a) Maintain the CNIC application / system portfolio to include WAAN.

(b) Process portfolio change requests associated with WAAN.

(c) Register and maintain portfolio items in Navy databases of record (e.g., DoD Information Technology Portfolio-DON, Database Management System) associated with WAAN.

(d) Include WAAN when conducting application, system, database and network reporting.

(e) Provide hosting services and assistance with moving an application/system into one or more CNIC Service Delivery Points associated with WAAN.

(f) Provide systems life cycle management, requirements management and configuration management guidance associated with WAAN.

(5) CNIC HQ Training and Readiness (N7) shall:

(a) Coordinate with N3 for involvement of WAAN in the CNIC Exercise Program.

(b) Support training requirement evaluation and tracking in accordance with approved Workforce Training and Education responsibilities.

(c) Identify WAAN training solutions based on identified training requirements. Incorporate WAAN training into current Shore Force Training Center courses.

(d) Develop and implement WAAN training programs compliant with references (a), (b), and (c).

(6) CNIC HQ Financial Management (N8) shall support N3 with WAAN budget formulation and execution.

b. Navy region and installation emergency managers will have the responsibility of ensuring the list of personnel requiring notification is kept up to date.

(1) Region commanders shall be responsible for implementation of WAAN standardization and implementation within their assigned region.

(2) Region emergency managers shall:

(a) Engage in WAAN requirements definition efforts.

(b) Work closely with NAVFAC and Naval Warfare Systems Command to ensure the WAAN facility design and information technology elements are provided.

c. Installation commanders are responsible for the timely and effectual notification of personnel during all-hazard events impacting assigned personnel, ships within local harbors/ installations, aircraft, and installation structures. WAAN registration and use by individuals is the responsibility of the member's commanding officer.

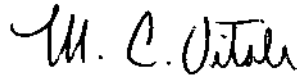
d. Installation emergency management officers shall ensure the list of personnel requiring notification for the installation is kept up to date.

e. Tenant commanders and commanding officers of individual commands and units are ultimately responsible for the safety of assigned personnel and resources and shall ensure WAAN registration and use by their assigned personnel is completed.

NOV 1 2010

5. Actions. Region, installation and tenant commanders and commanding officers of commands and units shall ensure WAAN registration and use by their assigned personnel is completed in support of the use of WAAN within their respective Area of Responsibility in accordance with this instruction. Use of enclosure (1) will assist towards adapting WAAN use within the command's emergency management planning efforts.

6. Effective Date. This instruction is effective immediately.



M. C. VITALE

Vice Admiral, U.S. Navy

Distribution:

Electronic only, via CNIC Gateway

<https://cnicgateway.cnic.navy.mil/HQ/N00/CAPM/DIRPR/Directives/Forms/AllItems.aspx>



**Commander, Navy Installations Command
Wide Area Alert Network
Concept of Operations**

xx 2010

This page intentionally blank

This page intentionally blank

TRANSMITTAL LETTER

The requirement for timely threat and hazard warnings to populations has been documented throughout history. During the twenty-first century, our nation has already endured catastrophic weather events, large-scale and coordinated terrorist attacks, disastrous hazardous material releases, and active shooters in public and private environments. We must make every effort to provide timely threat and hazard warnings to all members of the Navy Family whenever they may be in a potential impact area.

CNIC Instruction 3440.17, *Installation Emergency Management (EM) Program Manual*, provides guidance and fundamental requirements for mass warning and notification. The short time periods required for notification of the Navy Family necessitate the use of contemporary information technologies. When interoperable, resilient, and comprehensive in scope, these technologies are termed a Wide Area Alert Network (WAAN).

The successful development and implementation of a CNIC WAAN as a part of the EM program will take a coordinated effort among all stakeholders. Only by working together will the Navy achieve greater efficiency and effectiveness in preparing for, mitigating the potential effects of, responding to, and recovering from all identified hazards and threats, including acts of terrorism. I look forward to working with all to achieve our common WAAN goal.

M. C. VITALE
Vice Admiral, U.S. Navy

This page intentionally blank

TABLE OF CONTENTS

1.0	INTRODUCTION	1
1.1	References.....	1
1.2	Purpose.....	1
1.3	Scope.....	1
1.4	Background.....	1
1.5	Overview.....	2
2.0	GOALS, OBJECTIVES, AND RATIONALE	2
2.1	Goals	2
2.2	Objectives	2
2.3	Rationale	3
3.0	CONCEPT OF EMPLOYMENT	3
3.1	Automatic Telephone Notification System.....	3
3.2	Computer Desktop Notification System	4
3.3	Giant Voice/Indoor Voice.....	4
4.0	FUNCTIONAL REQUIREMENTS	4
4.1	The Alerting Process.....	5
4.2	Alert Information	9
4.3	The Alerting Environment	10
4.4	Functional Principles	10
4.5	Architecture.....	11
5.0	SYSTEM OPERATIONAL REQUIREMENTS	13
5.1	Automated Telephone Notification System.....	13
5.2	Computer Desktop Notification System	16
5.3	Giant Voice/Indoor Voice.....	18
6.0	OPERATIONAL USAGE	20
6.1	User Categories.....	20
6.2	User Categories Mapped to Functional Requirements	21
6.3	Sample Operational Scenarios	22
6.4	WAAN Operations Duties and Responsibilities.....	24
7.0	IMPACT CONSIDERATIONS.....	26
7.1	Speed.....	26
7.2	Reliability.....	27
7.3	Resilience.....	27
7.4	Interoperability.....	27
7.5	Flexibility.....	28
7.6	Support.....	28
7.7	Maintenance.....	28
7.8	Security	28
	Appendix A. ACRONYMS	30

This page intentionally blank

1.0 INTRODUCTION

1.1 REFERENCES

- (a) CNIC Instruction 3440.17, *Navy Installation Emergency Management (EM) Program Manual*, 23 January 2006
- (b) DOD Instruction 6055.17, *DOD Installation Emergency Management Program (IEM)*, 13 January 2009
- (c) *OPNAV Task Force Navy Family Functional Plan*, 15 April 2006
- (d) UFC 4-021-01, *Unified Facilities Criteria, Design and O&M: Mass Notification Systems*, 9 April 2008
- (e) ATFP PRF ATNS OCONUS-000.10, *Performance Specification for the Anti-Terrorism/Force Protection Automated Telephone Notification System (ATNS) OCONUS*, undated
- (f) ATFP PRF CDNS-00080, *Performance Specification for the Anti-Terrorism/Force Protection Computer Desktop Notification System (CDNS)*, undated
- (g) ATFP PRF-GVIV-001.30, *Performance Specification for the Anti-Terrorism/Force Protection Giant Voice (GV)/Indoor Voice (IV) System*, undated
- (h) NFPA 72, *National Fire Alarm Code*, 2007 Edition

1.2 PURPOSE

This document provides functional requirements and a vision of the Commander, Navy Installations Command (CNIC) Wide Area Alert Network (WAAN). It describes who will use the WAAN, how it will be used, the benefits of its use, standards to be leveraged during its development and provides a high-level description of the WAAN operational and systems architecture. The architectural description is presented to aid development of operational and system view architectures per Department of Defense Architectural Framework (DODAF) requirements.

1.3 SCOPE

The functional scope of this document includes the functional requirements and alerting process for the WAAN. The system scope includes the interoperating family of systems supporting the complete alerting process and three systems that have been piloted at selected CNIC locations to support portions of the alerting process:

- Giant Voice/Indoor Voice (GV/IV)
- Computer Desktop Notification System (CDNS)
- Automatic Telephone Notification System (ATNS)

1.4 BACKGROUND

The dual goal of emergency preparedness is to save lives and minimize property loss. An essential component in saving lives is the capability to warn members of the public who may be at risk of exposure to a hazard. The requirement for a means to provide timely warning of hazards is fundamental and has been documented in reference (b).

The time that elapses from the detection or identification of a threat/hazard to the decision to warn that population to the time the population receives warning and protection information must be as short as possible. Speed of execution in the alerting process is of paramount importance to the success of the Navy Ashore WAAN. References (a) and (b) provide the fundamental functional requirement for the Navy Ashore WAAN.

1.5 OVERVIEW

The Navy Ashore WAAN is envisioned as a family of interoperating systems that leverage existing standards and technologies to provide time-effective alerts and protective guidance to members of the Navy Family¹ whenever hazards threaten their welfare. Sensors, systems, and system components that support threat detection and identification will transmit threat attributes in a standard form to a centralized workstation, where individuals rapidly structure alerts for dissemination to the public. Upon rapidly structuring the alert and protective guidance, the operator will be able to quickly disseminate the information to a quickly definable target group or groups of recipients. The alert information may be disseminated in multiple visual and auditory forms using multiple dissemination means and modes. The WAAN will accommodate the mobile nature of recipients and be 99.99% reliable in all terrain and weather environments.

2.0 GOALS, OBJECTIVES, AND RATIONALE

2.1 GOALS

Following the initial decision by commanders and authorized emergency personnel to warn and notify the Navy Family, the goals of a WAAN are as follows:

- Provide warning in a time-effective manner to persons within a potential area of impact of a threat/hazard that has the potential of causing harm
- Notify every person within the potential area of impact with applicable instructions and protective measures

2.2 OBJECTIVES

Objectives toward achieving those goals include the following:

- Development of a target WAAN architecture
- Identification of existing standards to enable or facilitate data sharing among WAAN components and systems
- Pilot testing of auditory and visual alerting systems compliant with the target architecture and data-sharing standards
- Acquisition of a WAAN data-sharing infrastructure compliant with the target WAAN architecture and selected standards

¹ The term "Navy Family" is used consistent with its definition in reference (c).

- Acquisition and fielding of successful pilot systems compliant with the WAAN architecture and selected standards
- Development of Automated Program Interfaces (APIs) between the acquired alerting systems and the WAAN data-sharing infrastructure
- Acquisition or development of additional WAAN systems or components that further speed the alerting process
- Development of APIs between the additional systems/components and the WAAN data-sharing infrastructure

2.3 RATIONALE

Navy Family members are the Navy's most valuable resource. The incapacitation or loss of any member of the Navy Family adversely impacts the Navy mission. Expressed as a business case, the rationale for a robust Navy Ashore WAAN is that the costs to alert Navy Family members are justified as essential to protect and secure these valuable Navy resources.

3.0 CONCEPT OF EMPLOYMENT

The WAAN System will consist of an interoperating family of systems which support warning to all personnel within the mandated 10-minute time period as described in reference (b).

To shorten alerting time near term, three commercial off-the-shelf (COTS) systems have been pilot tested at selected Navy installations. Those systems are ATNS, CDNS, and GV/IV.

Ultimately, these systems must be interoperable and controlled from a manned watch station such as a Regional Operations Center (ROC) or installation Emergency Operations Center (EOC) with capability for operation at the region/installation dispatch center. Remote capabilities must also be provided for use in the event the primary location is not available. The routine operation and maintenance of this system must be supported by local standard operating procedures (SOPs) that clearly define the operational parameters, release authority, and maintenance responsibilities for the WAAN System.

3.1 AUTOMATIC TELEPHONE NOTIFICATION SYSTEM

The ATNS CONUS servers will be installed at the Transitional Hosting Center (THC) and will support the Navy installations within their specific regions. ATNS will be capable of being controlled from a primary location such as an EOC and one or more alternate locations (such as the alternate EOC, ROC, alternate ROC, regional/installation dispatch center, or Command Duty Officer [CDO] Desk). ATNS outside the continental United States (OCONUS) will contain installation mapping information and end users phone data for all Navy Family members associated with the installations covered by the EOC area of responsibility (AOR) both on and off the installation.

3.2 COMPUTER DESKTOP NOTIFICATION SYSTEM

The CDNS servers for each region will be installed at the THC and will support the Navy installations within their specific regions. CDNS will provide for segregating each of the installations into a virtual installation, where each will be able to control the generating, sending, and tracking of alerts to its on-installation personnel. All parts of the CDNS will be capable of being controlled from a primary location such as a ROC and one or more alternate locations (such as the installation EOC, alternate ROC, regional/installation dispatch center, or CDO Desk) via a web interface over the network.

3.3 GIANT VOICE/INDOOR VOICE

The GV/IV capability will consist of networked zones that can be controlled locally and regionally. At the lowest level, a command will be able to use its GV/IV assets within a shared building complex to make announcements or conduct drills without interfering with adjacent command activities. The networking of these small zones will allow higher-level commands to control the system within multiple zones simultaneously. At the highest levels, all GV/IV zones on a Navy installation will be capable of being controlled from a primary location, such as the Dispatch Center or EOC. Selected zones on multiple bases within a region will be controlled from a ROC.

The ability to de-conflict and prioritize control of a given zone is required since there will be multiple access points which control each zone. In addition, higher-level commands will require the ability to disseminate multiple messages to different zones simultaneously. For example, personnel within a high-threat zone may be directed to evacuate while personnel in lower-threat zones are directed to shelter-in-place until the high-threat zones are cleared. Prioritization of messages and alerts will be required to allow routine uses of GV/IV to be overridden by emergency alerts. Objectively, all WAAN capabilities (ATNS, CDNS, and GV/IV) will be controlled from a common interface or at least a common piece of hardware.

4.0 FUNCTIONAL REQUIREMENTS

In addition to the notification of Navy Family within the 10-minute time period required by reference (b), mass warning and notification systems must support the following installation emergency preparedness (EP) Navy mission-essential tasks (NMETs):

- 4.8.3 Perform interagency coordination
- 5.1.1 Communicate information
- 5.2.1 Analyze mission and current situation
- 5.8 Provide Public Affairs services
- 6.1 Enhance survivability

The CNIC WAAN shall support the following installation command, control, and communications (C3) NMETs:

- OP 2.2 Collect and share operational information

- OP 2.2.1 Collect information on operational situation
- OP 2.2.3 Collect and assess METOC operational information
- OP 2.4.1.1 Identify operational issues and threats
- OP 2.5 Gain and maintain situational understanding (SU)
- OP 5.1.1 Communicate operational information
- OP 5.1.3 Determine commander's critical information requirements
- OP 5.2 Assess operational situation
- OP 5.3 Prepare plans and orders
- OP 5.7.4 Coordinate plans with non-DOD organizations

The recent nationwide emphasis on mass warning and notification has led to increased use of the term “alerting” to refer to the overall warning and notification process and “alert” to refer to both the act of warning and the information that constitutes a warning. Thus, a WAAN is a networked system of interoperating components that execute the alerting process and deliver an alert to a person, a population, or another system.

4.1 THE ALERTING PROCESS

Five basic functions or sequential steps span the alerting process: detection, input transmission, alert structuring, alert distribution, and alert reception. When the alerting process is considered as a “system,” the basic input/output model is as depicted in Figure 1.



Figure 1. The WAAN Alerting Process.

As used in Figure 1, the word “threat” represents all threats and hazards.

4.1.1 Threat Detection

The organizations constituting the Commander, Navy Installations Command face a wide range of man-made threats and natural hazards. The threat detection step of a WAAN can be accomplished by sensors, animate or inanimate sensory systems, or human cognition/recognition capable of expressing threat attributes in a broadly adopted standard data form. Examples of categories of threats/ hazards requiring notification of personnel within the command include, but are not limited to:

- Destructive weather
- Seismic/geological hazards
- Fire hazards
- Pandemic disease
- Hazardous materials spill/release
- Transportation accidents
- Structural failure/collapse

- Infrastructure or utility loss or interruption
- Environmental pollution/contamination
- Food/water contamination
- Chemical terrorism
- Biological terrorism
- Radiological terrorism
- Nuclear terrorism
- Explosive or incendiary terrorism
- Electromagnetic or cyber terrorism
- Civil disturbance
- Naval nuclear reactor accidents/incidents
- Commercial nuclear reactor accidents/incidents
- Nuclear weapon accidents/incidents
- Active Shooter

Inherent within the detect threat step is the requirement to articulate the attributes of the threat necessary to structure an alert. The CNIC WAAN threat attribute information shall include the threat's type, description, urgency, severity, certainty, potential geospatial area of impact, and source/sender identification, all expressed in a broadly adopted standard data form.

4.1.2 Threat Information Transmission

Once a threat is detected and information regarding the attributes of the threat are compiled, those attributes must be transmitted to a system and/or person capable of assessing the threat information and, if appropriate, structuring an alert. Transmission of the threat attributes may be in any form from human speech to electronic message using any communication mode.

4.1.3 Alert Structuring

If the threat information is transmitted as electronic data and if it is received by a data-processing system supporting the structure alert step, the data must be in the format, or convertible into the format, used by the alert structuring system.

In a WAAN, an alert is most often structured by a human based on threat attributes provided by the threat detection source. While automated threat structuring and response action (e.g., smoke sensor to sprinkler system) are desirable for simple local situations, the scope of this concept of operations focuses on the more complex threat situations occurring over a wide area. The process model within that scope may be a "human in the loop" (Figure 2), or more efficiently, a human in the loop aided by a system (Figure 3). The information within the alert must be structured quickly and succinctly.

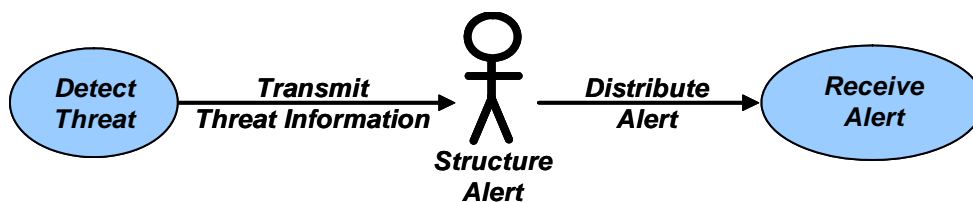


Figure 2. Human in the Loop.

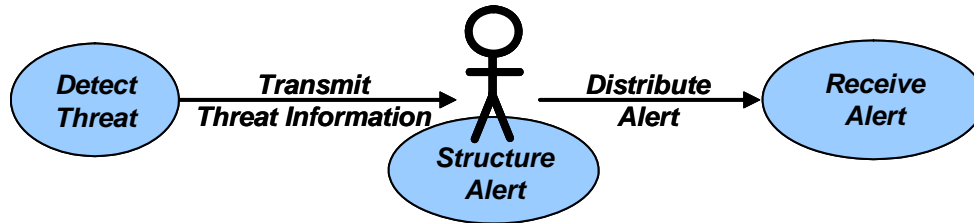


Figure 3. Human in the Loop Aided by a System.

(NOTE: The detect threat step may also be represented by a system, a person, or a person using a system.)

The CNIC WAAN is envisioned to incorporate multiple sources of inputs from the threat detection step and multiple systems for the alert distribution step. While most contemporary alerting technologies employ the Common Alerting Protocol (CAP) standard, a few do not. If a non-CAP standard system or component is selected for inclusion within the CNIC WAAN family of systems, a data transform common service will be required along with other common services to establish system interoperability, provide user control, and facilitate system administrator maintenance and management of the WAAN. Role-based access control of system permissions and privileges and alert authoring shall be two of the accessible WAAN common services.

4.1.4 Alert Distribution

Systems or components supporting the structure alert step of the alerting process in the CNIC WAAN shall provide decision support for defining who will receive the alert and rapid selection of the communication means/modes by which it will be distributed.

Any system supporting the structure alert step of the alerting process in the CNIC WAAN shall provide the capability for the user to rapidly select one or more alert distribution types and rapidly specify the extent of the alert distribution within each type. Distribution types include but are not limited to the following:

- Geographic distribution—dissemination of an alert via best available communication means and modes to a clearly defined geospatial area.
- Organization type distribution—dissemination of an alert via best available communication means and modes to types of organizations, e.g., all fire stations, all medical treatment facilities, etc.
- Specified organizations/individuals—dissemination of an alert via best available communication means and modes to organizations or individuals as specified by the system user.
- Specified categories of individuals—dissemination of an alert via best available communication means and modes to one or more categories of individuals as specified by the system user. For CNIC, the categories of individuals are Categories 1–5 as specified in reference (a).

4.1.5 Alert Reception

An alert may be received by a human, a system, or a human using a system/communication device. If the alert is in electronic data form, it must be in a format usable by the receiving system/device or convertible by the receiving system/device.

4.2 ALERT INFORMATION

The Common Alerting Protocol (CAP), Version 1.1 was adopted on 1 October 2005 by the Organization for the Advancement of Structured Information Standards (OASIS) international standard development organization. The CAP 1.1 standard (available at www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf and incorporated by reference in this document) has been adopted by the U.S. Federal Emergency Management Agency (FEMA), the National Oceanographic and Atmospheric Administration (NOAA), and all significant vendors of alerting systems in North America. It is now engaged in the standard adoption process in the European Community and Australia. The alert data model and definitions are now accepted as definitive by the U.S. EM community. The CAP data model is presented in Figure 4. See the CAP 1.1 standard for the associated data dictionary.

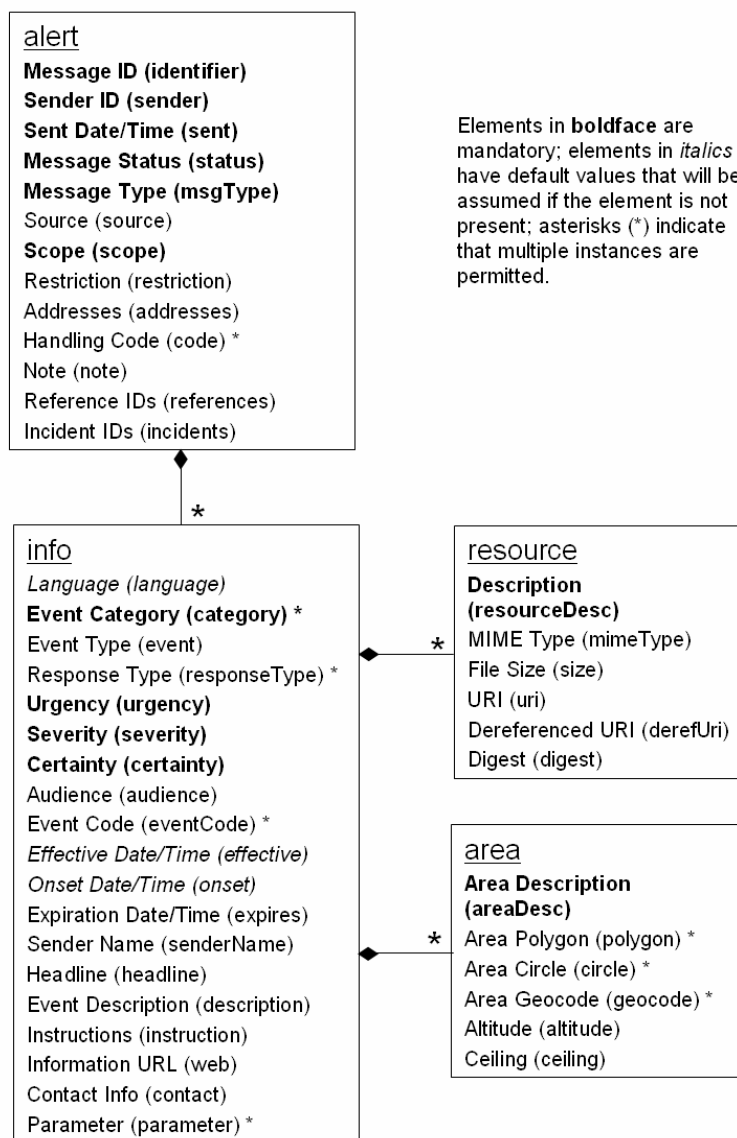


Figure 4. CAP Data Model.

4.3 THE ALERTING ENVIRONMENT

The characteristics of the environments in which the CNIC WAAN will operate are significant factors shaping functional and operational requirements and the overall system architecture.

4.3.1 Physical Environments

The vision for CNIC WAAN is to have a capability of capturing and transmitting threat detection information and disseminating alerts in all Navy installation physical environments.

4.3.2 Organizational Environments

The CNIC WAAN shall be capable of disseminating threat and alert information vertically among the CNIC echelons of command and horizontally with military and civilian peers at each echelon and among the other uniformed Service tenants on a joint base.

4.3.3 National Environments

The CNIC WAAN shall be capable of employing communication means and modes in the continental United States (CONUS) and OCONUS in host nations where family members of Department of Navy personnel live.

4.3.4 Population Attributes

Generally, members of the Navy Family are very mobile and alert, monitor public radio and television communications, and are comfortable using common information technology (IT) devices such as computers and cellular telephones. While Navy Family members are generally “reachable” at any point in time, the communications means/mode by which they may be reached at any moment can vary widely. This fact drives the need for the CNIC WAAN to be capable of using a wide range of communications to disseminate alerts.

4.3.5 Population Distribution

The CNIC WAAN must be able to deliver threat information and alerts to Navy personnel and their family members whether at work, at home, or travelling within the installation’s AOR.

4.3.6 Threats

The threats and hazards that prompt the need for the CNIC WAAN also threaten the CNIC WAAN itself. These threats/hazards drive system architecture and deployment requirements to make the overall system survivable, resilient, reliable, and accessible even if some of its components are adversely impacted by a disaster incident.

4.4 FUNCTIONAL PRINCIPLES

From the WAAN user and alert recipient stakeholders’ functional perspectives and requirements, 10 key principles emerge:

Principle 1: Speed. The objective of a WAAN is to warn a population at risk in time for each individual to take protective actions. The need for speed is paramount.

Principle 2: Assured Delivery. Alert messages must be delivered to alert recipients in a form that makes them aware of the presence of the alert information.

Principle 3: Reliability. Each system and component of a WAAN must work the first time, every time.

Principle 4: Resiliency. External factors can cause degradation or loss of WAAN systems and components. WAAN architecture must employ best practices such as failover redundancy and database replication to ensure survival of WAAN functionality despite loss of systems or components.

Principle 5: Interoperability. A WAAN consists of multiple systems and components. Data must be shared among them. CNIC WAAN shall also consider interoperability with civilian partner CDNS, ATNS, WAAN, and EOCs and the national Integrated Public Alert and Warning System (IPAWS) where possible.

Principle 6: Intelligibility. Threat and alert information must be readily understood by each recipient.

Principle 7: Accessibility. Systems and components of the WAAN must be readily accessible to WAAN users and alert recipients.

Principle 8: Portability. System users and alert recipients move about. Mobile information technologies must be leveraged to enable WAAN access by system users and alert recipients.

Principle 9: Flexibility. The WAAN must employ broadly adopted standards to enable “plug in” of new systems/components at minimal cost and risk to existing systems.

Principle 10: Security. While some components supporting threat detection and transmission of threat information and access to alert structuring functions need to be controlled, alerts must be open for widest possible dissemination to the population at risk.

In addition to WAAN user and alert recipient functional requirements, these principles should be used to drive and shape operational, system, and technology architectures and system operational requirements for the CNIC WAAN.

4.5 ARCHITECTURE

Figure 5, an informal “architectural” representation, is useful in the following ways:

- Is easily understandable.
- Helps user stakeholders relate the alerting process steps to the range of systems, networks, and devices that could potentially constitute a WAAN.

- Depicts an interoperability hub with the clear implication that users have access to common services as appropriate for their role.
- Depicts the requirement for the WAAN to be capable of employing the full range of contemporary communication means and modes.
- Assists with development of formal architectural views per DODAF requirements.
- Implies a service-oriented architecture or common services architecture approach to the interoperability requirement, whereby any system or component participating in the “family of systems” needs to develop and maintain only a single systems interface. of systems” needs to develop and maintain only a single systems interface.
- Depicts an “integrated base station” from which the WAAN may be controlled.

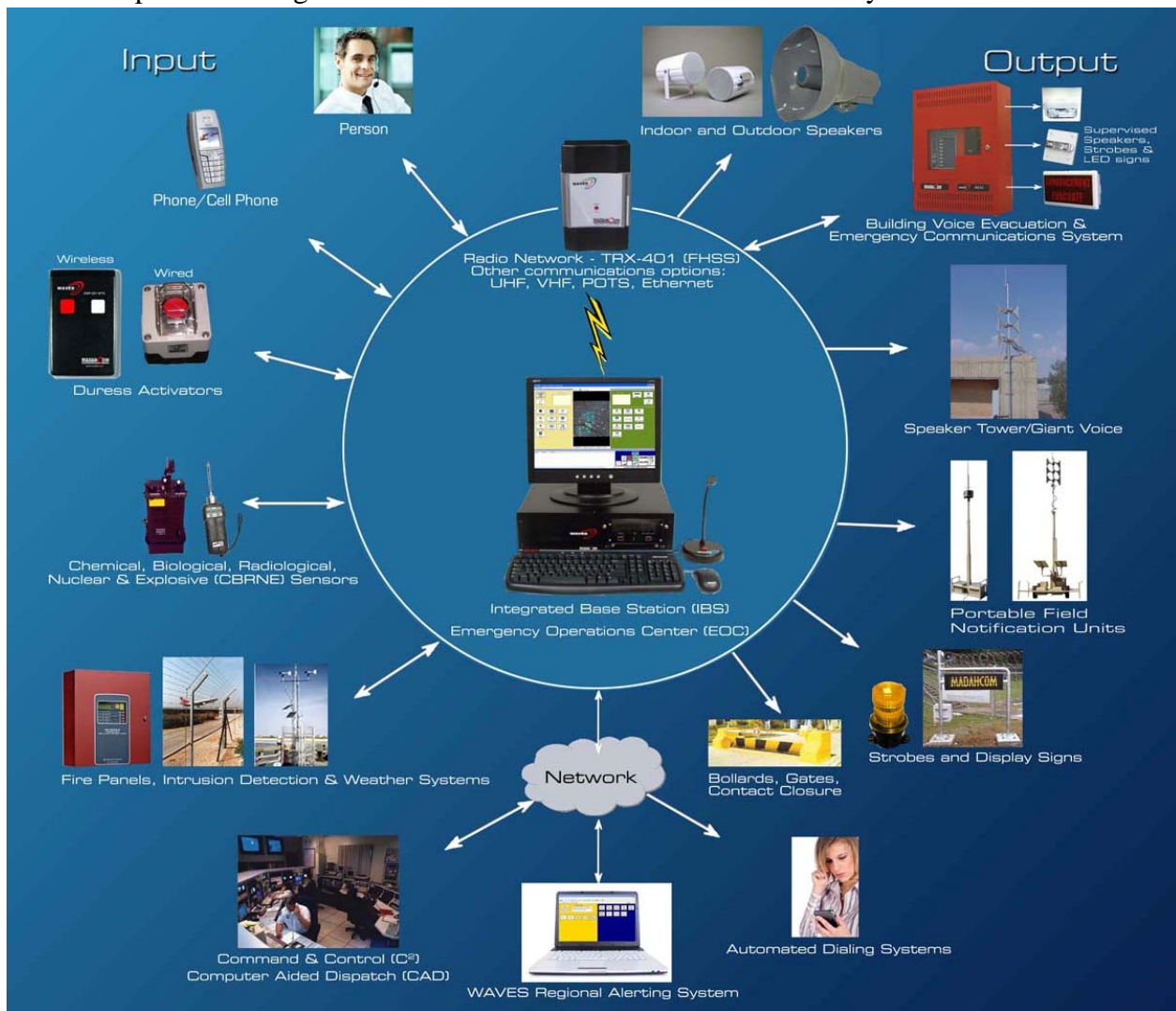


Figure 5. Informal Architectural Representation of WAAN.

(Courtesy Ray Grill, Arup Group, 25 January 2008 presentation “Mass Notification: NFPA 72-2007 and Beyond!”)

More formal operational, system, and technology architectural views should be developed in accordance with DoDAF requirements to assist understanding of multisystem interoperability requirements.

5.0 SYSTEM OPERATIONAL REQUIREMENTS

Reference (d) is written solely from a facility or building perspective and is terrorism-threat focused. It addresses individual building mass notification systems, GV notification systems, telephone alerting systems, and base-wide control systems. The functional features listed presume delivery of only audio alerts to buildings and the vicinities of buildings. Within those constraints, the document does provide listings of functional features and maintenance criteria for each of the four systems. Those features and criteria are considered included within this document by reference.

References (e) and (f) state the three principal WAAN capabilities currently fielded to meet these needs. References (e), (f), and (g) provide performance specifications for the individual systems supporting the three capabilities. Each of the three references also provides a listing of “system functional elements.” These capabilities are described as follows:

- Interactive, community notifications systems capable of providing voice and/or data messages to multiple receivers (telephone and cellular phones)
- Broadcasts across the computer system network consisting of a notice from a central location that would override the current computer user’s applications, thereby reaching all computer users nearly instantaneously
- Region/installation-wide voice announcing system, including interior (IV) and exterior (GV) speakers.

5.1 AUTOMATED TELEPHONE NOTIFICATION SYSTEM

5.1.1 ATNS Functional Description

ATNS provides military installations with the ability to rapidly and effectively disseminate emergency alerting and notifications throughout the telephone and data network environments, including signals or messaging appropriate to force protection conditions (FPCONs), weather conditions, watches, warnings, evacuation routes, and other alerting information to meet Department of Defense (DOD) and federal warning requirements.

5.1.2 ATNS Performance Requirements

Principle 1: Speed. All personnel shall receive warning/notification within 10 minutes of an event, and Categories 1 and 5 personnel must receive notification within 5 minutes of an event.

Principle 2: Assured Delivery. Assuring delivery to all personnel is a critical requirement. ATNS capability ensures that alerts will be delivered to authorized users. ATNS will track responses to each call, which can be displayed through system-generated reports. In addition, scenarios can be defined where the intended recipient must enter an access code prior to receiving the message,

which can be tracked by the server. These scenarios can be set up for repeat attempts to deliver the message to the same device or to an alternate device if the recipient is not present.

Principle 3: Reliability. The ATNS shall have an operational availability (A_o) equal to or greater than 99.99% and 1,000 hours mean time between critical failures (MTBCF).

Principle 4: Resiliency. The use of multiple servers to increase call throughput capacity and provide redundancy for contingency operations must be considered. The addition of load-balancing and fail-over capabilities to accommodate use surges during incident response and mitigate risk of system degradation when impacted by external forces would satisfy the requirements inherent in this principle.

Principle 5: Interoperability. Specification of the Open GIS Web Map Services standard vice a proprietary geographic information system (GIS) product Environmental Systems Research Institute (ESRI) would mitigate the risk of single-vendor contract issues. It will also create a more flexible API capable of interfacing to more than one GIS product. Similarly, the specification to interface to single government off-the-shelf (GOTS) plume model could limit flexibility to interface to other plume models should they come into common use.

Principle 6: Intelligibility. While the depiction of a web client application in Figure 1 of reference (e) and some functional elements imply support to the alert structuring step, alert intelligibility also needs to be considered.

Principle 7: Accessibility. ATNS will be installed within each of the installations' EOCs and the ROCs and will support the installations within each AOR. ATNS will contain base-mapping information and end user phone data for each of the installations being covered by the EOC AOR. ATNS will be capable of being controlled from a primary location such as an EOC and one or more alternate locations (such as the alternate EOC, ROC, Regional Dispatch Center (RDC), or CDO Desk) and from the CDNS.

Principle 8: Portability. ATNS OCONUS shall have the ability to reach all installation personnel connected to the telephone and data networks through effective routing and delivery of time-sensitive messages. Alerts can be delivered using audio notifications via the base or commercial telephone network with TTY/TDD support when required. In selected scenarios, the use of multiple devices such pagers, mobile phone, e-mail, and text message-based devices can be used as an alternate method of alerting personnel. In a multi device scenario, a user can choose the delivery device per alert type. Urgent messages, for example, could appear both as a telephone call-out (desk, cellular, or home phone) and as a text message such as e-mail. Administrators can predefine and mandate delivery preferences to broadly distribute urgent alerts through any available device.

Principle 9: Flexibility. The ATNS design shall be of a modular, scalable nature that will facilitate reconfigurations, including adding or removing subcomponents depending on the resources and specific needs of the parent unit, the threat condition, and the operating environment. The modular design concept is also intended to increase logistics flexibility, simplify maintenance of the system, and accelerate implementation of future planned upgrades.

The government anticipates that the ATNS will maximize the use of existing commercial and government subsystems and components. The ATNS shall comply with the DOD IT Standards Registry (DISR) to support uniformity and interoperability with other DOD command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems. The ATNS design shall also comply with applicable sections of the Unified Facilities Criteria (UFC) and local codes and regulations.

Principle 10: Security. The ATNS shall comply with the following security measures at a minimum:

- The system shall allow multiple levels of group based access/security permissions.
- The system shall allow 128-bit digital encryption with user interface.
- The system shall be capable of supporting server- and client-based DOD digital certificates for Public Key Infrastructure (PKI).
- The system shall allow scheduled self-diagnostic testing to ensure functionality of phone lines.
- DIACAP certification, NMCI/ONE-Net certification and installation requirements and JITC certification.

5.1.3 ATNS Deployment Requirements

The ATNS design shall be of a modular and scalable nature that will facilitate reconfigurations, including adding or removing subcomponents depending on the resources and specific needs of the parent unit, the threat condition, and the operating environment. The modular design concept is also intended to increase logistics flexibility, simplify maintenance of the system, and accelerate implementation of future planned upgrades. The government anticipates that the ATNS will maximize the use of existing commercial and government subsystems and components. The ATNS shall comply with the DISR to support uniformity and interoperability with other DOD C4ISR systems. The ATNS design shall also comply with applicable sections of the UFC and local codes and regulations.

5.1.4 ATNS Support and Maintenance Requirements

At a minimum, the ATNS should provide rigorous context-sensitive help via the Web Client Application. The ATNS maintenance plan will be developed by the Procurement, Installation, Maintenance Multi-Award Contract contractor in accordance with the statement of work. The maintenance plan should provide the optimal balance between maintaining the mandated, mission-driven A_o and total ownership cost. It shall be focused on maintaining the concept of mission-relevant, A_o -significant line-replaceable units (LRUs) identified by the vendor, using a systems-engineered, top-down breakdown approach. It shall consider the knowledge, skills, and abilities of the intended ATNS operator and maintainer levels and the resources available at each level. The maintenance concept shall benefit from the system's modular design and shall facilitate the identification of those LRUs to be spared to sustain the ATNS A_o in its intended mission scenario.

5.1.5 Telephone Automated System (TAS)

The OCONUS installations have a mixture of networked and stand alone telephonic systems. The standalone systems work from the base station located in operation centers or other locations selected by the installation Commanding Officer. Due to telephone and network infrastructure OCONUS TAS will be the main telephonic system used.

5.2 COMPUTER DESKTOP NOTIFICATION SYSTEM

5.2.1 CDNS Functional Description

CDNS provides Navy installations with the ability to rapidly and effectively disseminate emergency alerting and notification information throughout the data networks environment, including signals or messaging appropriate to FPCONS, information operations conditions (INFOCONS), watches, warnings, evacuation routes, and other alerting information to meet DOD and federal warning requirements.

5.2.2 CDNS Performance Requirements

Principle 1: Speed. All personnel shall receive warning/notification within 10 minutes of an event.

Principle 2. Assured Delivery and Response.

- *Assured Delivery*—Assuring delivery to all personnel is a critical requirement of CDNS. Its capability to store-and-forward ensures that alerts will never be lost even if a user is temporarily not connected to the network. To assure reach to off-site personnel, CDNS shall use communications protocols that can work seamlessly and reliably across firewalls, routers, and wireless networks. Personal alert history shall be available as well, enabling users to view all recent and active alerts.
- *Assured Response*—Assuring responsiveness to alerts is as important as delivering them. CDNS shall enable customization of each alert to signify different content type or priority (e.g., FPCONS, watches), which then can be matched to the appropriate audiovisual effect for the level of alert and responsiveness required. As an additional method for assuring responsiveness, forced acknowledgement to alerts can be required upon receipt and can be tracked by the server.

Principle 3: Reliability. The CDNS shall have an A_o equal to or greater than 99.99% and 1,000 hours MTBCF.

Principle 4: Resiliency. The CDNS shall use a multi-server configuration with load-balancing and fail-over capabilities to accommodate use surges during incident response and mitigate risk of system degradation when impacted by external forces.

Principle 5: Interoperability. The CDNS shall have the capability to interface with feeds for weather, Rich Site Summary (RSS), CAP, and Extensible Markup Language (XML)–based messages as required.

Principle 6: Intelligibility. The CDNS alert publishing capabilities listed below provide sufficient functionality to support the production of alerts that will be intelligible to recipients:

- *Web-Based Publishing Application*—Enables flexible access from any networked computer without requiring any software installation. This feature is especially valuable for enabling multiple users to publish from different locations and to create alternative communication posts when main post is disabled.
- *Permission-Based Multi-Publishers*—Delegate publishing responsibility throughout the organization.
- *Alert Channels*—Create messages according to types, such as FPCON and INFOCON alerts.
- *Scheduling*—Immediately transmit alerts or schedule for future delivery. Define alert expiration time.
- *Select Templates*—Control desired alert look and feel.
- *Target Alerts*—Publish alerts to targeted users based on their role, location, or department (subject to using the targeting support and connecting CDNS to the installation's user directory).

Principle 7: Accessibility. All parts of the CDNS will be capable of being controlled from a primary location such as an EOC and one or more alternate locations (such as the alternate EOC, ROC, RDC, or CDO Desk) via a web interface over the network.

Principle 8: Portability. CDNS reaches all installation personnel that are connected to the network through effective routing and delivery of time-sensitive messages. Alerts can be delivered using audiovisual notifications via multiple devices, including desktop popup alerts; optional devices include pager, mobile phone, and e-mail. In a multi-device installation, a user can choose the delivery device per alert type. Administrators can predefine and mandate delivery preferences to broadly distribute urgent alerts through any available device.

Principle 9: Flexibility. The CDNS shall be an integration of modular, scalable COTS/GOTS computer networking equipment that will facilitate reconfiguration specific to the needs of each installation. The modular design concept is also intended to increase logistic flexibility, simplify maintenance of the system, and accelerate implementation of future planned upgrades. The CDNS shall comply with DISR to support uniformity and interoperability with other DOD C3 systems.

Principle 10: Security. The CDNS shall comply with the following security measures at a minimum:

- The system shall be compliant with DOD password management policy.
- The system shall be capable of 128-bit digital encryption.
- The system shall be capable of supporting server-based DOD digital certificates for PKI.
- The system shall meet all DOD Information Assurance Certification and Accreditation Process (DIACAP) network certifications requirements per DOD policy.
- The system shall meet all Navy Marine Corps Internet (NMCI)/One Net certification and installation requirements.

5.2.3 CDNS Deployment Requirements

The CDNS should have a multiserver configuration with load balancing and fail-over capabilities. These capabilities are required to accommodate system use surges and mitigate risk of system degradation during a disaster event at or near any single server location.

5.2.4 CDNS Support and Maintenance Requirements

At a minimum, the CDNS should provide rigorous context-sensitive help features which are resident on servers and recalled via the client web application. An additional level of user support would be provided by a 24/7 Help Desk with staff knowledgeable about the system.

5.3 GIANT VOICE/INDOOR VOICE (GV/IV)

5.3.1 GV/IV Functional Description

The outdoor component consists of the outside speaker(s) positioned on pole(s), or other similar outdoor fixtures across the installation. The GV system is installed as an installation-wide system to provide a siren signal and prerecorded and live voice messages. Normally, to create the right level of sound output, multiple poles and speakers will be positioned and professionally installed across the installation by a qualified contractor. The design and operation specifications for the GV/IV are compliant with NFPA 72 standards and will be installed in accordance with Annex \$ (Mass Notification Systems) of NFPA 72. The GV component is most useful for providing mass notification for personnel in outdoor areas, expeditionary structures, and temporary buildings. It is generally not suitable for mass notification to personnel in permanent structures because of the difficulty in achieving acceptable intelligibility of voice messages.

Individual building IV systems are installed to provide real-time information to all building occupants or personnel in the immediate vicinity of a building, including exterior egress and gathering areas.

5.3.2 GV/IV Performance Requirements

Principle 1: Speed. All personnel shall receive warning/notification within 10 minutes of an event.

Principle 2: Assured Delivery. Reference (g) specifies daily use (e.g., playing of the National Anthem, Attention to Colors, Reveille, and Taps). Each of these routine uses constitutes a system test, thus ensuring a high degree of delivery assurance for GV. IV delivery assurance will be tested and evaluated during full-scale exercises on the installation.

Principle 3: Reliability. GV/IV shall have an A_0 equal to or greater than 99.99% and 1,000 hours MTBCF.

Principle 4: Resiliency. GV/IV shall use alternative base control workstations (BCWSs) in addition to the primary to allow for fail-over capabilities and accessibility during incident response and mitigate risk of system degradation when impacted by external forces. These additional BCWSs may be connected using CAP to contribute to the resiliency of the system.

Principle 5: Interoperability. Open, broadly adopted standards such as CAP, the Open GIS Consortium Web Map Services, and transmission control protocol/Internet protocol (TCP/IP) to achieve interoperability among systems, and system components shall be leveraged.

Principle 6: Intelligibility. National Fire Protection Association (NFPA) standards on National Fire Alarm Code (NFPA 72) provides national consensus standards for CONUS. Annex E (Mass Notification Systems) of NFPA 72 provides best practice for system intelligibility requirements.

Principle 7: Accessibility. Accessibility to central control stations and full dissemination of alerts to the population at risk in specified zones shall be accounted for within GV/IV design.

Principle 8: Portability. The portability principle is not applicable to GV/IV.

Principle 9: Flexibility. The modular system design and capability to define and selectively activate alert zones provide the flexibility required of a voice alerting system.

Principle 10: Security. While the following minimum requirements are appropriate for certain operational circumstances, they are not always necessary and in some cases can hinder the accomplishment of desired alerting process actions. The GV/IV specification should include the capability to apply access controls and security measures where and when required. Security considerations for GV/IV assets deployed in Sensitive Compartmented Information Facilities are correctly expressed in paragraph 3.3.2.4 of reference (g). GV/IV shall comply with the following security measures at a minimum:

- Allow multiple levels of group based access/security permissions.
- Be capable of 128-bit digital encryption.
- Be capable of supporting server-based DOD digital certificates (PKI).
- Be capable of supporting client-based DOD digital certificates (PKI).
- Meet all DOD Information Technology Security Certification and Accreditation Process (DITSCAP)/DIACAP network certifications requirements per DOD policy.
- Meet all NMCI/One Net certification and installation requirements.

5.3.3 GV/IV Deployment Requirements

The use of UFCs, design characteristics, functional description and elements, and system interface specifications and recommendations shall ensure deployment requirements are fully understood and are expressed in requirements documentation for the implementation contractor(s).

5.3.4 GV/IV Support and Maintenance Requirements

At a minimum, GV/IV should provide rigorous context-sensitive help at central control stations. The maintenance contractor's plan should provide the optimal balance between maintaining the mandated, mission-driven A_o, and total ownership cost.

6.0 OPERATIONAL USAGE

WAAN users² will vary depending on the step or steps of the alerting process they support and their role. The receive alert step of the alerting process is local. No matter where the threat or hazard is detected/identified, or where the structure alert step is accomplished, the alert must be received by all within the potential geographic area of impact.

6.1 USER CATEGORIES

Table 1 identifies broad categories and example roles within each category to the alerting process they support or execute.

Table 1. WAAN User Categories and Example Roles/Products

Alerting Process Step	User Category	Example Roles and Products
Detect threat and transmit threat information	Human threat/hazard detector-transmitter	Intelligence analyst
		Meteorologist
		Seismologist
		Event observer
	Threat/hazard detector-transmitter technologies	Sensor
		Detection system (e.g., weather station, intrusion system)
RSS feeds		
Structure alert and distribute alert	Human alert author	Shore Support Center/ROC Watch Officer
		CDO
		Region/installation dispatch center staff member
		EM/Emergency Management Officer (EMO)
		EOC staff member
		Incident Commander
	Automated alert authoring and distribution support technologies	WAAN common service (e.g., NOAA HazCollect)
		Incident Management System alert authoring tool
Receive alert	Auditory message reception/presentation technologies	GV/IV system
		ATNS
	Visual message reception/presentation device	Palm-top message devices
		E-mail
		Message display boards
		Incident Management Systems
	Human alert recipient	Any Navy Family member, Categories 1-5

² For the purpose of this document, the term “user” refers to both a human interacting with a WAAN component or system and a WAAN component or system interoperating with another component or system. In Unified Software Development Process Use Case terms, an “actor.”

6.2 USER CATEGORIES MAPPED TO FUNCTIONAL REQUIREMENTS

Table 2 maps WAAN user categories that would be supported by the functional requirements presented in paragraph 4.0.

Table 2. Functional Requirements Relevant to User Categories

User Category	Supporting Functional Requirements
<ul style="list-style-type: none"> • Human threat/hazard detector-transmitter • Threat/hazard detector-transmitter technologies 	#1. Warning time and extent
	#2. EM NMETS (all)
	#3. C3 NMETS (all)
	#4. Threat attribute standardization
	#5. Specified threat attributes
	#6. Multiple threat information transmission modes
	#13. Operation in all physical environments
	#14. Horizontal and vertical information dissemination
	#15. Multiple communications means
<ul style="list-style-type: none"> • Human alert author • Automated alert authoring and distribution support technologies 	#1. Warning time and extent
	#2. EM NMETS (all)
	#3. C3 NMETS (all)
	#4. Threat attribute standardization
	#5. Specified threat attributes
	#6. Multiple threat information transmission modes
	#7. Standard alert data
	#8. Specified alert attributes
	#9. Data transmission services
	#10. WAAN common services
	#11. Alert distribution decision support
	#12. Rapid alert distribution definition
	#13. Operation in all physical environments
	#14. Horizontal and vertical information dissemination
	#15. Multiple communications means
<ul style="list-style-type: none"> • Auditory message reception/presentation technologies • Visual message reception/presentation device • Human alert recipient 	#1. Warning time and extent
	#2. EM NMETS (all)
	#7. Standard alert data
	#8. Specified alert attributes
	#9. Data transmission services
	#11. Alert distribution decision support
	#12. Rapid alert distribution definition
	#13. Operation in all physical environments
	#14. Horizontal and vertical information dissemination
#15. Multiple communications means	

6.3 SAMPLE OPERATIONAL SCENARIOS

The following scenarios are designed to assist system analysts and designers with the understanding of data and work flow within the context of user (human and technological) requirements and operating environments.³

6.3.1 Hurricane Ralph

At 0830 hours, National Hurricane Center analysts determine that Hurricane Ralph, previously classified as Category 2, is dramatically increasing in intensity and will likely strike the Jacksonville area as a Category 4 hurricane in approximately 7 hours. By 0835, the National Weather Service (NWS) is using the NOAA HazCollect system to disseminate a CAP standard alert to emergency managers at state, county, municipal, and military organizations within the potential impact area. At 0837, the Naval Air Station Jacksonville (NAS JAX) EMO receives the NWS CAP message in the form of an e-mail on his Blackberry. Per the EMO's defined preference, the message is automatically forwarded from the Incident Management System in the NAS JAX EOC. The EMO immediately forwards the CAP message to his predefined NAS JAX Commanding Officer (CO)/Executive Officer (XO)/CDO alert message group and calls the XO to ensure the CO sees the NWS alert.

At nearly the same time, the Navy Region Southeast (NRSE) Battle Watch Stander in the ROC receives the NWS CAP alert in the Command, Control, Communications, Computers, and Intelligence (C4I) Suite environment. She immediately brings the alert to the attention of the NRSE CDO. By 0845 the NAS JAX CO and the Commander, NRSE (CNRSE) are conferring with each other. By 0855 decisions are made to execute aircraft relocation, stand up the alternate ROC in Georgia, and implement the nonessential personnel hurricane evacuation plan, and the teleconference is concluded.

The NAS JAX CO immediately directs the CDO to employ the WAAN to warn all hands of the increased hurricane threat and to implement aircraft relocation operations and evacuation of all nonessential personnel. When the EMO forwards the NWS CAP alert, the CDO receives it in both his WAAN message account as well as his regular "navy.mil" e-mail account. By 0855, the CDO accesses the WAAN alert authoring tool, imports the NWS CAP data into it, selects the "All Hands" alert distribution option, and selects the GV/IV and CDNS modes for alert dissemination. When the CO directs him to structure an alert and distribute it via the WAAN, he enters the CO's directions for protective actions. The CO approves the message as the CDO finishes entering the protective action directions. By 0907, all hands either hear the WAAN alert by GV/IV or read the WAAN alert on their computer or handheld device screens.

Simultaneously, the CNRSE directs the NRSE ROC Battle Watch Captain to disseminate the alert throughout the command and include an "informal warning order" within it to prepare for alternate ROC activation. He also directs that an alternate ROC activation Execution Order be prepared and sent for his signature immediately following issuance of the alert. The NRSE ROC Battle Watch member who takes initial action on the NWS CAP alert anticipates the need to

³ These scenarios are not intended to represent policy regarding local procedures. They reflect only plausible actions under the circumstances described.

disseminate its content throughout the command. While waiting CNRSE guidance, she accesses the WAAN alert authoring tool, imports the NWS CAP data into it, selects the “All NRSE” alert distribution option, and selects the CDNS mode for alert dissemination. When the Battle Watch Captain informs her of the “informal warning order” direction by the CNRSE, she enters the information in the alert instructions field. The Battle Watch Captain approves her entry and releases the alert at 0907 hours.

6.3.2 Hazardous Material Release

Naval Construction Battalion Center (CBC) Gulfport, Dispatch Center call recording, 1424 hours:

Caller: Hey, I’m a Seabee. There has just been some kind of problem with a train close to Pass Road. I’m on 25th Avenue at 28th Street and can see a yellow-greenish cloud coming from a tanker truck.

Dispatcher: Sir, which direction is the cloud moving?

Caller: Toward the installation. There’s an on-shore wind [blowing inland from the sea].

Dispatcher: Is the cloud rising?

Caller: No, it seems to be staying within a few feet of the ground. Good grief, I can see some people getting out of their cars. They’re grabbing their throats and coughing. Oh, man, a couple of them just passed out!

Dispatcher (looking at map of the Gulfport area): Sir, I want you to stay on the phone with me but move toward the north along 25th Avenue. See if you can find a spot where you can be at least 400 feet away but still see the incident. If the wind shifts toward you, move quickly to the east.

The Dispatcher calls the Hancock County, MS, Sheriff and Fire Dispatch Center. They confirm the report of the event and inform the Dispatcher that the City of Gulfport Hazardous Materials Response Team has just arrived on site. The Incident Commander IC just spotted 1017 (chlorine) on the tanker truck placard and has directed evacuation to the north and south, then upwind to the east in an area that includes the Navy Construction Center.

The Dispatch Supervisor calls the CBC Gulfport CDO and quickly briefs the situation to the XO. The CO is on leave. At 1428 hours, the XO directs the Dispatch Supervisor to use the WAAN to issue a “by order of the Commander” evacuation order per the on-scene Incident Commander’s recommendation. The Dispatcher Supervisor accesses the WAAN alert structuring tool; selects a predefined Hazardous Materials Alert with Evacuation template; quickly tailors the template information for the current situation; selects the “All Hands” distribution scope; selects GV/IV, CDNS, and ATNS distribution modes; and sends the alert at 1430 hours.

These scenarios demonstrate the following:

- The urgency with which alerts must be disseminated
- Differences in information flow, depending on organization structure, processes, and protocols
- The variety of roles that may require access to the WAAN alert structuring and dissemination tool/common service

- The necessity for multiple modes of alert dissemination

6.4 WAAN OPERATIONS DUTIES AND RESPONSIBILITIES

6.4.1 Region Commander

The Region Commander shall:

- Be responsible for the overall supervision of the operation of the WAAN throughout the region.
- Provide oversight of WAAN use scenarios, alert messages, groups, protocols, and procedures throughout the region.

6.4.2 Region Emergency Manager

The Region Emergency Manager shall:

- Perform WAAN administrator and/or publisher duties, as required.
- Provide alert messages and group(s) sets to the ROC for all EM scenarios.
- Develop scenarios, alert message templates, and message dissemination user group(s) sets that pertain to the region.
- Verify currency and accuracy of user group(s) sets, including key personnel from Region staff on a periodic but at least quarterly basis.
- Verify the currency and accuracy of WAAN guidance on a semiannual basis, which can be coordinated with the Region Emergency Management Working Group.
- Ensure the ROC is on distribution for all non-administrative messages.
- Conduct and document quarterly tests of WAAN systems.

6.4.3 ROC Battle Watch Captain (BWC)

The ROC BWC shall:

- Be responsible for the timely/accurate release of all messages by the Battle Watch Team.
- Obtain guidance to address emergent scenarios not covered by existing guidance.
- Perform primary administrator and message publisher duties and responsibilities.
- Ensure static groups, group sets, and custom attributes are update monthly.
- Train key installation personnel on system capability and use.

6.4.4 ROC Battle Watch Standers

The ROC Battle Watch Standers shall:

- Be responsible for the publishing and releasing of all WAAN messages for the region not already completed by the WAAN.
- Inform the BWC when WAAN messages are published/launched.
- Monitor published alerts.

6.4.5 Regional Dispatch Center

The RDC shall:

- Be responsible for the publishing and releasing WAAN messages as directed and in accordance with policy/SOPs.
- Ensure the ROC is on distribution for all WAAN messages.

6.4.6 Information Technology Officer (N6)

The Region IT Officer shall:

- Ensure hardware and software upgrades are incorporated in the WAAN in a timely manner.
- Ensure a priority response to system hardware or software malfunctions.
- Coordinate with the N36 (where applicable) and N37 to schedule system tests and maintenance and ensure those actions are completed, as required.
- Assign administrator and/or publisher privileges to appropriate personnel, including watch standers.
- Coordinate with CNIC N6 on Tier 1 and 2 help desk efforts.

6.4.7 Region Force Protection/Security Officer

The Region Force Protection/Security Officer shall:

- Provide alert messages and group(s) sets to the ROC BWC for all force protection/security scenarios.
- Develop scenarios, alert messages, and user group(s) sets that pertain to force protection/security at the regional level.

6.4.8 Installation Commanding Officer (ICO)

The ICO (or designee) shall have overall responsibility of the operation of the WAAN program at the installation level, including the following:

- Message release authority
- Delegation of message release authority to ensure timely alert dissemination under all circumstances
- Approval authority for administrative rights granted to tenants/users
- Assignment of primary administrator and publisher privileges to the appropriate personnel, including watch standers
- Provide the final approval authority over WAAN use scenarios, alert messages, groups, protocols, and procedures throughout the region.

6.4.9 Installation Command Duty Officer

The CDO shall be trained and prepared to rapidly publish alert messages in accordance with guidance from the ICO (or designee).

6.4.10 Installation Emergency Management Officer

The EMO shall:

- Perform administrator and/or publisher duties, as required.
- Provide alert message templates and dissemination group(s) sets to the EOC for all EM scenarios.
- Develop scenarios, alert message templates, and message dissemination user group(s) sets that pertain to the installation.
- Collaboratively develop WAAN SOPs with all potential WAAN users.
- Verify currency and accuracy of user group(s) sets, including key personnel from local tenant commands on a quarterly basis.
- Verify the currency and accuracy of WAAN guidance on a semiannual basis, which can be coordinated with the installation Emergency Management Working Group.
- Ensure the ROC is on distribution for all non-administrative messages.
- Conduct and document periodic but at least quarterly tests of WAAN systems.

6.4.11 Installation Force Protection/Security Officer

The Force Protection/Security Officer shall:

- Perform publisher duties, as required.
- Coordinate with the EMO to develop scenarios, alert messages, and user group(s) sets that pertain to force protection/ security at the installation level.

7.0 IMPACT CONSIDERATIONS

This paragraph describes:

- Anticipated operational and organizational sustainment issues
- Mitigation for risks associated with the issues
- Impacts to existing operations and organizations

While each of the alerting systems provides a significant functional contribution to portions of the alerting process, documentation available to date has not specified how the three independent alerting systems that are now being piloted and fielded will become an interoperating family of systems that satisfy the functional requirements. Eight interrelated areas are identified below where further efforts toward understanding user functional requirements, systems analysis, and systems design are needed to produce a sustainable WAAN.

7.1 SPEED

Speed is the most critical attribute of a WAAN. As described in current documentation, the three systems now being piloted and fielded are independent. This separation has a negative impact on speed when two or more systems are needed to attain the necessary alert distribution coverage

and meet time requirements for notification of personnel. Users will expect to control all three systems from a single web client application.

7.2 RELIABILITY

Reliability is a critical attribute of any component or system within a WAAN. The 90% A_o specification cited for each of the three pilot systems is far below expectations and the A_o target for such systems in the civil sector. MTBCF specifications were similarly below the industry norm. Alerting saves lives.

Navy Emergency Managers expect, and the Navy Family deserves, WAAN reliability on par with civil sector counterparts such as the Federal Emergency Management Agency's IPAWS (www.fema.gov/emergency/ipaws/) and NWS's HazCollect system (www.nws.noaa.gov/os/hazcollect/).

The existence of all three systems currently being piloted and fielded on an installation would help mitigate risk of incomplete coverage on the installation should one system be unavailable. However, ATNS is the only system that would be available to contact Category 2 personnel living off installation OCONUS. Its target A_o should be in line with expectations in the U.S. civil sector.

7.3 RESILIENCE

WAANs must be able to withstand external forces from the very threats and hazards for which they are to provide warning. Single-server configurations are single-point-of-failure configurations with respect to disasters. WAAN architectures and operational requirements should include multiple servers, geographically segregated servers, and servers networked by robust communications. The multiple servers should be load-balanced for resilience to load surge, have uninterrupted power supply, and be capable of rapid fail-over in the event of loss of any server.

7.4 INTEROPERABILITY

While each of the previously stated references recognizes the interoperability requirement, there is little to describe how WAAN interoperability will be accomplished or to what extent it will be accomplished. Accomplishing interoperability among fielded systems is always far more costly than analyzing, designing, and implementing interoperability architecture prior to system deployment. Often, after-the-fact interoperability is created with custom point-to-point interfaces between individual systems. As systems are added to a family of systems by the custom point-to-point method, the number of interfaces to be maintained grows exponentially. A change to any system on any side of such interface corrupts the interface, creating additional maintenance costs.

At a minimum, interoperability among these three systems to support the structure alert and distribute alert steps of the alerting process should be professionally analyzed and designed. As currently documented, individuals would have to structure an alert in each system and then disseminate the alert via each of the three systems. This is an inefficient, ineffective, and

unacceptable process for a function citing speed as its primary design principle. End users expect a WAAN to have a single alert authoring tool with the capability to rapidly select one or more modes of alert distribution. The impact of deploying three independent alerting systems will likely be user rejection and disuse. A common services architecture employing nonproprietary API, web service, and message standards could satisfy the most basic aspects of interoperability. The extent of interoperability should not consider only threat inputs as described in the alerting process, but future operations planning for interoperability with computer-aided dispatch systems, Incident Management Systems, and the C4I Suite.

7.5 FLEXIBILITY

Three independent systems provide some flexibility regarding the means and modes of alert distribution. Without an interoperability infrastructure employing common services and a controlling web application for the WAAN, there is little, if any, flexibility to add and effectively use additional threat feeds or alert dissemination mechanisms. An effort by professional IT interoperability architects, analysts, and designers is necessary to plan the data-sharing infrastructure necessary to efficiently and effectively support the entire alerting process. That effort should consider use of existing GOTS products such as the Disaster Management Open Platform for Emergency Networks (www.usgovxml.com/DataService.aspx?ds=DMOPEN) or commercial products such as the Cisco Open Platform for Safety and Security (www.athoc.com/news/release_Cisco.aspx) as a cost-saving approach to the technical solution.

7.6 SUPPORT

A clearer understanding and definition of WAAN users is necessary to formulate efficient and effective training and post-training assistance support. Definition of the user base and understanding of the complexity of the controlling WAAN web application will be necessary to formulate support policy. Issues for consideration include the following:

- What are the roles that will be responsible for receiving and assessing threats, structuring alerts, and disseminating alerts?
- Are they Battle Watch staff at the Shore Support Center and ROCs?
- Are they dispatch personnel?
- Are they Command Duty Office personnel at installation level?

7.7 MAINTENANCE

System maintenance must be structured to keep system A_o at the maximum achievable. A network operations center should be monitoring all aspects of the WAAN with network and system performance diagnostic tools capable of immediate alerting of any failure and, when possible, warning of potential failure. Levels 1, 2, and 3 network and systems support should be available 24/7 for an alerting system designed to protect the Navy Family.

7.8 SECURITY

The objective of a WAAN is to warn a population at risk in the shortest time possible. A careful analysis of security requirements is necessary to design and implement security mechanisms that control access where necessary without slowing execution of the alerting process. Holistic application of security policies and processes to the entire WAAN may not be desirable once security requirements are fully identified and analyzed.

Appendix A. ACRONYMS

A _o	operational availability
AOR	area of responsibility
API	automated program interface
ATFP	antiterrorism/force protection
ATNS	Automatic Telephone Notification System
BCWS	base control workstation
BWC	Battle Watch Captain
C2	Command and Control
C3	command, control, and communications
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CAD	Computer Aided Dispatch
CAP	Common Alerting Protocol
CBC	Construction Battalion Center
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive
CDNS	Computer Desktop Notification System
CDO	Command Duty Officer
CNIC	Commander, Navy Installations Command
CNRSE	Commander, Navy Region Southeast
CO	Commanding Officer
CONUS	in the continental United States
COTS	commercial off-the-shelf
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISR	DOD IT Standards Registry
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DODAF	Department of Defense Architectural Framework
EM	emergency management
EMO	Emergency Management Officer
EOC	Emergency Operations Center
FPCON	force protection condition
GIS	geographical information system
GOTS	government off-the-shelf
GV	Giant Voice
IBS	Integrated Base Station
ICO	Installation Commanding Officer
INFOCON	information operations condition
IPAWS	Integrated Public Alert and Warning System
IT	information technology
IV	Indoor Voice
LRU	line-replaceable unit
METOC	meteorological and oceanographic
MTBCF	mean time between critical failure

NAS JAX	Naval Air Station Jacksonville
NFPA	National Fire Protection Association
NMCI	Navy Marine Corps Internet
NMET	Navy mission-essential task
NOAA	National Oceanographic and Atmospheric Administration
NRSE	Navy Region Southeast
NWS	National Weather Service
OCONUS	outside the 48 continental United States
OPNAV	Office of the Chief of Naval Operations
PKI	Public Key Infrastructure
RDC	Regional Dispatch Center
ROC	Regional Operations Center
RSS	Rich Site Summary
SOP	standard operating procedure
TCP/IP	transmission control protocol/Internet protocol
TDD	Telecommunications Devices for the Deaf
THC	Transitional Hosting Center
TTY	Telephone typewriter
UFC	Unified Facilities Criteria
WAAN	Wide Area Alert and Notification
XML	Extensible Markup Language
XO	Executive Officer