DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) 19 January 2018

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Desktop Alert, Inc. Total Alert, Net-Centric Alerting System (NCAS) Release 5.2

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements (UCR) 2013 Change 2," 14 September 2017
(c) through (d), see Enclosure 1

1. **Certification Authority.** Reference (a) establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority (CA) for Department of Defense Information Network (DoDIN) products, Reference (b).

2. **Conditions of Certification.** The Desktop Alert, Inc. Total Alert, Net-Centric Alerting System (NCAS) Release 5.2, hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements, Reference (b), and is certified for joint use as an NCAS with the conditions described in Table 1. The SUT, the Federal Emergency Management Agency Integrated Public Alert and Warning System, and another NCAS vendor product demonstrated Common Alerting Protocol version 1.2 inter-enclave interoperability. This certification expires upon changes that affect interoperability, but no later than the expiration date specified in the DoDIN Approved Products List (APL) memorandum.

Table 1. Conditions

Description		Operational Impact	Remarks
UCR Waivers			
None.			
Conditions of Fielding			
None.			
TDR#	**Open Test Discrepancies**		
002	The SUT is unable to block select subscriber and groups from a pre-built notification scenario.	Minor	See note 1.
003	The SUT does not support all of the required data types, such as Boolean, string, date-time, and numeric.	Minor	See note 1.
004	Recurring alerts are not always sent at the Configured/Set Time.	Minor	See note 1.

Table 1. Conditions (continued)

Description		Operational Impact	Remarks
TDR#	**Open Test Discrepancies (continued)**		
005	The SUT cannot perform alerts based upon filtering User Attributes.	Minor	See note 1.
006	The SUT does not support Attributes with names over 20 characters.	Minor	See note 1.
009	The SUT does not have the ability to dial DSN directory numbers or support a Telephony Application Programming Interface to support interface to voice systems.	Minor	See notes 1 and 2.
010	Automated callback response phone number not supported.	Minor	See note 1.
011	The SUT does not support a dial in number to trigger a pre-configured alert.	Minor	See note 1.

NOTES:
1. DISA accepted the vendors POA&M and adjudicated this discrepancy as minor.
2. DISA has adjudicated this discrepancy as having a minor operational impact and stated the intent to change this requirement to optional in the next version of the UCR.

LEGEND:

DISA	Defense Information Systems Agency	POA&M	Plan of Action and Milestones
DSN	Defense Switched Network	TDR	Test Discrepancy Report
SUT	System Under Test	UCR	Unified Capabilities Requirements

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status, and Table 3 provides the Capability Requirements and Functional Requirements status. Table 4 provides a DoDIN APL product summary.

Table 2. NCAS Interface Status

Interface	Status	Remarks (See note 1.)
Network Interfaces (See note 2.)		
10BaseT (C)	Not Tested	The IEEE 802.3i interface was not tested and is therefore not certified.
100BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u Ethernet interface.
1000BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab Ethernet interface.
1000BaseX (C)	Not Tested	The IEEE 802.3z interface was not tested and is therefore not certified.
10GBaseX (C)	Not Tested	This IEEE 802.3ae interface was not tested and is therefore not certified.
Network Management Interfaces (See note 3.)		
10BaseT (C)	Not Tested	The IEEE 802.3i interface was not tested and is therefore not certified.
100BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u Ethernet interface.
1000BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab Ethernet interface.
1000BaseX (C)	Not Tested	The IEEE 802.3z interface was not tested and is therefore not certified.
10GBaseX (C)	Not Tested	This IEEE 802.3ae interface was not tested and is therefore not certified.

NOTES:
1. Table 3 depicts the SUT high-level requirements.
2. If the NCAS is a self-contained hardware/software solution, the SUT must minimally support one of the following IEEE Network interfaces: 802.3i, 802.3z, 802.3ab, and any additional IEEE 802.3 interfaces may be provided as optional interfaces.
3. The NCAS shall support an Ethernet physical interface to the DISA VVoIP EMS meeting one of the following specifications: 10 Mbps IAW IEEE 802.3i, 10 Mbps IAW IEEE 802.3j, 100 Mbps IAW IEEE 802.3u, 1000 Mbps IAW IEEE 802.3z, 1000 Mbps IAW IEEE 802.3ab, and 10 Gbps IAW IEEE 802.3ae.

LEGEND:

C	Conditional	IEEE	Institute of Electrical and Electronics Engineers
CR	Capability Requirements	IP	Internet Protocol
DISA	Defense Information Systems Agency	Mbps	Megabits per second
EMS	Electronic Message System	NCAS	Net-Centric Alerting System
FR	Functional Requirements	SUT	System Under Test
Gbps	Gigabits per second	VVoIP	Voice and Video over IP
IAW	In accordance with		

Table 3. NCAS Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (See note 1.)	UCR 2013 Change 2	Status
1	Interfaces (C)	3.10.1	Met
2	NCAS Management Requirements (R)	3.10.2	Partially Met (See note 2.)
3	NCAS Alerting Requirements (R)	3.10.3	Partially Met (See note 2.)
4	NCAS Interaction Requirements (R)	3.10.4	Met
5	IPv6 Requirements (R)	3.10.5	Met
6	CS Requirements (R)	3.10.6	Met (See note 3.)
7	Reliability Requirements (R)	3.10.7	Met

NOTES:
1. The annotation of 'required' refers to a high-level requirement category.
2. The SUT met the requirements with the exceptions noted in Table 1.
3. JITC-led CS test teams accomplished security testing and the results are published in a separate report, Reference (d).

LEGEND:

C	Conditional	IPv6	Internet Protocol version 6
CR	Capability Requirements	JITC	Joint Interoperability Test Command
CS	Cybersecurity	NCAS	Net-Centric Alerting System
FR	Functional Requirements	R	Required
ID	Identification	UCR	Unified Capabilities Requirements

Table 4. DoDIN APL Product Summary

Product Identification			
Product Name	Desktop Alert, Inc. Total Alert		
Software Release	5.2		
DoDIN Product Type(s)	NCAS		
Product Description	The NCASs allow effective regional and enterprise wide alerting, tracking, and reporting capabilities. The NCASs are used to disseminate and track delivery and responses from personnel via personal devices, such as PC, tablets, and mobile devices via popup alerts, voice phone calls, text messages or SMS, messages to mobile applications, and e-mails. The NCASs are used to activate, via its interfaces, audible and visual alerting to MNSs, such as indoor and outdoor alerting, fire alarms, and LMRs. The NCASs are intended to support MNS systems on DoD installations as described in UFC 4-010-0.		
Product Components	**Component Name**	**Version**	**Remarks**
Server	Dell Server Power Edge R530	Windows Server 2016, Microsoft IIS 10.0.14393.0, Microsoft NET Framework 4.0.30319, VMware vSphere Virtual	See note.
Base Software	Desktop Alert Total Alert Server license	Release 5.2	
500 Subscriber License	Extended 500 Seat License	Release 5.2	
MNS interface	IIM	Release 5.2	

NOTE: The SUT is a software product, although it was tested with a specific hardware platform, the vendor does not provide hardware. The vendor does provide guidelines for hardware scaling which covers the range of likely implementations.

LEGEND:

APL	Approved Products List	NCAS	Net-Centric Alerting System
DoD	Department of Defense	PC	Personal Computer
DoDIN	Department of Defense Information Network	SMS	Short Message Service
IIM	Internet Protocol Integration Module	SUT	System Under Test
LMR	Land Mobile Radio	UFC	Unified Facilities Criteria
MNS	Mass Notification System		

4. **Test Details.** This certification is based on interoperability testing, the Defense Information Systems Agency (DISA) adjudication of open test discrepancy reports (TDRs), review of the vendor's Letters of Compliance (LoC), and DISA CA Recommendation for inclusion on the DoDIN APL. Review of the vendor LoC was completed on 4 September 2017. Interoperability testing was conducted from 28 August through 15 September 2017 at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona. DISA completed the initial adjudication

of outstanding TDRs on 23 October 2017; however, final release could not be issued until the vendor completed testing, which was completed on 22 December 2017 via WebEx and included a validation of the required fail-over capability of the SUT, using test procedures derived from Reference (c). JITC-led Cybersecurity (CS) test teams conducted CS testing and published the results in a separate report, Reference (d). Enclosure 2 provides the interoperability test results, which describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified Internet Protocol Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Industry Toolkit (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Cybersecurity Assessment Package that contains the approved configuration and deployment guide must be requested directly from the Approved Products Certification Office (APCO), e-mail: disa.meade.ie.list.approved-products-certification-office@mail.mil. All associated information is available on the DISA APCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. **Point of Contact (POC).** The JITC POC is Mr. Joseph Schulte; Commercial telephone (520) 538-5100; DSN telephone 879-5100; FAX DSN 879-4347; E-mail address joseph.t.schulte.civ@mail.mil; Mailing address: Joint Interoperability Test Command, ATTN: JTE (Joseph Schulte), P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The APCO tracking number for the SUT is 1716702.

FOR THE COMMANDER:

CLARK.BRADLEY.ALAN.1231466564 Digitally signed by CLARK.BRADLEY.ALAN.1231466564 Date: 2018.01.19 10:21:29 -07'00'

3 Enclosures a/s

for RIC HARRISON
Chief
Networks/Communications & DoDIN
Capabilities Division

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD (AT&L)
ISG Secretariat, DISA, JT
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA (ALT), SAIS-IOQ
US Air Force, SAF/CIO A6XA
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
DISA/ISG REP
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS PEO T&IVV
HQUSAISEC, AMSEL-IE-IS
APCO

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command, "Net-Centric Alerting System (NCAS) Test Procedures Version 1.0 for Unified Capabilities Requirements (UCR) 2013 Change 2," July 2017

(d) Joint Interoperability Test Command, "Cybersecurity Assessment Report for Desktop Alert Total Alert 7.x (Tracking Number 1716702)," October 2017

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Desktop Alert, Inc. Total Alert, Net-Centric Alerting System (NCAS), Release 5.2 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT's identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	Department of Army
Sponsor Point of Contact	Matthew Cassidy, mtthew.j.cassidy.civ@mail.mil
Vendor Point of Contact	John Monville, john@desktopalert.net
System Name	Total Alert, Version 5.2
Increment and/or Version	Version 5.2
Product Category	Net-Centric Alerting System
System Background	
Previous certifications	None
Tracking	
APCO ID	1716702
System Tracking Program ID	STP #6347, Test Activity #15745
Requirements Source	
UCR	UCR 2013, Change 2 Section 3.10 and 5
Remarks	None
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND:	
APCO ID Approved Products Certification Office Identification	UCR Unified Capabilities Requirements

2. SYSTEM DESCRIPTION. The NCASs allow effective regional and enterprise wide alerting, tracking, and reporting capabilities. The NCASs are used to disseminate and track delivery and responses from personnel via personal devices, such as personal computer, tablets, and mobile devices via popup alerts, voice phone calls, text messages or short message service (SMS), messages to mobile applications, and e-mails. The NCASs are used to activate, via its interfaces, audible and visual alerting to Mass Notification Systems (MNSs), such as indoor and outdoor alerting, fire alarms, and Land Mobile Radios. The NCASs are intended to support MNS systems on Department of Defense (DoD) installations as described in Unified Facilities Criteria (UFC) 4-010-0.

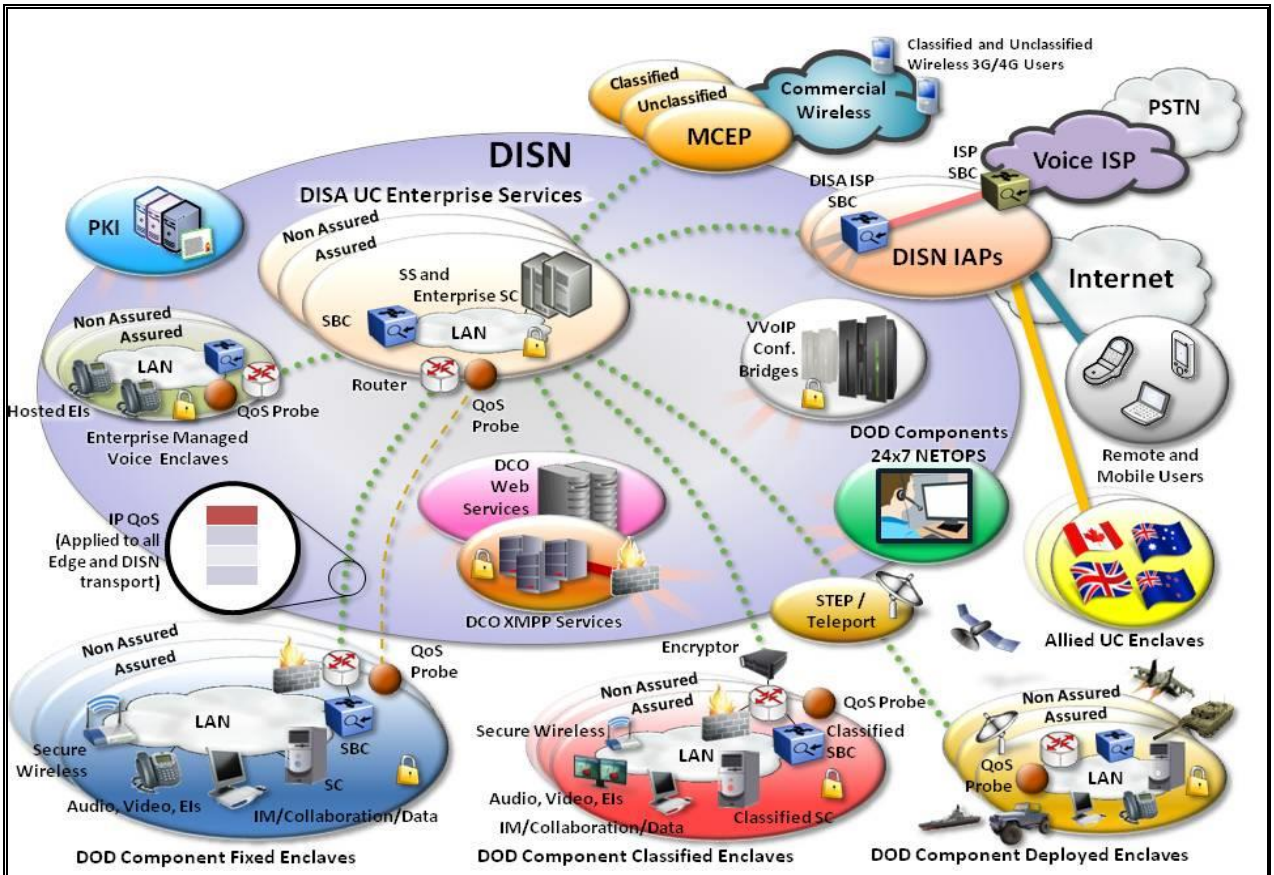
The SUT is a software product that provides a Web-Facing interface for Subscriber Management, Alert Generation, Alert Response Logging, and Alert Dissemination. The SUT depends on server hardware, Operating System, external Structured Query Language (SQL) Database software, Cloud-Based resources for E-Mail, SMS, and Integrated Public Alert and Warning System (IPAWS) alert sharing. The SUT also makes use of an external Active Directory structure that aids in Subscriber Creation and credentialing for access to network resources. The SUT leverages standard network Required Ancillary Equipment, such as Domain Name Service and Network Time Protocol servers, for name resolution and time. Lastly, the software runs on a hardware platform, which is typically scaled for the number of supported subscribers.

For the purpose of the test, an MNS was provided by the vendor to validate the ability to generate output for Big Voice, Signage, and systems via serial interface to key them (i.e., alarm system, radio system etc.). The MNS used Hyper Text Transfer Protocol Secure (HTTPS) protocol messaging between the NCAS and the MNS to transmit audible, serial information.

3. OPERATIONAL ARCHITECTURE. The Unified Capabilities (UC) architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The DoD Chief Information Officer and Joint Staff policy and subscriber mission requirements determine which type of switch allowable at a particular location. The DoD Information Network (DoDIN) architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational DoDIN architecture in which the SUT may be used.

4. TEST CONFIGURATION. The test team tested the SUT at the Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona, in a manner and configuration similar to that of a notional operational environment. Figure 2-2 depicts the notional connectivity, interfaces, systems, and components for the NCAS solutions. Figure 2-3 depicts the SUT test architecture.

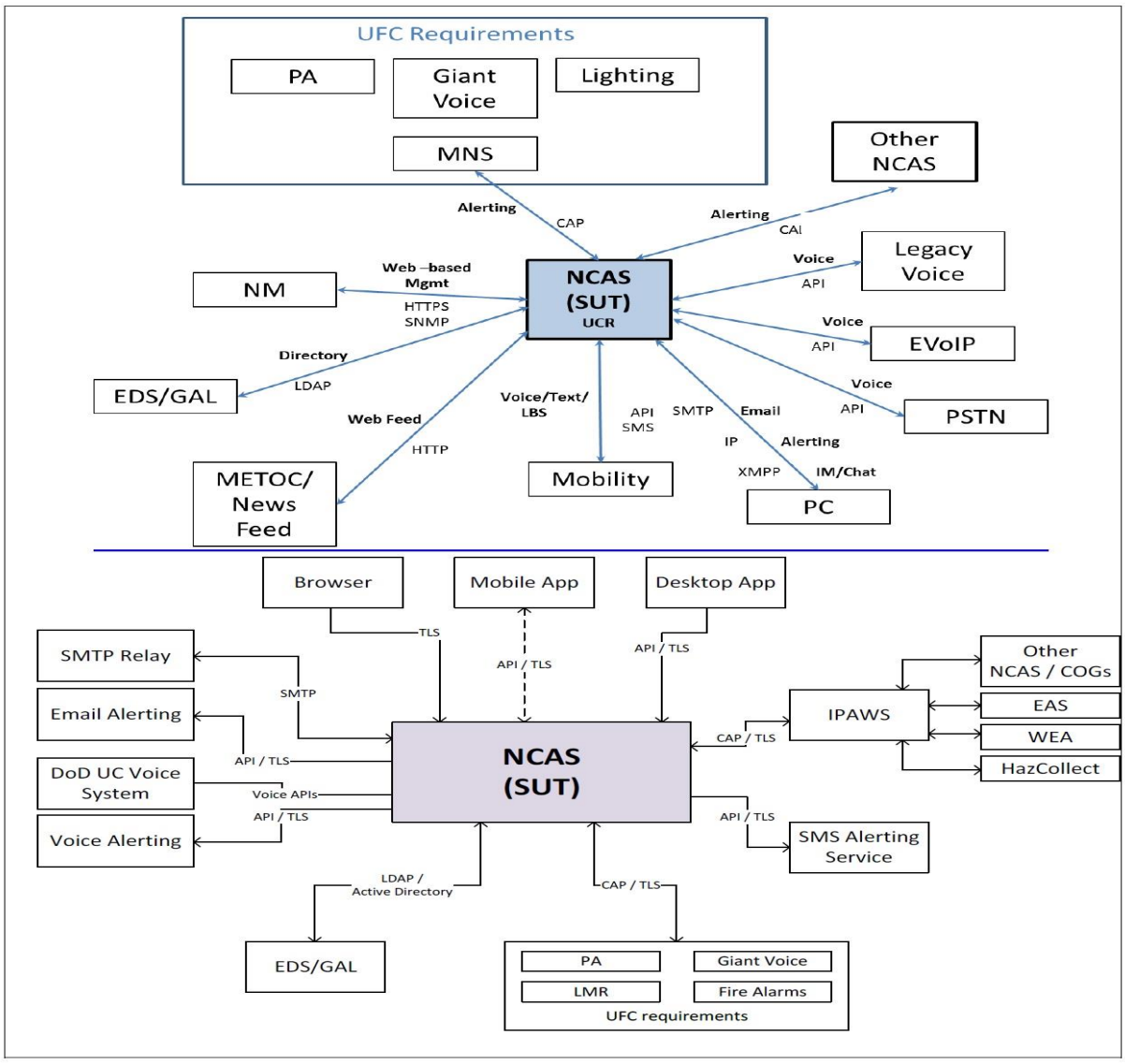
5. METHODOLOGY. Testing was conducted using the NCAS requirements derived from the Unified Capabilities Requirements (UCR) 2013, Change 2, Reference (b), and the NCAS test procedures, Reference (c). Any test discrepancies were documented in test discrepancy reports (TDRs). The vendor submitted a Plan of Action and Milestones (PoA&M) as required for the TDRs. The Defense Information Systems Agency (DISA) reviewed the POA&M and adjudicated the TDRs as minor. Any new discrepancies noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor POA&M, which will address all new critical TDRs within 120 days of identification.



LEGEND:

Conf.	Conference		
DCO	Defense Connection Online	NETOPS	Network Operations
DISA	Defense Information Systems Agency	PKI	Public Key Infrastructure
DISN	Defense Information Systems Network	PSTN	Public Switched Telephone Network
DoD	Department of Defense	QoS	Quality of Service
DoDIN	DoD Information Network	SBC	Session Border Controller
EI	End Instrument	SC	Session Controller
IAP	Internet Access Point	SS	Softswitch
IM	Instant Message	STEP	Standardized Tactical Entry Point
IP	Internet Protocol	UC	Unified Capabilities
ISP	Internet Service Provider	VVoIP	Voice and Video over IP
LAN	Local Area Network	XMPP	Extensible Messaging and Presence Protocol
MCEP	Multi-Carrier Entry Point		

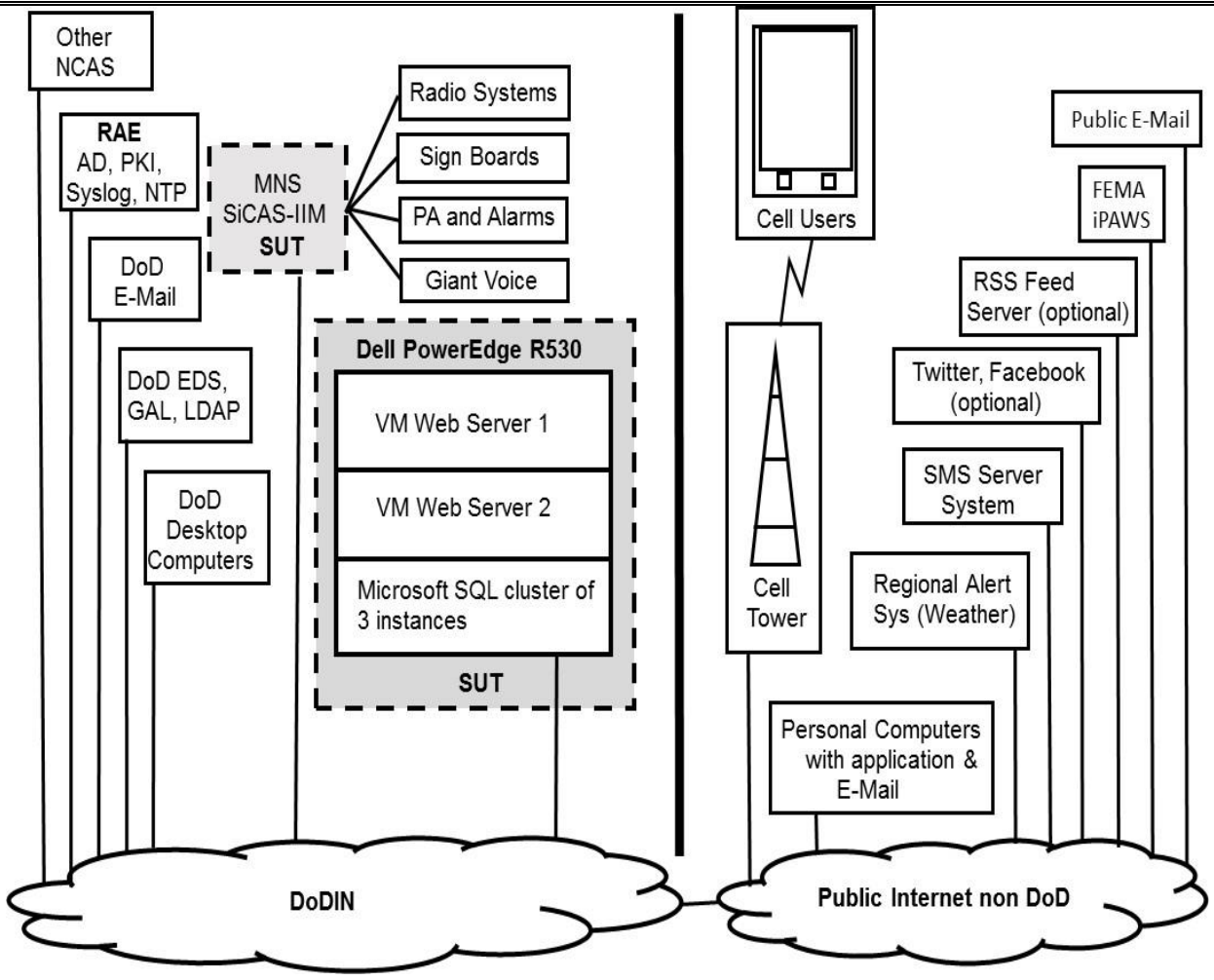
Figure 2-1. Notional DoDIN Network Architecture



LEGEND:

API	Application Programming Interface	Mgmt	Management
App	Application	MNS	Mass Notification System
CAP	Common Alerting Protocol	NCAS	Net-Centric Alerting System
COG	Collaborative Operating Group	NM	Network Management
DoD	Department of Defense	PA	Personal Agent
EAS	Emergency Alert System	PC	Personal Computer
EDS	Enterprise Directory Services	PSTN	Public Switched Telephone Network
EVoIP	Enterprise Voice over IP	SMS	Short Message Service
GAL	Global Access List	SMTP	Simple Mail Transfer Protocol
HTTP	Hyper Text Transfer Protocol	SNMP	Simple Network Management Protocol
HTTPS	Hyper Text Transfer Protocol Secure	SUT	System under Test
IM	Instant Messaging	TLS	Transport Layer Security
IP	Internet Protocol	UC	Unified Capabilities
IPAWS	Integrated Public Alert and Warning System	UCR	Unified Capabilities Requirements
LBS	Location-Based Services	UFC	Unified Facilities Criteria
LDAP	Lightweight Directory Access Protocol	WEA	Wireless Emergency Alerts
LMR	Land Mobile Radios	XMPP	Extensible Messaging and Presence Protocol
METOC	Meteorological and Oceanographic		

Figure 2-2. Notional Connectivity, Interfaces, Systems, and Components for NCAS Solutions



LEGEND:

AD	Active Directory	NTP	Network Time Protocol
DoD	Department of Defense	PA	Public Address
DoDIN	DoD Information Network	PKI	Public Key Infrastructure
EDS	Enterprise Directory Services	RAE	Required Ancillary Equipment
FEMA	Federal Emergency Management Agency	RSS	Rich Site Summary
GAL	Global Access List	SMS	Short Message Service
IIM	Internet Protocol Integration Module	SQL	Structured Query Language used by Database
iPAWS	Integrated Public Alert and Warning System	SUT	System under Test
LDAP	Lightweight Directory Access Protocol	Sys	System
MNS	Mass Notification System	Syslog	System Log
NCAS	Network Centric Alerting System	VM	Virtual Machine

Figure 2-3. SUT Test Architecture

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. UCR 2013 Change 2, Sections 3.10 and 5 define the NCAS interfaces, Capability Requirements (CRs), Functional Requirements (FRs), Cybersecurity (CS), and other requirements. Table 3-1 provides the JITC SUT testing interface status and Table 3-2 provides the CRs and FRs status. The following sub-paragraphs provide testing details and results.

a. **The UCR 2013 Change 2, section 3.10 includes the Net-Centric Alerting System (NCAS) requirements.** Section 3.10 outlines the NCAS product requirements. The paragraphs below specify the requirements.

(1) **Interfaces.** Section 3.10.1 provides the following conditional Interface requirements for the NCAS.

(a) If the NCAS is a self-contained hardware/software solution, the NCAS solution must minimally support one of the following interfaces: 802.3z, 802.3ab, additional Institute of Electrical and Electronics Engineers (IEEE) 802.3 interfaces may be provided as optional interfaces. The SUT met this requirement with testing and the vendor's Letters of Compliance (LoC).

(b) If the NCAS is a self-contained hardware/software solution, the NCAS must support network management interfaces in accordance with (IAW) Section 2.7.4 and meet the following: SCM-001830 interface rates (required) and SCM-001850 Virtual Local Area Network (VLAN) support (conditional). The SUT met this requirement with testing and the vendor's LoC.

(2) **NCAS Management Requirements.** Section 3.10.2 outlines the management functions and capabilities the NCAS solution (the integrated hardware/software – self-contained or hosted) must support, unless explicitly specified.

(a) **NCAS Fault, Configuration, Accounting, Performance, and Security (FCAPS) Requirements.** Section 3.10.2.1 states if the NCAS is a self-contained hardware/software solution, the NCAS must support network management requirements IAW the following Section 2.19 requirements: SCM-009190 (.a through .c), SCM-009230, SCM-009240, SCM-009250, SCM-009260, SCM-009270, and SCM-009280. The SUT met this conditional requirement with the vendor's LoC. Also, security testing was met by the JITC-led CS test teams and the results are published in a separate report, Reference (d)

(b) **NCAS Management Capabilities.** Section 3.10.2.2 includes the Management Capability Requirements of the NCAS. The SUT met all these requirements with testing and the vendor's LoC with exceptions noted below.

1. The NCAS solution shall support enterprise wide organizations in an effective manner using a central NCAS installation with a multi-tenant capability – supporting distributed organizations by logically segmenting and isolating tenants, each assigned with resources, and capable of managing their own users and alerting. The SUT met this requirement with testing.

2. Access to the NCAS functions, assets, and resources are governed by the permissions assigned to each administrator. Resources assigned to administrators shall include subscribers, such that administrators shall be granted access and targeting privilege to all or a subset of the subscribers. The SUT met this requirement with testing.

3. The NCAS shall be capable of assigning permissions on a group-wide role basis, such that each member of a particular group receives identical permission to the NCAS functions, assets, and resources. The SUT met this requirement with testing.

4. The NCAS shall support assigning administrator's access to one or more tenants, while assigning different roles and permissions to functions, assets and resources for each tenant. The SUT met this requirement with testing.

5. The NCAS shall support complete access and visibility from the Command level into all subordinate units/locations of the system to view alert activity. The SUT met this requirement with testing via Groups.

6. The NCAS shall provide supervision and a monitoring capability of its connected components and delivery systems, and provide administrators with notification of a failure of a component or delivery system within 200 seconds of the occurrence of the failure. The SUT met this requirement with the vendor's LoC.

7. The NCAS administrators authorized to perform group management tasks shall be able to create groups, assign individual subscribers to new or existing groups, assign groups of subscribers to new or existing groups, remove subscribers and groups from existing groups, and delete groups without deleting the subscribers and groups composing the deleted group. The SUT met this requirement with testing and the vendor's LoC.

8. The NCAS administrators authorized to perform group management tasks shall be able to define static subscriber groups composed of a selected list of subscribers ("roster") that may include nested static groups. The SUT met this requirement with testing.

9. The NCAS administrators authorized to perform group management tasks shall be able to define dynamic subscriber groups composed of lists of subscribers based on data queries on their database attributes. The SUT met this requirement with testing with the following exception: The SUT cannot perform alerts based upon filtering User Attributes. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

10. The NCAS system shall be able to support at least three mandatory delivery methods (i.e., SMS, phone call, e-mail, etc.) to be used when alerting an individual subscriber or a group. The SUT met this requirement with testing.

11. The NCAS administrators having the requisite authorization shall be able to generate predefined alert notification scenarios for subscribers and groups. These scenarios include the content of the alert, at least one response option for the subscriber to choose from and target subscribers/audiences, mass communication mediums, organizations and preferred and

mandatory personal delivery devices to be used when alerting the target subscriber(s) and/or group(s). The SUT met this requirement with testing.

12. The NCAS administrators having the requisite authorization shall be able to manually activate predefined alert scenarios to trigger alert notifications. The administrator shall be able to specify the timing of the alert (i.e., immediate, prescheduled, etc.). The administrator shall be able to update any part of the predefined alert scenario, such as alert message, alert response options, targeted audience, used devices, etc. The SUT met this requirement with testing with the following exception: Recurring Alerts are not always sent at the Configured/Set Time. If the alert is configured prior to the set alert time, it recurs appropriately based on the alert time set. However, if the alert is configured after the set alert time, it will not recur on the set time but rather at the time the alert was created. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

13. The NCAS administrators having the requisite authorization shall be able to create and activate alerts in real-time for the system's designated subscribers. When an administrator creates an alert, they designate the target subscribers and/or groups, mass communication medium, organizations, and the contents and timing (e.g., immediately, at a certain time, etc.) of the alert message. The SUT met this requirement with testing.

14. The NCAS administrators having the requisite authorization shall be able to target subscribers for alert notification based on organizational structure, distribution lists, physical location over a Geographical Information System (GIS) map or by specifying zone code(s) or location name(s), or identifiable information captured from DoD global directory services. The SUT met this requirement with testing and the vendor's LoC.

15. The NCAS administrators having the requisite authorization shall be able to block or remove subscribers or groups from a pre-built alert notification scenario or from a pending alert notification. Blocking subscribers shall explicitly prevent an alert from being sent to specified subscribers, even if they are part of a targeted group. The SUT met this requirement with testing and the vendor's LoC with the following exception: The SUT is unable to block select subscribers and groups from a pre-built notification scenario. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

16. The NCAS administrators having the requisite authorization shall be able to schedule activation of recurring and real-time test alerts. The SUT met this requirement with testing with the following exception: Recurring Alerts are not always sent at the Configured/Set Time. If the alert is configured prior to the set alert time, it recurs appropriately based on the alert time set. However, if the alert is configured after the set alert time, it will not recur on the set time but rather at the time the alert was created. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor

17. The NCAS system administrators having the requisite authorization shall have the capability to track and generate reports such as: Delivery of alerts and Subscriber response(s) to alerts. The SUT met this requirement with testing.

18. For any given alert, administrators having the requisite authorization shall be able to retrieve and display the count of targeted recipients, the actual number of recipients, the number of recipients who acknowledged receipt of the alert, and the number of recipients who respond to a specific response option (if option was requested). The SUT met this requirement with testing.

19. For any given alert, administrators having the requisite authorization shall be able to retrieve and display the count of targeted recipients and view the coverage of existing contact details per the selected notification devices against the count of targeted recipients prior to activating the alert. The SUT met this requirement with testing.

20. For non-hosted, self-contained solutions, administrators shall have the ability to access and manage the system via client-server interface (i.e., thick client). The SUT met this requirement with testing.

21. For hosted solutions, administrators shall have the ability to access and manage the system via open source web based interface. The SUT met this requirement with testing.

22. Access shall only be granted using DoD issued Common Access Card (CAC). The SUT met this requirement with testing.

23. Administrator session shall timeout after a configurable period of inactivity and the administrator shall establish a new web-based session with the NCAS Web server. The SUT met this requirement with testing.

24. The NCAS administrators having the requisite authorization shall be able to add subscriber attribute fields of any of the following data types: string, numeric, date-time, Boolean, single pick-list of values, multi pick-list of values, and memo. Such addition shall not require SQL access or knowledge, or vendor assistance. The SUT met this requirement with testing with the following exception: The SUT does not support all of the required data types, such as Boolean, string, date-time, and numeric. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

25. The NCAS administrators having the requisite authorization shall be able to add three communication mediums at a minimum. The SUT met this requirement with testing.

26. The NCAS administrators having the requisite authorization shall be able to manually add subscribers to the database, update the contact information, for a given subscriber and other attributes of a subscriber record, and remove subscribers from the NCAS database. The SUT met this requirement with testing and the vendor's LoC.

27. The NCAS administrators having the requisite authorization shall be able to import user data from flat text files, such as Comma-Separated-Values (CSV). The SUT met this requirement with the vendor's LoC.

28. The NCAS administrators having the requisite authorization shall be able to export user data to flat text files, such as CSV; administrators shall be able to specify what subset of users and user attributes to export. The SUT met this requirement with the vendor's LoC.

(c) **Web-Management Capabilities.** Section 3.10.2.3 includes the Web-Management Capabilities.

1. The NCAS shall have a web-based administrator interface to publish and track alerts and perform administrative tasks including, but not limited to, the management of subscribers, delivery devices, and pre-built alert scenarios. The SUT met this requirement with the vendor's LoC.

2. The administrator's web-based interface shall be role and permission based, and only those capabilities allowed by the authorization will be available. The SUT met this requirement with testing.

3. The web-based administrator interface shall work on personal computers and servers running DoD-approved operating systems and on all DoD-approved Web browsers. The SUT met this requirement with testing.

4. The web-based session between the browser and the NCAS Web server shall be secured using Secure Hypertext Transfer Protocol (HTTP). The NCAS is required to provide provisions for secure authentication using DoD and industry-standard technologies. The SUT met this requirement with testing.

(d) **NCAS Database**. Section 3.10.2.4 includes the following requirements.

1. The database and the NCAS solution shall minimally provide services and features described for up to 250,000 subscribers. The SUT met this requirement with documentation describing scaling of the system for 250,000 subscribers and the vendor's LoC.

2. The NCAS shall minimally provide the following subscribe attribute fields: Name, Title, Grade/Rank, Organization Title, Sub-organization/Unit Title, Organization Address Street, Organization State, Organization Zone Improvement Plan (ZIP), E-mail Address, Work Phone Number, DoD Mobile Phone Number, Home Phone Number, Personal Mobile Number, Building Number, Cubicle/Office Number, Supervisor Name, Service, Government/Service/Contractor Affiliation, Last Known Location (Latitude/Longitude), and Last Known Location date-time stamp. The SUT met this requirement with testing with the following exception: The SUT does not support Attributes with names over 20 characters. Any of the required Attribute fields, which have over 20 characters in their name, are truncated at the 20th character. The following required fields are truncated: Sub-organization/Unit Title, Organization Address Street, DoD Mobile Phone Number, Personal Mobile Number, Cubicle/Office Number, Government/Service/Contractor Affiliation, Last Known Location (Latitude/Longitude), and Last Known Location date-time stamp. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

(e) **Subscriber Access**. Section 3.10.2.5 states subscribers shall not be allowed direct access to the NCAS system. Access shall be granted to only authorized administrators. Subscribers' information shall be populated using the DoD's global directory. The SUT met this requirement with the vendor's LoC.

(3) **NCAS Alerting Requirements.** Section 3.10.3 provides the NCAS Alerting Requirements. The paragraphs below specify the requirements.

(a) **General Alerting Requirements.** Section 3.10.3.1 includes the following requirements.

1. The NCAS shall be capable of sending alert messages to target recipients according to: Hierarchical organizational structure (as would be imported from an Lightweight Directory Access Protocol (LDAP) or Active Directory), Organizational roles, Specific distribution lists (e.g., hazardous materials (HAZMAT) response teams), Dynamic groups created through on-the-fly queries of the user directory, Geographical locations (e.g., entire bases, zones within bases), Rule –based criteria based on subscriber attribute information, and Computer name (required for targeting devices where Internet Protocol (IP) addresses are dynamically assigned). The SUT met this requirement with the vendor's LoC.

2. The NCAS shall centrally track and store all alerting activities for each individual recipient, including sending, receiving, and responding to alerts, and be able to generate reports based on tracked information. The SUT met this requirement with testing.

3. The NCAS shall be able to incorporate a pre-defined library of alerts and messages appropriate to: Force Protection Conditions, Terrorism threats, watches, or warnings, Evacuation routes, Battle staff directives, Personnel recall requirements, Federal, DoD, or installation-specific warning and notification requirements, and Weather warnings and watches. The SUT met this requirement with testing.

4. The NCAS shall offer unfettered flexibility to place target subscribers into groups that can then be targeted for specified alerts. The types of groups that can be created include, but are not limited to, groups based on organization, rank, roles and responsibilities, location, device delivery preference, and phone number. In addition, the groups can be static ("rosters") or dynamic (based on subscriber data attributes). The SUT met this requirement with testing with the following exception: The SUT cannot perform alerts based upon filtering User Attributes. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

5. The NCAS shall be Section 508 compliant. The SUT met this requirement with the vendor's LoC.

6. The NCAS shall be capable of delivering installation-wide alert notification to all targeted personnel within a threshold of 10 minutes but with an objective notification time of 2 minutes. The SUT met this requirement with the vendor's LoC.

7. The NCAS shall be capable of designating severity and type for every alert message. The SUT fully met this requirement. The SUT is compliant with the Common Alerting Protocol (CAP) version (v) 1.2 protocol.

8. The NCAS shall be capable of attaching the following to an alert message: Geographic region(s) and marker(s) and Link. The SUT met this requirement with testing.

9. The NCAS shall minimally support the following user responses of alert acknowledgement or selection from response options defined for the activated alert. Alert responses are available via - Desktop notification, E-mail response, Self-Service end-user acknowledgement, Text (SMS) response, Phone keypad response, and Mobile application response. The SUT met this requirement with testing.

(b) **Desktop Alerting Requirements.** Section 3.10.3.2 includes the following Conditional requirements.

1. When an alert occurs, which is intended for the subscriber, then the client software shall provide an audio alert accompanied by a persistent visual display of the alert message on the computer until the alert is acknowledged or canceled; no user action will be required to receive desktop notifications. The SUT met this conditional requirement with testing.

2. If a subscriber logs into the computer after one or more alerts have been sent and are still active, then the client software shall provide an audio alert accompanied by a persistent visual display of the currently active alert message(s) on the computer until the subscriber responds to the alert(s). The SUT met this conditional requirement with testing.

3. When the client software displays an alert on the computer, the subscriber shall be presented with at least one response option enabling the subscriber to respond to the alert. When the subscriber responds, the client software shall transmit the subscriber response to the NCAS server. The NCAS server stores the subscriber response, and the subscriber response is accessible to authorized operators and administrators. The SUT met this conditional requirement with testing.

4. If the connection between the NCAS client and NCAS server is secured using Secure HTTP, the NCAS server is required to authenticate itself to the client using its server certificate. The subscriber shall authenticate to the NCAS server using a DoD issued CAC. The SUT met this conditional requirement with testing.

(c) **Phone Alerting Requirements**. Section 3.10.3.3 includes the following requirements.

1. The NCAS shall provide alerting capability to both DoD worldwide numbering plan and commercial public switched telephone numbers using either:

a. An internal voice alerting subsystem or service capable of providing voice messages to DoD and commercial numbers. The SUT met this requirement with testing.

b. A Telephony Application Programming Interface (TAPI) and/or an Extensible Markup Language IP interface to DoD voice systems (Session Controllers and End-Offices) that support voice alerting to DoD and commercial telephone numbers. The SUT did not meet this requirement. The SUT does not have the ability to dial Defense Switched Network (DSN) directory numbers. DISA adjudicated this discrepancy as a change requirement with the intent to make requirement optional. The SUT does not support a TAPI for voice systems. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

2. The voice alerting capabilities shall minimally include:

a. An Audio messaging dissemination to subscribers, as defined in the activated alert. The SUT met this requirement with testing. The SUT does not support a TAPI for voice systems. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

b. An Interactive Voice Response (IVR) support that enables users to listen and respond to prerecorded messages. The SUT met this requirement with testing.

3. The voice alerting interactions shall minimally include:

a. Capability to detect when the call has been deferred to voicemail and to leave an audio message in response. Upon completion of the audio message, the system shall have the ability to disconnect the call. The SUT met this requirement with testing.

b. Capability to report telephone numbers that were successfully answered, unanswered, or when a voicemail was left. The SUT met this requirement with testing.

c. Capability to reattempt to alert those numbers not successfully reached. The number of reattempts shall be configurable between 1 and 5. The SUT met this requirement with testing.

d. Capability to accept call-backs from subscribers, to replay the voice message and accept a response option from the calling subscriber. The SUT met this requirement with testing.

e. Capability to limit playing the voice message to a subscriber who enters a personal PIN to identity call recipient. The SUT met this requirement with testing.

4. If initiating an alert via an in-bound phone call from a recognized number, then the NCAS shall allow initiation of alert with an operator authorization code. The SUT did not meet this conditional requirement. DISA accepted the vendor's POA&M and adjudicated this discrepancy as minor.

5. When using the internal voice alerting service capability, the NCAS shall ensure the internal voice alerting service blocks phone numbers (masking or deleting) and contact details. The SUT met this requirement with testing.

6. The voice alerting capability shall support the ability to reduce concurrent call volume to defined prefixes to prevent flooding of DoD or commercial phone systems. The SUT met this requirement with the vendor's LoC.

(d) **Mobile Client Alerting Requirements.** Section 3.10.3.4 includes the following requirements.

1. The NCAS shall furnish warning notification applications for mobile devices commonly used by subscribers (e.g., warning notification apps for iOS, Android, Microsoft). The SUT met this requirement with testing.

2. Mobile applications shall be evaluated and approved by the DoD application vetting environment. This is an external requirement. Mobile client applications were evaluated for only a limited number of Mobile Device types (i.e., Android, Windows). Testing was performed to determine only if the SUT was capable of generating messages to and responses from mobile devices. This certification does not include the certification of the respective Mobile Application. Certification of Unified Capability Mobile applications are accomplished under a separate product category through the DISA Mobility Program Manager.

3. The mobile applications shall provide audio and visual warning notifications to the user of the mobile device. The SUT met this requirement with testing.

4. The mobile applications shall allow users to select a response option that will be recorded by the NCAS. The SUT met this requirement with testing.

5. If the DoD issued mobile device has the embedded Global Positioning System capability enabled, then the mobile application may use device location (subject to all applicable privacy rules) to perform real-time, location-based alert targeting, and tag user alert responses with real-time location information. The SUT met this conditional requirement with testing.

6. If the mobile application supports delivery of geographical location(s), markers, and multi-media (image, video) as part of the alert message, then it may incorporate these capabilities into the alert message. The SUT met this conditional requirement with testing.

7. The NCAS shall be capable of interfacing with SMS aggregation services for the following purposes, which the SUT met with testing:

a. Sending text message alerts to a set of target subscribers.

b. Obtaining reports of event alert delivery and obtaining subscriber responses to text alerts (selecting one of multiple response options).

c. Obtaining reports of the operational status for the SMS aggregation service.

8. The connection between the NCAS and the DoD SMS aggregation service shall be secured using Secure HTTP. The SUT met this requirement with testing.

9. In order to instruct the SMS aggregation service to send text alerts, the NCAS shall provide the minimum set of data items necessary including user names and SMS addresses (e.g., mobile phone numbers). The SUT met this requirement with testing.

10. Within 1 minute, the NCAS shall be capable of sending an SMS message to 5,000 subscribers. The SUT met this requirement with the vendor's LoC.

(e) **E-Mail Alerting Requirements**. Section 3.10.3.5 includes the following requirements.

1. The NCAS shall provide e-mail alerting capability to both DoD e-mails and to commercial e-mail addresses using a Simple Mail Transfer Protocol component that sends outbound e-mail alerts to DoD host .mil e-mail servers to relay e-mails to target subscribers. The SUT met this requirement with testing.

2. The NCAS e-mail alerting capability shall support the following, which the SUT met with testing and the vendor's LoC:

a. Sending Public Key Infrastructure (PKI)-signed e-mail alerts.

b. Receiving incoming e-mail responses (selecting one of multiple response options) from subscribers.

c. Sending e-mail alerts to subscribers must be in plain text only.

3. The NCAS shall support:

a. Tracking and reporting of e-mail alert delivery events including reporting of subscriber responses.

b. Reporting on the operational status of the NCAS e-mail alerting capability.

4. The NCAS e-mail capability shall authenticate with the DoD e-mail server using DoD PKI certificates before sending outbound alert messages. The SUT met this requirement with testing and the vendor's LoC.

5. The DoD e-mail server shall authenticate to the NCAS server before the NCAS server will accept inbound messages from the DoD e-mail server. The SUT met this requirement with testing and the vendor's LoC

(4) **NCAS Interaction Requirements**. Section 3.10.4 includes the following requirements.

(a) **Other NCAS Interaction Requirements using Common Alerting Protocol (CAP)**. Section 3.10.4.1 states the NCAS shall support the CAP as defined in the Organization for the Advancement of Structured Information Standards (OASIS) Version 1.2 standard for

exchanging alerts with other systems, via either middleware capability, such as Federal Emergency Management Agency (FEMA) IPAWS, or Direct HTTPS posting between the systems, as agreed to between the vendors and system owners. The SUT met this requirement with testing and the vendor's LoC.

(b) **MNS interaction requirements.** Section 3.10.4.2 includes the following requirements, which were met by the SUT with testing and the vendor's LoC.

1. The NCAS shall be capable of sending alerts to FEMA IPAWS. The NCAS shall support the CAP v1.2 IPAWS Profile Version 1.0.

2. The NCAS shall be able to collect alerting tracking data and subscriber responses from an external MNS.

3. The NCAS shall interface with a media gateway to support legacy non-IP delivery systems (i.e., non-IP Giant Voice systems, public address systems, and non-IP land mobile radio systems) located at DoD installations.

4. The NCAS shall interact with the non-IP delivery systems via means of the media gateway for the following purposes: Sending alerts, Canceling alerts, Reporting on alert delivery status, and Reporting on the status of the non-IP delivery system.

(c) **Enterprise Directory Services (EDS)/ Global Access List (GAL) interaction Requirements.** Section 3.10.4.3 includes the following requirements.

1. The NCAS shall support one-way synchronization of its users' data and meta-data from DoD EDS and Global Directory Services using DoD recommended encryption. The SUT met this requirement with testing and the vendor's LoC.

2. The frequency with which the NCAS synchronizes its database with other relevant existing DoD databases shall be configurable. The NCAS must support a minimum synchronization frequency of one-hour. The SUT met this requirement with the vendor's LoC.

3. The NCAS synchronization with LDAP / Active Directory shall support the following capabilities: a. Creation of subscribers. b. Removal or disablement of subscribers. c. Update of subscriber attributes including contact details. d. Update of the NCAS organizational hierarchy based on LDAP / Active Directory Organizational Unit structure. e. Import of select Distribution Lists and Security Groups to create and update the NCAS groups. The SUT met this requirement with testing and the vendor's LoC.

(d) **External Event Sources System Interaction Requirements.** Section 3.10.4.5 states the NCAS shall be capable of monitoring emergency notifications from multiple data sources (such as National Weather Service, Emergency Managers Weather Information Network, Meteorology and Oceanography, and others) and automatically sending out notifications to designated groups or subscribers. The SUT met this requirement with testing and the vendor's LoC.

(5) **IPv6 Requirements**. Section 3.10.5 states the NCAS shall meet the IPv6 requirements for Network Appliances and Simple Servers (NA/SS) as defined in Section 5. The SUT met this requirement with the vendor's LoC.

(6) **Cybersecurity Requirements**. Section 3.10.6 was met by the JITC-led CS test teams and the results are published in a separate report, Reference (d).

(7) **Reliability Requirements.** Section 3.10.7 includes the following requirements.

(a) The NCAS shall support multiple server configurations to achieve a "hot standby" failover configuration (i.e., no down time in case of failure in a single server) as well as to support higher load scenarios (e.g., more users). The SUT met this requirement with testing, documentation, and the vendor's LoC.

(b) The NCAS shall provide a high availability service having a complete set of redundant primary and standby platforms, and this redundant configuration shall have an availability of 99.95 percent (including scheduled maintenance). The SUT met this requirement with testing, documentation, and the vendor's LoC.

(c) The NCAS disaster recovery configuration shall use online database replication between the primary and standby NCAS platform to achieve Recovery Point objective (RPO) of up to 5 minutes. The SUT makes use of Database Clustering, which has inherent recovery and synchronization features. The SUT met this requirement with WebEx demonstration and the vendor's LoC.

(d) The standby NCAS platform shall fully provide the level of service and capacity as the primary NCAS, and will connect to same event sources and delivery devices of the primary NCAS platform. The SUT met this requirement with testing, documentation, and the vendor's LoC.

7. HARDWARE/SOFTWARE/FIRMWARE VERSION IDENTIFICATION. Table 3-3 provides the SUT components' hardware, software, and firmware tested. JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

8. TESTING LIMITATIONS. The JITC test team noted the following testing limitation: Actual connection to the GAL database was not available; however, user importation and creation of subscribers was tested in a simulated environment with Active Directory users. There is no operational impact.

9. CONCLUSIONS. The SUT meets the critical interoperability requirements for an NCAS product in accordance with the UCR and is certified for joint use with other NCAS products listed on the Approved Products List.

DATA TABLES

Table 3-1. Interface Status

Interface	Status	Remarks (See note 1.)
Network Interfaces (See note 2.)		
10BaseT (C)	Not Tested	The IEEE 802.3i interface was not tested and is therefore not certified.
100BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u Ethernet interface.
1000BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab Ethernet interface.
1000BaseX (C)	Not Tested	The IEEE 802.3z interface was not tested and is therefore not certified.
10GBaseX (C)	Not Tested	This IEEE 802.3ae interface was not tested and is therefore not certified.
Network Management Interfaces (See note 3.)		
10BaseT (C)	Not Tested	The IEEE 802.3i interface was not tested and is therefore not certified.
100BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3u Ethernet interface.
1000BaseT (C)	Met	The SUT met the critical CRs and FRs for the IEEE 802.3ab Ethernet interface.
1000BaseX (C)	Not Tested	The IEEE 802.3z interface was not tested and is therefore not certified.
10GBaseX (C)	Not Tested	This IEEE 802.3ae interface was not tested and is therefore not certified.

NOTES:
1. Table 3-2 depicts the SUT high-level requirements.
2. If the NCAS is a self-contained hardware/software solution, the SUT must minimally support one of the following IEEE Network interfaces: 802.3i, 802.3z, 802.3ab, and any additional IEEE 802.3 interfaces may be provided as optional interfaces.
3. The NCAS shall support an Ethernet physical interface to the DISA VVoIP EMS meeting one of the following specifications: 10 Mbps IAW IEEE 802.3i, 10 Mbps IAW IEEE 802.3j, 100 Mbps IAW IEEE 802.3u, 1000 Mbps IAW IEEE 802.3z, 1000 Mbps IAW IEEE 802.3ab, and 10 Gbps IAW IEEE 802.3ae.

LEGEND:

C	Conditional	IEEE	Institute of Electrical and Electronics Engineers
CR	Capability Requirements	IP	Internet Protocol
DISA	Defense Information Systems Agency	Mbps	Megabits per second
EMS	Electronic Message System	NCAS	Net-Centric Alerting System
FR	Functional Requirements	SUT	System Under Test
Gbps	Gigabits per second	VVoIP	Voice and Video over IP
IAW	In accordance with		

Table 3-2. NCAS Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (See note 1.)	UCR 2013 Change 2	Status
1	Interfaces (C)	3.10.1	Met
2	NCAS Management Requirements (R)	3.10.2	Partially Met (See note 2.)
3	NCAS Alerting Requirements (R)	3.10.3	Partially Met (See note 2.)
4	NCAS Interaction Requirements (R)	3.10.4	Met
5	IPv6 Requirements (R)	3.10.5	Met
6	CS Requirements (R)	3.10.6	Met (See note 3.)
7	Reliability Requirements (R)	3.10.7	Met

NOTE(S):
1. The annotation of 'required' refers to a high-level requirement category.
2. The SUT met the requirements with the exceptions noted in Table 1.
3. JITC-led CS test teams accomplished security testing and the results are published in a separate report, Reference (d).

LEGEND:

C	Conditional	IPv6	Internet Protocol version 6
CR	Capability Requirements	JITC	Joint Interoperability Test Command
CS	Cybersecurity	NCAS	Net-Centric Alerting System
FR	Functional Requirements	R	Required
ID	Identification	UCR	Unified Capabilities Requirements

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Product Identification			
Product Name	Desktop Alert, Inc. Total Alert		
Software Release	5.2		
DoDIN Product Type(s)	NCAS		
Product Description	The NCASs allow effective regional and enterprise wide alerting, tracking and reporting capabilities. The NCASs are used to disseminate and track delivery and responses from personnel via personal devices, such as PC, tablets, and mobile devices via popup alerts, voice phone calls, text messages or SMS, messages to mobile applications, and e-mails. The NCASs are used to activate, via its interfaces, audible and visual alerting to MNSs, such as indoor and outdoor alerting, fire alarms and LMRs. The NCASs are intended to support MNS systems on DoD installations as described in UFC 4-010-0.		
Product Components	**Component Name**	**Version**	**Remarks**
Server	Dell Server Power Edge R530	Windows Server 2016, Microsoft IIS 10.0.14393.0, Microsoft, NET Framework 4.0.30319, VMware vSphere Virtual	See note.
Base Software	Desktop Alert Total Alert Server license	Release 5.2	
500 Subscriber License	Extended 500 Seat License	Release 5.2	
MNS interface	IIM	Release 5.2	

NOTE: The SUT is a software product, although it was tested with a specific hardware platform, the vendor does not provide hardware. The vendor does provide guidelines for hardware scaling which covers the range of likely implementations.

LEGEND:

APL	Approved Products List	NCAS	Net-Centric Alerting System
DoD	Department of Defense	PC	Personal Computer
DoDIN	Department of Defense Information Network	SMS	short message service
IIM	Internet Protocol Integration Module	SUT	System Under Test
LMR	Land Mobile Radios	UFC	Unified Facilities Criteria
MNS	Mass Notification System		

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

Required Ancillary Equipment		
Active Directory		
Public Key Infrastructure		
SysLog Server		
Terminal Access Controller Access Control System Plus		
System Name	**Software Release**	**Function**
Test Network Components		
Desktop Alert	5.2.	NCAS
Android mobile phone (See note.)	6.0	Non-MMD commercial Phone
Desktop Alert mobile phone (See note.)	Windows 10 OS	Non-MMD commercial Phone
Dell Laptop	Windows 10	Desktop alert Client

NOTE: Mobile client applications were only evaluated for a limited number of Mobile Device types (i.e., Android, Desktop Alert). The testing was only performed to determine if the SUT was capable of generating messages to and responses from mobile devices. This certification does not include the certification of the respective Mobile Application. Certification of Unified Capability Mobile applications are accomplished under a separate product category through the DISA Mobility PM.

LEGEND:

DISA	Defense Information Systems Agency	PM	Program Manager
MMD	Multimedia Mobile Device	SUT	System Under Test
NCAS	Net-Centric Alerting System	SysLog	System Log
OS	Operating System		