SPAWAR

Systems Center
PACIFIC

Technical Report 2003
July 2011

Wide Area Recovery & Resiliency Program (WARRP) Transition Manager Series

Coalition Warrior Interoperability Demonstration (CWID) 2011

SSC Pacific Civilian Message Systems in Trial 2.32

Francis Cortez
Douglas Hardy

Approved for public release; distribution is unlimited.

SSC Pacific
San Diego, CA 92152-5001

Technical Report 2003
July 2011

Wide Area Recovery & Resiliency Program (WARRP) Transition Manager Series Coalition Warrior Interoperability Demonstration (CWID) 2011

SSC Pacific Civilian Message Systems in Trial 2.32

Francis Cortez
Douglas Hardy

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

J.J. Beel, CAPT, USN **Commanding Officer**	**C. A. Keeney** **Executive Director**

ADMINISTRATIVE INFORMATION

This report was prepared for the U.S. Department of Homeland Security Science and Technology Directorate by the C2 Interoperability & Information Systems Branch (Code 53627) of the C2 Technology & Experimentation Division (Code 536), SSC Pacific.

Released by
Douglas Hardey, Head
5225 53627 Branch

Under authority of
Thomas Tiernan, Head
522 536 Division

ACKNOWLEDGMENTS

William Ginley, Donald Macfarlane and David Drummond provided outstanding overall direction and coordination in integrating our efforts with the overall Trial 2.32 efforts.

David Lamensdorf provided excellent support with Integrated Chemical, Biological, Radiological, Nuclear and Explosive (ICBRNE) sensors and equipment.

Francis Cortez, Son Nguyen, Paul Lee, Ritesh Patel, Bruce Plutchak, Henry Dong, Jeff Waters, Peggy West, Warren Tran, Bonnie Ferri, James Eitelberg, Jack Houghton, Christine Barton, Les Anderson and Doug Hardy provided the Space and Naval Warfare Systems Center Pacific (SSC) Pacific support for Trial 2.32 at the Coalition Warrior Interoperability Demonstration (CWID) 2011 exercise from June 6 - 16, 2011.

Francis Cortez led our efforts in Herndon, VA, while Son Nguyen and Paul Lee led the local Space and Naval Warfare Systems Center (SSC) efforts. The team demonstrated the following capabilities to distinguished visitors at the CWID sites: ICBRNE interface to Open Platform for Emergency Networks (OPEN) chemical, biological and radiological detection support to first responders, chemical and radiological sensors, sensor information to handheld device applications, and social media networks for improved communications and situational awareness. The leads also set up the hardware and software, and provided training to operators and other trainers.

SSC engineers Bruce Plutchak and Henry Dong led the development and testing of an interface between ICBRNE and the Federal Emergency Management Agency (FEMA) Integrated Public Alerting and Warning System (IPAWS) OPEN software application. Their success was shared with other organizations both government and contractors to aid in developing information sharing interfaces and became the first successful verification testing of the OPEN 2.0 production version.

SSC engineers Ritesh Patel, James Eitelberg and Francis Cortez worked on developing applications to run on Apple’s iPhone Operating System (IOS) and Android operating systems, and included messaging to Facebook and Twitter. Social media networking has become and is becoming an important and critical source of data and notification mechanism in emergency response and recovery operations.

SSC engineers Son Nguyen, Paul Lee, Jack Houghton, Jeff Waters and Christine Barton provided a related experiment involving the Integrated Checkpoint Dashboard, an information sharing and situational awareness tool, being prototyped for airport checkpoints. Barton and her team provided information exchange support to this effort from the Integrated Checkpoint Project (ICP) that supports the Transportation Security Administration and Transportation Security Lab.

SSC support staff, Peggy West, Bonnie Ferri and Warren Tran, were instrumental in all of the details of coordination, planning and executing. They acquired materials and equipment on short notice, and shipped and tracked equipment to the various locations for testing and operations.

SSC engineers Les Anderson and Doug Hardy assisted Edgewood Chemical and Biological Center (ECBC) engineer, Bill Ginley, with transitioning CWID Trial 2.32 demonstrated technology component called the Remote Message Center (RMC) to the Joint Warning and Reporting Network (JWARN) program, and continue to assess other components for transition.

CONTENTS

INTRODUCTION

CWID

Coalition Warrior Interoperability Demonstration (CWID) is a Chairman of the Joint Chiefs of Staff-directed annual event that engages cutting-edge information technology, focusing on operational shortfalls identified by combatant commanders and government agencies. Technologies are approved for participation because they address a new information sharing capability or potentially improve an existing capability. The demonstrations, which take place in various locations worldwide, focus on technology discovery, risk reduction and coalition interoperability.

CWID 2011 TRIAL 2.32

Trial 2.32 supported CWID Objective 2 to enhance the whole of government integration and interoperability, in order to improve cyber-operations, and support sustainable secure mission partner collaboration. Trial 2.32 was led by William Ginley and an engineering team from the Edgewood Chemical and Biological Center (ECBC) in support of Chris Russell from the Department of Homeland Security (DHS) Science and Technology (S&T) Office.

Trial 2.32 dealt with Managing Military Civilian Messaging (M2CM). M2CM is a system of systems approach to address the need for rapid information sharing between military and civilian emergency management communities. M2CM employs a mix of program of record, commercial and S&T applications/tools to provide end-to-end communications. Figure 1 depicts a system overview of Trial 2.32.

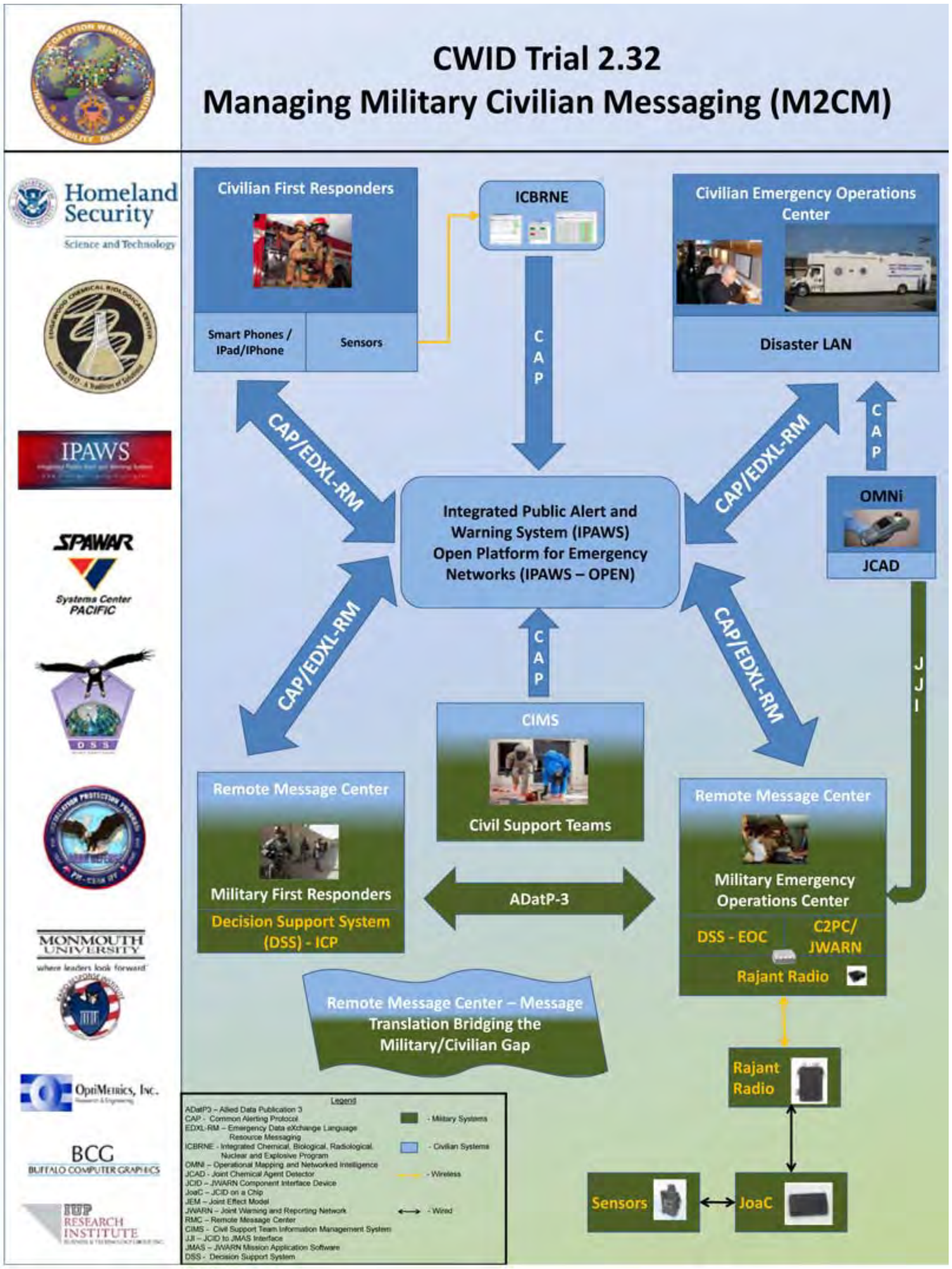
CWID Trial 2.32
Managing Military Civilian Messaging (M2CM)
Homeland Security
Science and Technology
IPAWS
SPAWAR
Systems Center PACIFIC
DSS
MONMOUTH UNIVERSITY
where leaders look forward
OptiMetrics, Inc.
BCG
BUFFALO COMPUTER GRAPHICS
IUP RESEARCH INSTITUTE
Civilian First Responders
Smart Phones / IPad/IPhone
Sensors
ICBRNE
CAP
Civilian Emergency Operations Center
Disaster LAN
CAP
OMNi
JCAD
CAP/EDXL-RM
CAP/EDXL-RM
Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (IPAWS – OPEN)
CAP/EDXL-RM
CAP/EDXL-RM
CAP
JJI
CIMS
Civil Support Teams
Remote Message Center
Military First Responders
Decision Support System (DSS) - ICP
ADatP-3
Remote Message Center
Military Emergency Operations Center
DSS - EOC
C2PC/ JWARN
Rajant Radio
Remote Message Center – Message Translation Bridging the Military/Civilian Gap
Rajant Radio
Sensors
JoaC
Legend
ADatP3 – Allied Data Publication 3
CAP - Common Alerting Protocol
EDXL-RM – Emergency Data eXchange Language Resource Messaging
ICBRNE - Integrated Chemical, Biological, Radiological, Nuclear and Explosive Program
OMNI – Operational Mapping and Networked Intelligence
JCAD - Joint Chemical Agent Detector
JCID – JWARN Component Interface Device
JoaC – JCID on a Chip
JEM – Joint Effect Model
JWARN – Joint Warning and Reporting Network
RMC – Remote Message Center
CIMS - Civil Support Team Information Management System
JJI – JCID to JMAS Interface
JMAS – JWARN Mission Application Software
DSS - Decision Support System
🟩 - Military Systems
🟦 - Civilian Systems
- Wireless
⟷ - Wired

Figure 1. System Overview of Trial 2.32.

SSC PACIFIC CIVILIAN MESSAGING SYSTEMS IN TRIAL 2.32

The Space and Naval Warfare Systems Center, Pacific (SSC Pacific) team supported the CWID 2011 Trial 2.32 M2CM at SSC Pacific and at the DHS Battle Lab, Joint Mobile Command Center (“The Truck”) in Herndon, VA. The SSC Pacific team supported ECBC in executing Trial 2.32 on the East Coast and expanded the trial to include information sharing and related experiments on the West Coast at SSC Pacific. Trial 2.32 was focused on providing information sharing of chemical, biological and radiological data across civilian emergency operation centers and military incident command posts (ICPs).

SSC Pacific’s main contributions were in modifying existing civilian messaging systems such as:

- Using integrated chemical, biological, radiological, nuclear and explosives (ICBRNE) tools and technologies to supplement the civilian emergency operation centers (EOC) systems.
- Developing an interface between ICBRNE and the Integrated Public Alerting and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN) 2.0.
- Sharing and collaborating with other OPEN interface developers.
- Testing the first working interface for OPEN 2.0 on the production system.
- Demonstrating real chemical and radiological sensors sending messages to OPEN.
- Providing the ability to inject a standard common alerting protocol (CAP) compliant biological sensor message to OPEN.
- Developing “apps” for both, an Apple IOS (IPAD) tablet and Android (Galaxy) tablet to display the common operating picture (COP).
- Providing social media connectivity via Facebook and Twitter.

SSC Pacific supported message sharing between the civilian EOC and the military ICPs. Civilian EOCs issued CAP messages via IPAWS-OPEN, while military ICPs sent messages via the Joint Warning and Reporting Network (JWARN) and the Remote Message Center (RMC) to OPEN.

SYSTEM SETUP

SSC Pacific team supported two exercise locations, one at the DHS Battle Lab and the Joint Mobile Command and Training Center (the “Truck”, see figure 2) in Herndon, VA ,and one at SSC Pacific, at Building 99, in San Diego, CA.

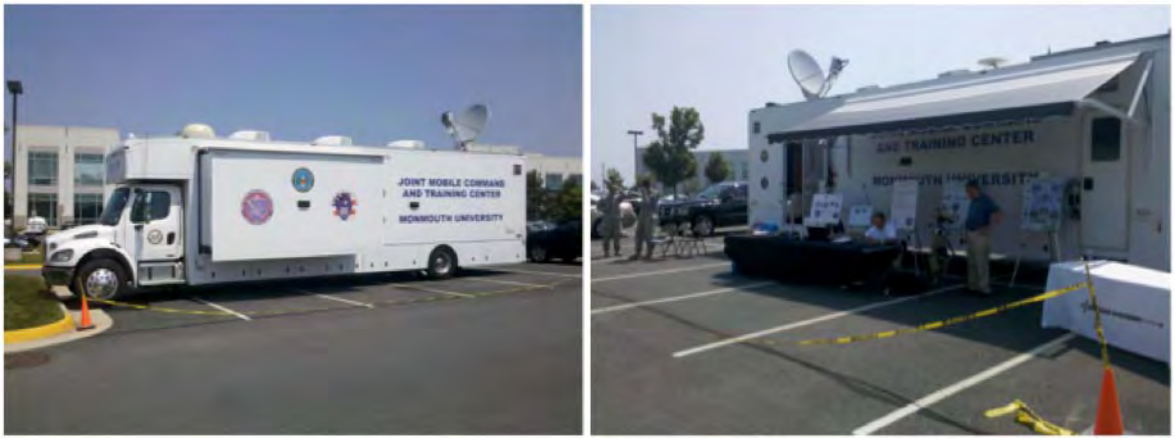

Figure 2. Left: The "Truck" in Herndon, VA, with DHS Battle Lab in distance. Right: Demonstrations setup inside and outside.

SSC Pacific’s participation in the M2CM trial involved similar setups of hardware and software at both the Herndon and San Diego sites.

HARDWARE

- **First Responder Sensors:** Three types of sensors were used, a ppbRAE Plus chemical detector, a MultiRAE Plus gas detector, and an identiFINDER radiation detector.

- **Sensor Wi-Fi Dongles:** Safe Environment Engineering Wi-Fi dongles were attached to the sensors to allow data to be sent from the sensors to the sensor laptop.
- **Sensor Laptop:** One laptop interfaced with the sensors, displaying live readings and posting the readings to the ICBRNE server.
- **OPEN Posting Laptop:** One laptop checked for alarms coming from the ICBRNE server and posted to IPAWS OPEN 2.0, Twitter and Facebook.
- **Handheld tablets:** Two tablets displayed sensor readings and maps: an Apple iPad and a Samsung Galaxy Tab.
- **Mobile Wi-Fi Hotspot:** A 3G AT&T MiFi integrated the sensors, laptops and handheld tablets, and provided internet access.

SOFTWARE

- **Sensor Monitoring:** ppbRAE, MultiRAE, and identiFINDER software displayed sensor information on the laptop, including sensor readings and global positioning system (GPS) locations. This software also posted alerts to the ICBRNE server if sensor thresholds were exceeded.
- **ICBRNE Polling/IPAWS OPEN 2.0 Posting:** This software checked the ICBRNE server periodically for new alerts. If an alert was found it was posted to IPAWS OPEN 2.0. Furthermore, alerts were posted to Facebook and Twitter.
- **ICBRNE Web App:** The ICBRNE web app displays live sensor readings and map positions, and could be accessed with the laptops and tablets.

SYSTEM DIAGRAM

Figure 3 shows the integrated system diagram for SSC Pacific’s civilian messaging participation using ICBRNE.

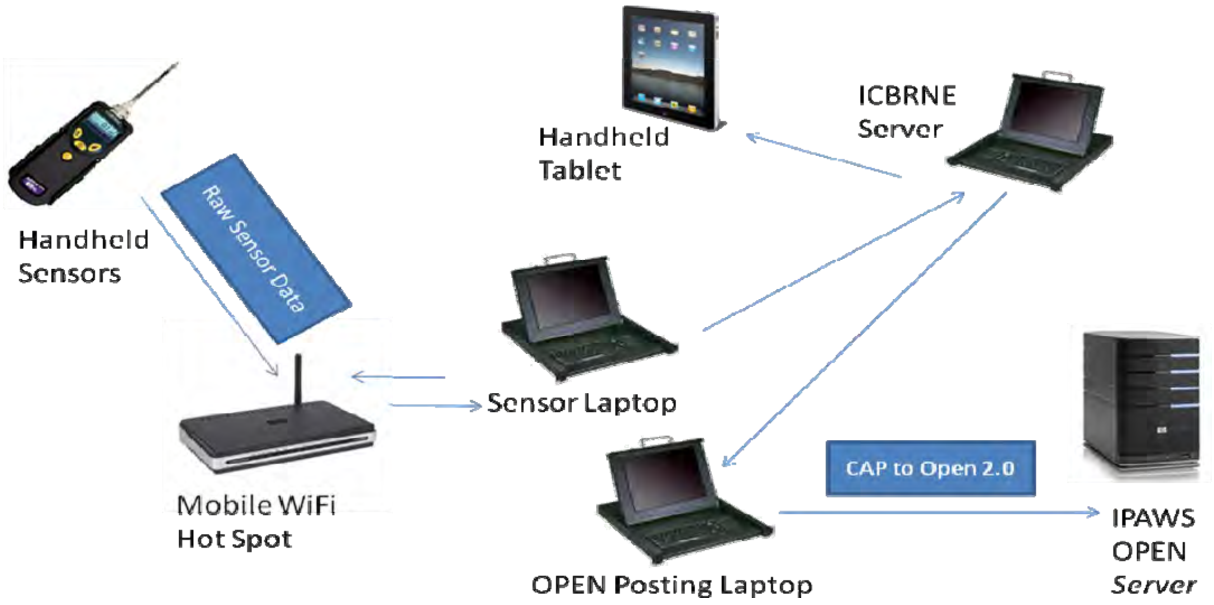

Figure 3. System Diagram for CWID.

EXERCISE

ROLE PLAYER TRAINING

National Guard members were trained by the SSC Pacific team as role players for Trial 2.32 at the Army National Guard Armory in Smyrna, Delaware on May 14 and 15. They were briefed about the history and future of ICBRNE and given an overview of how ICBRNE would be used during the CWID Master Scenario Events List (MSEL) play. Demos were provided to groups of National Guard members to allow each person to try out the ICBRNE web interface and to have hands on time with a sensor that would be used during the upcoming exercise.

JOINT MOBILE COMMAND AND TRAINING CENTER TRUCK

At the Herndon site, the system was set up inside the Joint Mobile Command and Training Center truck from Monmouth University’s Rapid Response Institute. Figure 4 shows the interior of the truck that housed and powered the various systems involved in the trial.

More importantly, the truck simulated real-world situations where the sensors would typically not be in close proximity to the EOC. First responders would use the sensors in a disaster area and transfer data to the truck. Configuration was restricted by the proximity of the Wi-Fi hotspot, but the team was able to emulate being separated from EOC operators.

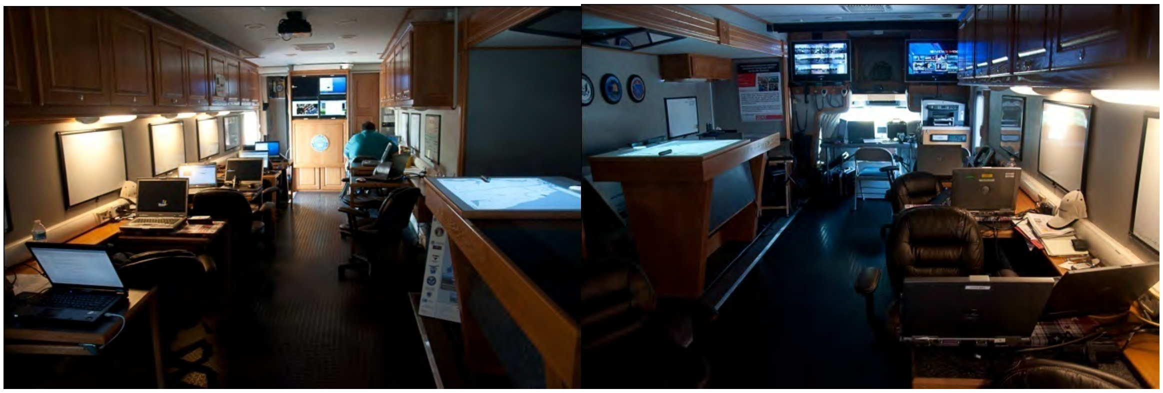

Figure 4. Joint Mobile Command and Training Center truck interior.

SETUP

The final setup had two laptops and the Wi-Fi hotspot inside the truck. Outside of the truck, there were sensors ready to fire and handheld tablets to display sensor readings and maps. This allowed for a quick briefing outside with the handheld tablets and for demonstrating the entire system in cases where time permitted. Figure 5 depicts the laptops inside the truck, and a handheld tablet and multiple sensors outside the truck.

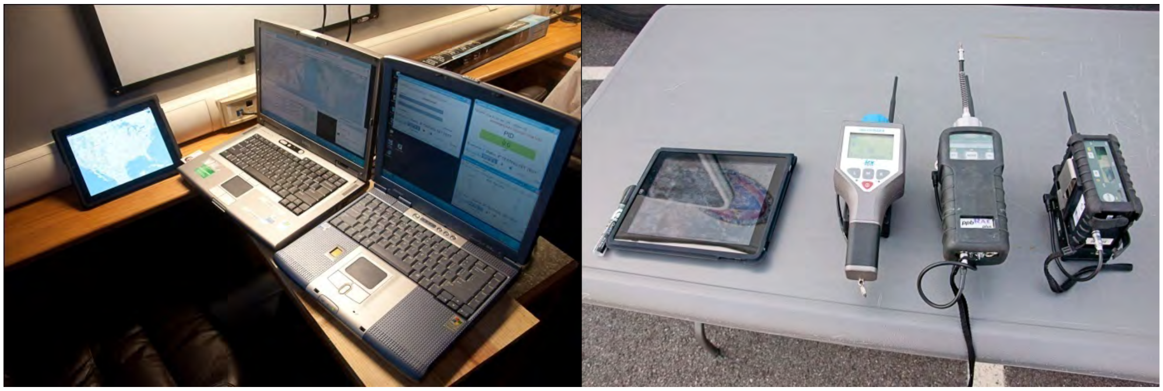

Figure 5. (Left) Emergency operations center (EOC) laptop and sensor laptop inside of truck. (Right) Handheld tablets and sensors outside of truck.

MSEL PLAY

The SSC Pacific team contributed to the MSEL play. There were not enough National Guard operators to operate every system, so SSC Pacific personnel supplemented National Guard operators for portions of the MSEL events.

The MSELs invoked the sensors shown in Figure 4 on the right, with the MSEL event typically requiring an operator to trigger a sensor beyond alarm thresholds and induce an alert transmitted to ICBRNE and then to IPAWS OPEN 2.0. Alerts were also sent to Twitter and Facebook, but these were not involved in the MSEL play.

TOURS

Tours were given throughout the day and allowed groups of people to meet with the different agencies involved in various CWID trials. The truck was the last stop on the tour. This created a lot of variation in the amount of time provided for briefings and demonstrations.

For briefings, emphasis was on the information sharing and interoperability aspects of the connectivity and the current state of ICBRNE tools being used. On occasion, there was enough time to demonstrate the "end-to-end" message flow of the system. In these cases, we demonstrated the ppbRAE chemical sensor and its corresponding sensor readings on the laptop and a handheld tablet. Then the sensor operator used a dry-erase marker to trigger the sensor to detect levels above alarm thresholds, causing the sensor laptop to send an alert to the ICBRNE server. The alert would subsequently be reflected and viewed on the geo displays of the handheld tablets with live sensor readings. Likewise, the server generated a CAP compliant message to OPEN. The Remote Message Center (RMC) would receive the OPEN message and then generate a military standard nuclear, biological, chemical (NBC) message to JWARN, thereby demonstrating the route from a civilian sensor to a military command and control system. Finally and simultaneously, formatted and condensed alerts would be shown on Twitter and Facebook using the tablet devices (IPAD and Galaxy).

CONCLUSION

WHAT WORKED

- Participation in MSEL exercises involving ICBRNE went smoothly. ICBRNE alerts were typically sent on time. As mentioned, being independent of the truck network and CWID network was crucial to the success, because the other MSEL players were experiencing delays in the first few days due to inconsistent connections.

    - It was also beneficial to have the sensor simulation software to send alerts as a backup if there were issues with communication between the Wi-Fi sensor dongles and the sensor laptop.
    - Running the system with our own mobile Wi-Fi hot spot proved worthwhile avoiding the network issues with the truck's satellite connection.
- At first, there were issues distinguishing between alerts sent for MSEL exercises, alerts sent for testing, and alerts resulting from demonstrations during briefings.
    - This confusion was solved by modifying the extensible markup language (XML) tags in the CAP alerts sent from the sensor laptop.
    - For MSEL exercises, the exercise number was included in the headline tag so that it could be found quickly in the RMC.
- Full demonstrations were given that showed "end-to-end", civilian-to-military, system capabilities.
    - Demonstrations showed system components, triggered sensor alarms, displayed sensor readings on handheld tablets, showed geo locations of sensors and their alarm status updating real-time depending on the sensor detections, and alert information displaying on social networks.
    - The demonstration provided first responders with a variety of options, a variety of tools to work with in communicating with civilian EOC, knowing that the information can easily be shared with corresponding military incident command posts.
- Twitter and Facebook capabilities worked well and provided a good example of the potential impact of social networks and media could have on the emergency response and follow-on recovery efforts following hazard events.
    - Demonstrating the Twitter and Facebook updates on the handheld tablets also revealed the open nature of ICBRNE and how it can be quickly adapted to different systems.
    - Twitter integration turned out particularly useful for confirming that messages were being posted and to see the most important parts of messages being sent.
    - Social networking continues to show promise in response and recovery, but the full magnitude of its potential is largely untapped at this time.

WHAT DID NOT WORK

- The use of the tablets was sometimes a distraction when trying to explain the overall "end-to-end" capability and the vision of the system. Persons would tend to be fascinated with the tablet technology and lose focus on the vision being described.
- Sensor laptops sometimes needed to be restarted. The sensor software would load, and the dongle connection would be made, but the sensor readings would not update.
- Shortage of National Guard operators meant that some groups had to execute their own MSEL events, which detracted from the ability to demonstrate and brief the system to visitors.
- The responsiveness of the sensors to trigger could be slow at times.
    - As a backup, the team used a simulation software capability to send the appropriate CAP messages for some MSEL plays, thus sending alerts to IPAWS OPEN 2.0.
- Sometimes it would take a few minutes before an alert would show up on Facebook or Twitter.
    - To improve this, a modification to increase the frequency of the polling software to check for state changes is needed.

- Sometimes sensors would clearly alarm but would require significant time above alarm thresholds before an alert would show up on the server.
- Having a consistent connection with the Wi-Fi hotspot was great, but sometimes the 3G speed was not sufficient for so many devices. In particular, the mobile apps could feel sluggish when refreshing map views and sensor information.
- The IPAD and Galaxy tablet screens were difficult to view from the outside glare and sunlight. Also, the devices were impacted by the outside heat, causing them to shutdown at times.
- In some cases, the ICBRNE Android app crashed, possibly due to a memory leak.

NEXT STEPS

The following steps are a combination of recommendations to solve issues found during our overall participation, and to resolve comments and questions from visitors that toured during the exercise weeks.

- Identify and solve security issues.
  - There were questions about the user authentication and message level security provided by the system. Currently, the system allows user level access, via password, but stronger methods, such as using PKI, will be investigated for the future.
  - There were questions about how issues, such as false positives, would be dealt with. All alerts that are accessible by the public will need to be checked and confirmed. Fusion algorithms will be investigated to lower numbers of false positives.
- Develop a solution for cell phone connectivity for the Safe Environment Engineering Wi-Fi dongles.
  - This functionality could be mimicked using a second Wi-Fi hotspot for the sensors and sensor laptop to allow virtually limitless distance between the truck and the first responders.
- Further development of social media possibilities in disaster situations.
  - Broadcasting data to specific groups of people is possible and its usefulness is obvious, but the next step is taking data in from people through social networks, opening up many creative possibilities.
  - Explore and identify the current level of use of social media in local EOCs, but also, beyond that, to include recovery operations and improve timely resiliency information to public entities.
  - Explore possibilities of pushing alerts to specific user groups based on different notification schemes, such as, users with experience in certain areas (example: CPR certified) or with many posts geo tagged in a certain location with a maximum number of followers.
  - Explore semantic standards and the use of semantic techniques, such as, ontology and the Resource Description Framework (RDF) to develop smarter alerting.
  - Investigate smart alerting techniques to notify the public based on numerous criteria, such as, geo tags in real-time posts.
    - ➢ **Example:** A fire breaks out in the city. People take pictures and post them to Twitter and Facebook. Then the team searches and imports the pictures from people from the area who included the word ‘fire’ in the same message. Next the team checks the geo tagged information against time to see which way the fire is traveling.
- Perhaps a different layout should be used for the ICBRNE.info sensor reading pages for tablets. The tradeoff would be having just text so that the page can refresh with more frequency.

- Continue refining the mobile apps. The iPad app has some refresh issues where the menu bar can disappear and restarting is necessary to bring it back.
- More analysis is needed on what can be done with Facebook integration. Twitter is limited to 140 characters so there are only so many possibilities to what can be included in a Twitter alert. However, Facebook opens a lot of possibilities since content, like images and videos, can be posted.
- Upgrade the laptop used for sensor software. In Herndon, the sensor laptop held up, but required restarts when functionality would stop.

TRANSITION SUMMARY

The following are items that were transitioned or have potential for transition:

- **Interface to OPEN:** Transitioned to FEMA IPAWS-OPEN. The interface, developed from ICBRNE to OPEN, was the first successful interface in Java, and was shared with the development community. As a result a .NET implementation was developed and shared back to ICBRNE.
- **Apps and Social Media:** Potential transition of apps and social media networks that can provide connectivity to critical emergency response, as well as, long term recovery efforts in a hazards environment.
- **Messaging Capability:** Potential transition to include data translation services between messaging standards, such as, CAP to USMTF and CAP to UCORE messages.

BENEFITS TO THE NAVY

Information sharing between civilian and military responders is critical to Naval forces worldwide. The ability of a civilian emergency responder to send a chemical, biological and/or radiological sensor alert with potential critical live sensor readings and pertinent information could be crucial to an appropriate and timely military response. In this CWID trial that message was initiated by a civilian ICBRNE sensor at the Joint Mobile Command Center in Herndon, VA and received by a JWARN system at SSC Pacific, in San Diego, CA. The civilian initiated message could have easily been pushed to Navy operators on board ship, or at a shore-based command and control center, thereby receiving a military standard NBC alert message on their respective command and control host platforms (e.g., Global Command and Control System – Maritime (GCCS-M)), a message originated by a civilian responder.

Figure 6. CWID benefits all services. Photo taken at SSC Pacific with two SSC Trial 2.32 operators in background and C2 operators in foreground.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

1. REPORT DATE *(DD-MM-YYYY)*
July 2011

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
July 2010-July 2011

4. TITLE AND SUBTITLE

Wide Area Recovery & Resiliency Program (WARRP) Transition Manager Series, Coalition Warrior Interoperability Demonstration (CWID) 2011: SSC Pacific Civilian Message Systems in Trial 2.32

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS
Francis Cortez
Douglas Hardy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC Pacific
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 2003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Homeland Security
Science and Technology Directorate
Washington, DC 20528

10. SPONSOR/MONITOR'S ACRONYM(S)
DHS S&T Directorate

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
This is the work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction.

14. ABSTRACT
The SSC Pacific team participated in the Coalition Warrior Interoperability Demonstration (CWID) by supporting Trial 2.32: Managing Military Civilian Messaging (M2CM). The SSC Pacific team set up hardware and software at Herndon, VA and San Diego, CA running Integrated Chemical, Biological, Radiological, Nuclear and Explosives Program (ICBRNE) tools and technologies. The trial successfully demonstrated the ability to rapidly share information between military and civilian emergency communities.

15. SUBJECT TERMS
CWID, Integrated Chemical, Biological, Radiological, Nuclear and Explosives (ICBRNE), Trial 2.32, Managing Military Civilian Messaging (M2CM), Integrated Public Alerting and Warning System (IPAWS), Common Alerting Protocol (CAP)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Francis Cortez
					19B. TELEPHONE NUMBER *(Include area code)*
U	U	U	U	20	619-553-2739

INITIAL DISTRIBUTION

84300 Library	(2)
85300 E. Sullivan	(1)
85300 Archive Stock	(1)
53627 Francis Cortez	(1)
Defense Technical Information Center Fort Belvoir, VA 22060-6218	(1)
SSC Pacific Liaison Office C/O PEO-SCS Arlington, VA 322202-4804	(1)
Center for Naval Analyses Alexandria, VA 22311-1850	(1)
Government-Industry Data Exchange Program Operations Center Corona, CA 91718-8000	(1)

Approved for public release; distribution unlimited.

SSC Pacific
San Diego, CA 92152-5001