

U.S. Coast Guard Research and Development Center

1082 Shennecossett Road, Groton, CT 06340-6048

Operational Evaluation of RDC Technology Capabilities Demonstrated During CWID 2007



**FINAL REPORT
FEBRUARY 2008**



This document is available to the U.S. public through the
National Technical Information Service, Springfield, VA 22161

Prepared for:

U.S. Department of Homeland Security
United States Coast Guard
(CG-926)
Washington, DC 20593-0001

NOTICE

This document is disseminated under the sponsorship of the Department of Homeland Security in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

This report does not constitute a standard, specification, or regulation.



J. W. McCready
C4ISR Branch Chief
United States Coast Guard
Research & Development Center
1082 Shennecossett Road
Groton, CT 06340-6048

1. Report No.		2. Government Accession Number		3. Recipient's Catalog No.	
4. Title and Subtitle Operational evaluation of RDC technology capabilities demonstrated during CWID 2007.				5. Report Date 29 February 2008	
				6. Performing Organization Code Project No. 5913	
7. Author(s) J. Davin and K. Kettel				8. Performing Report No. R&DC UDI 832	
9. Performing Organization Name and Address Potomac Management Group, Inc., a division of Advanced Technology Systems, Corp. 7915 Jones Branch Drive McLean, VA 22102		U.S. Coast Guard Research and Development Center 1082 Shennecossett Road Groton, CT 06340-6048		10. Work Unit No. (TRAIS)	
		SAIC Aquidneck Corporate Park 28 Jacome Way Middletown, RI 02842			
12. Sponsoring Organization Name and Address U.S. Department of Homeland Security Commandant (CG-926) United States Coast Guard Washington, DC 20593-0001				13. Type of Report & Period Covered Final Report	
				14. Sponsoring Agency Code Commandant (CG-926) U.S. Coast Guard Headquarters Washington, DC 20593-0001	
15. Supplementary Notes The R&D Center's technical point of contact is Kathy Shea, 860-441-2770, email: Kathleen.S.Kettel@uscg.mil . The ATS representative is John Davin. The USCG Headquarters representative is Buddy Hartberger (CG-926).					
16. Abstract (MAXIMUM 200 WORDS) Three innovative and promising communication/information systems were evaluated as part of the Coalition Warrior Interoperability Demonstration (CWID) event for 2007. Specifically evaluated were technologies being developed in separate programs by the U.S. Coast Guard Research & Development Center, Groton: (1) a Boarding Team Communications System, (2) a Maritime Biometric Identification System, and (3) a Maritime Domain Awareness Data Sharing Community of Interest (MDA-DS-COI) System. These three systems were demonstrated to show an ability to exchange a variety of data/information – including voice, biometric data (fingerprints), and video. Exercise scenarios were designed to bring these three technologies together at Project SeaHawk in Charleston, SC, to perform operational utility assessments in a realistic field setting. The results showed that the Boarding Team Communications System and the Maritime Biometric Identification System are both at an advanced stage of development, and should be given serious consideration for USCG implementation. The Domain Awareness/Data Sharing Community of Interest system had limited success and should undergo additional development and evaluation.					
17. Key Words Biometric, CWID, Boarding Team Communications, Maritime Domain Awareness Data Sharing Community of Interest (MDA COI), Maritime Biometric Identification System, Identix.				18. Distribution Statement This document is available to the U.S. public through the National Technical Information Service, Springfield, VA 22161.	
19. Security Class (This Report) UNCLASSIFIED		20. Security Class (This Page) UNCLASSIFIED		21. No of Pages	
				22. Price	

(This page intentionally left blank.)

EXECUTIVE SUMMARY

This report summarizes the results of an evaluation conducted on three communications/information systems under development at the U.S. Coast Guard (USCG) Research & Development Center, and was developed from the CWID 2007 After Action Report.

The evaluation was conducted during the 2007 Coalition Warrior Interoperability Demonstration (CWID). CWID is an annual exercise that enables U.S. combatant commands, as well as similar international entities, to evaluate cutting-edge command-and-control technologies capable of being moved into operational use within 6–12 months after CWID evaluation.

During the CWID 2007 exercise, new command-and-control technologies interact over a temporary global network in accordance with the goals of scripted scenarios.

CWID 2007 was held June 11–22, 2007 at Dahlgren, VA, and at the SeaHawk operations center in Charleston, SC. The following USCG technologies were evaluated:

- Boarding Team Communications (BT Comms) – a rapidly-deployable communications system used to support USCG boarding-team operations conducted inside the superstructures of large, deep-draft merchant vessels.
- Maritime Biometric Identification System – a system that collects biometric and biographic data for transmission, by means of an encrypted wireless network, for comparison against an existing back-end database.
- Maritime Domain Awareness Data Sharing Community of Interest (MDA-DS-COI) system – an enhanced method for data-sharing that greatly improves situational awareness for USCG surface, air, and shore units when a command center is working a case.

The specific objectives of the evaluation were to:

- To demonstrate an ability to exchange a variety of data/information – including voice, biometric data (fingerprints), and video. This data is passed between USCG assets, sector command (SeaHawk), and externally to Department of Homeland Security (DHS), U.S. Northern Command (NORTHCOM), and CWID.
- To perform Operational Test and Evaluation of the MDA-DS-COI capability for data sharing

The Biometric Identification System worked extremely well during the CWID 2007 trial. The Identix® portable fingerprint scanner worked without any problems, as did the SAIC software on the laptop that supported the interface between the handheld and the back-end database. This system would be very useful to any cutters involved in positive identification of unknown persons encountered by the Coast Guard.

Several issues were discovered when deploying the BT Comms system software in a real world environment and proved an invaluable test. After troubleshooting the system worked sufficiently well. However, the size and weight of the routers, and the manner of use, were a source of frustration. Follow-on versions of the routers are intended to be smaller and provide longer

battery life. With improvements to the routers, this system should have wide applicability throughout the USCG.

The MDA-DS-COI System was once again a very good test of a capability service. As the first real consumers of the data being provided, CWID 2007 discovered several issues with the quality of the data. However sharing of data across the network with multiple consumers was effective.

The general consensus among the planners and participants is that CWID 2007 was worthwhile, and provided an excellent opportunity to evaluate new USCG technologies.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	v
1. INTRODUCTION.....	1
1.1 Background	1
1.2 Objectives	2
2. EVALUATED TECHNOLOGIES.....	2
2.1 Boarding Team Support/Communications System.....	3
2.2 Maritime Biometric Identification System	3
2.3 Maritime Domain Awareness Data Sharing Community of Interest.....	4
3. PROCEDURE	5
3.1 CWID Logistics	5
3.2 CWID Activities	6
3.3 CWID Evaluation Scenarios	6
4. FINDINGS	9
4.1 Watchstander Comments	9
4.1.1 NORTHCOM Comments	9
4.1.2 Dahlgren Comments	10
4.1.3 SeaHawk Comments.....	12
4.2 Overall Impressions	12
4.2.1 Personal Observations.....	12
4.2.2 USCG Observations and Recommendations	13
4.2.3 CWID General Observations and Recommendations.....	13
5. CONCLUSIONS	13
6. RECOMMENDATIONS.....	14
APPENDIX A. BOARDING TEAM SUPPORT/COMMUNICATIONS PROGRAM	A-1
APPENDIX B. MARITIME BIOMETRIC IDENTIFICATION.....	B-1
APPENDIX C. CWID TRIAL 3.58 DETAILED DATA SUMMARY	C-1
APPENDIX D. CWID TRIAL 3.58 DATA FLOW DIAGRAM.....	D-1
APPENDIX E. CWID TRIAL 3.58 OPERATIONAL OVERVIEW	E-1
APPENDIX F. CWID TRIAL 3.58 PROCESS FLOW	F-1
APPENDIX G. CWID TRIAL 3.58 BIOMETRICS ARCHITECTURE.....	G-1

APPENDIX H.	CWID TRIAL 3.58 CAPABILITIES & FUNCTION WORKSHEET	H-1
APPENDIX I.	CWID TRIAL 3.58 TRAINING PLAN	I-1
APPENDIX J.	CWID 2007 PARTICIPANTS	J-1
APPENDIX K.	SAIC TRIP REPORT FOR DAHLGREN, VA	K-1
APPENDIX L.	SAIC TRIP REPORT FOR CHARLESTON, SC SITE SURVEY.....	L-1
APPENDIX M.	CWID 2007 VIP BRIEF	M-1
APPENDIX N.	SAIC CWID BIOMETRICS TEST PLAN	N-1
APPENDIX O.	CWID TRIAL 3.58 INFORMATION ASSURANCE FINAL SCAN RESULTS	O-1
APPENDIX P.	CWID 2007 NSWC DAHLGREN AFTER ACTION REPORT	P-1

LIST OF FIGURES

Figure 1. System overview for USCG Trial IT 3.58.....	2
Figure 2. Maritime Biometric Identification System.....	4
Figure 3. Data flow diagram for Trial IT 3.58.....	8
Figure 4. Operational overview for USCG Trial IT 3.58.	9
Figure E-1. Operational view-1: IT 3.58.	E-1
Figure F-1. Operational view-5: IT 3.58 process flow.	F-1
Figure G-1. Biometrics architecture: IT 3.58.....	G-1
Figure I-1. USCG information sharing and communication solution.....	I-3

LIST OF TABLES

Table O-1. Transportation Protocol X.X.4.63.	O-3
Table O-2. Application Protocol X.X.4.233.....	O-4

LIST OF ACRONYMS

AIS	Automatic Identification System
BT Comms	Boarding Team Communications
CDO	Command Duty Officer
COI	Community of Interest
CWID	Coalition Warrior Interoperability Demonstration
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOJ	Department of Justice
DV	Distinguished Visitor
HSIN	Homeland Security Information Network
IBIS	Integrated Biometric Identification System
IS&C	Information Sharing & Communication
MDA	Maritime Domain Awareness
MDS-DS- COI	Maritime Domain Awareness Data Sharing Community of Interest
MSEL	Master Scenario Event List
NCES	Net-Centric Enterprise Services
NORTHCOM	U.S. Northern Command
NSWC-DD	Naval Surface Warfare Center - Dahlgren Division
PDA	Personal Digital Assistant
PMG	PMG a division of Advanced Technology Systems
R&D Center	U.S. Coast Guard Research & Development Center
SAIC	Science Applications International Corporation
SME	Subject Matter Expert
U.S.	United States
USCG	United States Coast Guard
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VIP	Very Important Person

1. INTRODUCTION

Three innovative and promising information/communication systems were evaluated as part of the June 2007 Coalition Warrior Interoperability Demonstration (CWID). CWID is an annual opportunity, sponsored by the Joint Chiefs of Staff for U.S. combatant commands, as well as international organizations, to evaluate new and emerging technologies that can be deployed within 6–12 months after the exercise. This report was developed from the CWID 2007 After Action Report.

For each CWID, a temporary global network is established over which cutting-edge command-and-control technologies interact to support scripted scenarios. Specific technologies are evaluated for utility, interoperability with existing and new systems, and security.

The three systems evaluated were:

- The Boarding Team Communications (BT Comms) system – a high-speed, secure, broadband, wireless network that supports sensitive voice, data, and video communications among boarding-team members operating within the superstructure of large ships.
- The Maritime Biometric Identification System – a system, composed of a handheld collection device and software on a Toughbook®-74, that collects fingerprints, digital photo, and biographical data for immediate transmission to a national database to check against watchlists.
- The Maritime Domain Awareness Data Sharing Community of Interest (MDA-DS-COI) system – an enhanced method for data-sharing that greatly improves situational awareness for USCG surface, air, and shore units when a command center is working a case.

These systems were evaluated in combination toward supporting U.S. Coast Guard (USCG) mission execution and interaction with other Department of Homeland Security (DHS) and Department of Defense (DOD) agencies

1.1 Background

A decision was made in late 2006 to evaluate the interoperability of the three technologies mentioned above at CWID 2007. These technologies were being developed in separate programs at the U.S. Coast Guard Research & Development Center (R&D Center), Groton, CT. It was determined that evaluating these technologies at CWID would provide many benefits, including an opportunity to test and evaluate the systems in a controlled exercise.

The USCG Research & Development Program (CG-926 and R&D Center), in partnership with the Maritime Domain Awareness Program Integration Office (CG-52), of the Policy and Planning Directorate (CG-5), were tasked with coordinating the USCG's participation in CWID 2007. CG-926 and the R&D Center hired PMG, a division of Advanced Technology Systems, to assist with the planning and documentation required from CWID participants. The R&D Center also hired Science Applications International Corporation (SAIC) to provide Subject Matter Experts (SME), coordination, and execution of the CWID.

1.2 Objectives

The specific purpose of USCG participation in CWID 2007 was to demonstrate and assess the interoperability of USCG Command, Control, Communications, Computers, Information, Surveillance, and Reconnaissance systems with those of other federal, state, and local agencies, including, but not limited, to U.S. Northern Command (NORTHCOM); the DHS Office of Preparedness; USCG boarding teams; Joint Port and Harbor Operations Centers (at the USCG Sector level); SeaHawk Joint Operations Center, Charleston, SC; local law enforcement, and the National Guard.

Specific objectives include:

- To demonstrate an ability to exchange a variety of data/information – including voice, biometric data (fingerprints), and video. This data is passed between USCG assets, sector command (SeaHawk), and externally to DHS, NORTHCOM, and CWID.
- To perform Operational Test and Evaluation of the MDA-DS-COI capability for data sharing.

2. EVALUATED TECHNOLOGIES

The USCG was assigned trial number IT 3.58 for CWID 2007. Figure 1 depicts the operational overview for USCG Trial IT 3.58: Information Sharing and Communications.

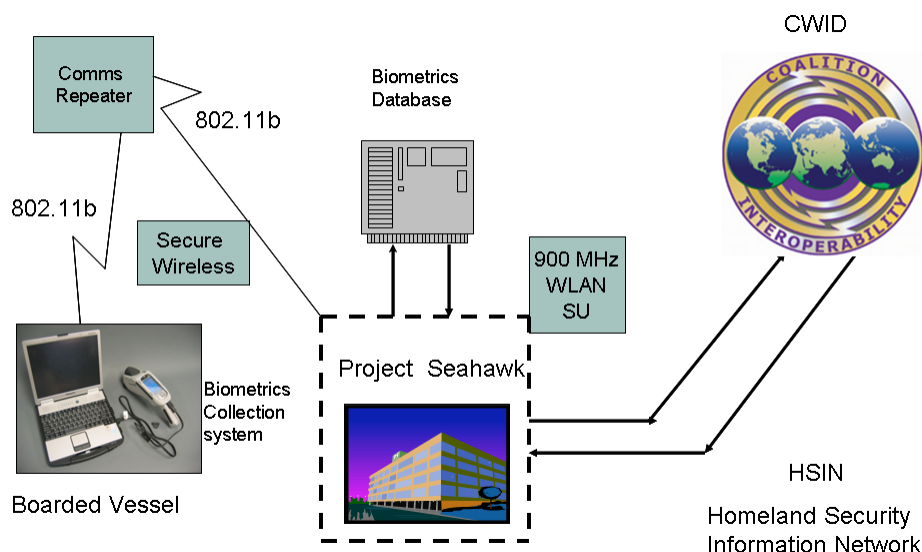


Figure 1. System overview for USCG Trial IT 3.58.

The Maritime Biometrics Identification System is carried aboard a vessel by USCG Boarding Team members. The collected fingerprints, digital photos and biographic data are transmitted by the BT Comms system of wireless 802.11b repeaters through the SeaHawk 900 MHz wireless network to a Biometrics Database where the information is evaluated. The results from biometrics evaluation plus data from the MDA-DS-COI are then posted on the DHS Homeland Security Information Network (HSIN) where it is available for decision-making at CWID. The

3.58 Information Sharing and Communications trial was the primary focus of the USCG technology evaluation. This section describes in detail the three technologies evaluated over the course of this trial.

2.1 Boarding Team Support/Communications System

Boarding-team members dispersed inside a commercial vessel often have difficulty staying in communication with each other. Uninterrupted communication is necessary both for the success of the mission and for the safety of the boarding-team members.

The USCG BT Comms system is a rapidly-deployable communications system used to support USCG boarding-teams, including the boarding of deep-draft merchant vessels and fishing vessels.

The BT Comms system provides a high-speed, secure, broadband, wireless network that supports sensitive voice, data, and video communications. The BT Comms system is capable of interfacing with military or commercial satellites, as well as with terrestrial wireless systems, to extend the communications reach to shore or parent cutter-commands.

The BT Comms system is transport-independent, and can interface with a variety networks (e.g., Public Switched Telephone Network, Very High Frequency, High Frequency, Military Satellite Communications, and Evolution-Data Optimized); allowing boarding teams multiple paths for communication.

The BT Comms system involves the use of Personal Digital Assistants (PDA) and wireless routers to form a secure, self-healing network throughout a boarded vessel. This network can transmit voice, data, and video. The system can also integrate with handheld radios.

Refer to Appendix A for additional information on the Boarding Team Support, or the Communications Program.

2.2 Maritime Biometric Identification System

To date, there has been no way to verify whether or not the crew and passengers on a boarded vessel are on the national watchlist. To overcome this problem, the Maritime Biometric Identification System provides a means for collecting biometrics and biographical information, searching existing national databases for biometrics match/no match and subsequently enrolling the personnel into that database.

As part of this system, a standalone system running Cogent fingerprint-matching software is made available to boarding teams on a Panasonic Toughbook®-74. The device used to collect fingerprint data is the Identix® Integrated Biometric Identification System (IBIS). The IBIS is connected to the laptop; the fingerprints are run against a subset database. The Maritime Biometric Identification System components are shown in Figure 2.



Figure 2. Maritime Biometric Identification System.

Biometric and biographic data is collected from the personnel of the boarded vessel. The photograph, fingerprint data and biographic data are sent via the BT Comms system through the SeaHawk wireless network to a biometrics database which identifies the fingerprints as “match” or “no match”. This simulated sending the data to a central database (i.e. the United States Visitor and Immigrant Status Indicator Technology, or US-VISIT). A message is then sent back to the boarding teams to verify whether or not the boarded crew and personnel are on a national watchlist.

For more information on the Maritime Biometric Identification System, refer to Appendix B.

2.3 Maritime Domain Awareness Data Sharing Community of Interest

The MDA-DS-COI System supports information sharing by providing access to a set of data sharing services deployed in a net-centric manner. The architecture that supports this capability is the Defense Information Systems Agency (DISA) Net-Centric Enterprise Services (NCES). The MDA-DS-COI System shares Automatic Identification System (AIS) data as the initial test capability. Several sources including the USCG, the U.S. Navy, and the U.S. Department of Transportation provide AIS data to the DISA NCES. Multiple consumers can then retrieve the information from the DISA NCES and use it to track vessels, including unified commands like SeaHawk.

This net-centric approach was integrated into SeaHawk over the course of a few weeks, resulting in a strategic view of approximately 5,000 vessels at any one time. For CWID 2007, this capability allowed watch centers to track vessels of interest and report their findings by means of the Homeland Security Information Network (HSIN). This approach provided broad interoperability with federal, state, and local partners.

SeaHawk implemented a simple web service and acquired DoD compliant certificates in order to connect to the NCES system. Once a subscription to the data was acquired by SeaHawk, NCES pushed all the data to SeaHawk’s web service. SeaHawk then stored the data in a database to generate the routes and provided the real time view of the vessel AIS data.

FalconView™ was then loaded at the SeaHawk joint command center to display the MDA-DS-COI data. FalconView™ is a non-proprietary government off-the-shelf application for analyzing and displaying geographical data crucial to the operators. Google Earth was also used at SeaHawk to display vessel tracks to illustrate the capability of integrating MDA shared data into any GIS mapping tool.

FalconView™ displayed various kinds of digital map data and associated geographically-referenced overlays. Routes were mapped for each vessel of interest and a full history of the movement of the vessel was stored for each phase of the exercise. Screenshots of the mapped routes was then uploaded to HSIN Portal to share with other players in CWID 2007 including Naval Surface Warfare Center - Dahlgren Division (NSWC-DD) and NORTHCOM.

3. PROCEDURE

Preparing to participate in an exercise such as CWID is complex and time-intensive, taking approximately one year. Preparations began with an initial planning conference in August, followed by a mid planning conference and a final planning conference, between November and April. Exercise scenarios were developed and incorporated into the Master Scenario Event List (MSEL), which describes the actions that the different exercise players will take. Additional man-hours were required to oversee the CWID 2007 effort as well as to attend the meetings and develop a number of the required documents, including:

CWID Trial 3.58 Detailed Data Summary	Appendix C
CWID Trial 3.58 Data Flow Diagram	Appendix D
CWID Trial 3.58 Operational Overview	Appendix E
CWID Trial 3.58 Process Flow	Appendix F
CWID Trial 3.58 Biometrics Architecture	Appendix G
CWID Trial 3.58 Capabilities & Function Worksheet	Appendix H
CWID Trial 3.58 Training Plan	Appendix I

3.1 CWID Logistics

The following sites were used for the CWID exercises:

- U.S. Northern Command (NORTHCOM), Colorado Springs, CO
- Naval Surface Warfare Center – Dahlgren Division (NSWC-DD), Dahlgren, VA
- Department of Justice (DOJ) Project SeaHawk, Charleston, SC
- SS Cape Chalmers, Charleston, SC
- Wellington, New Zealand (NZ) (virtual)

U.S. Coast Guard personnel and contractor support were located at all the above locations, with the exception of Wellington, NZ. The New Zealand Navy was interested in the Boarding Team

Communications program for possible use within its own ships, and their role players were able to access the information posted by the USCG on the CWID network.

A list of participants, together with the location where each participant was involved, is provided in APPENDIX J.

At the NORTHCOM site, two USCG representatives participated in role playing as a USCG liaison officer to NORTHCOM.

Three USCG representatives participated at NSWC-DD. The roles played were: USCG District/Area Commander, USCG Sector Chief Duty Officer (CDO), and DHS National Operations Center. See Appendix K for details.

One representative from SeaHawk played the role of SeaHawk CDO; two USCG representatives and one SeaHawk Task Force Officer made up a boarding team consisting of one team leader and two boarding-team members. See Appendix L for details.

The majority of the equipment and SMEs were located in Charleston, where the actual testing and evaluations took place. SS Cape Chalmers was used to test and demonstrate the BT Comms program and the Maritime Biometric Identification System. The Cape Chalmers is a training ship used by the Federal Law Enforcement Training Center in Charleston, SC. It is a standard United States Maritime Commission C3 type break bulk ship, 492 feet long, 69.5 feet wide, with a 28.5 foot draft, 7,800 gross tons, and 12,000 deadweight tons, built between 1939 and 1947. A duplicate set of biometric-identification-system equipment, consisting of a laptop and a portable fingerprint scanner, were used at NSWC-DD for demonstration purposes during the VIP tours.

3.2 CWID Activities

The first week of CWID 2007 consisted of training related to the CWID, the HSIN, and the equipment used during CWID. The second and third weeks consisted of exercise play with Master Scenario Event Lists (MSELs) /scenario prosecution and registered distinguished visitors (DV) and very important persons (VIPs) touring the CWID sites at NSWC-DD during both execution weeks (June 11–15, and June 18–22, 2007).

A typical tour consisted of a general CWID overview presentation (APPENDIX M) that included a question & answer session, followed by an escorted tour of the demonstration area. These tours allowed visitors to get first-hand information regarding the various trials, and to talk with the role players and system operators using the technologies. Some of the visiting VIPs are mentioned in SAIC's Trip Report for Dahlgren, VA (APPENDIX K).

3.3 CWID Evaluation Scenarios

The USCG used CWID 2007 as an opportunity to evaluate the efficacy and interoperability of three related information/communication systems being developed independently at the R&D Center. Exercise situations were designed to bring these technologies together at Project SeaHawk in Charleston, SC, for the purpose of performing operational utility assessments in a command center.

The following scenarios were used for the evaluations:

- Vessels of interest are missing with possible nuclear devices; exercise situational awareness.
- Suspicious vessel boarded; biometrics passed to US-VISIT.
- Suspicious ship with cargo not matching manifest; vessel boarded to investigate.
- Suspicious ship; crewmember is on the Known and Suspected Terrorist watch list.
- Survey harbor for hurricane damage; send video.

All boardings were conducted by SeaHawk Task Force Officers and U.S. Coast Guard personnel at Charleston, SC.

The scenarios involved the following activities:

- A BT Comms system of wireless 802.11b repeaters enabled a boarding team to exchange voice, data, and video information below decks.
- An on-board Biometrics system captured crew fingerprints and photographs and compared the captured data with data in the simulated US-VISIT database. See APPENDIX N for the preliminary test plan.
- The boarding team sent biometrics data, voice, and video to the SeaHawk CDO by way of the BT Comms system and the SeaHawk 900-Megahertz wireless local area network. See Appendix O for results of integration.
- This information and other SeaHawk products were posted on the HSIN. HSIN is a secure, unclassified, Web-based communications system that serves as DHS's primary nation-wide information-sharing and collaboration network. The network provides connectivity between DHS's Homeland Security Operations Center and critical private-industry and federal, state, and local organizations responsible for, or involved in, combating terrorism, responding to critical incidents, and/or managing special events.
- SeaHawk acquired a DoD compliant certificate in order for the systems to interface with the worldwide AIS as published by the MDA-DS-COI on the DISA NCES.
- The HSIN also connected the SeaHawk node to the rest of the CWID infrastructure and organization, including NSWC-DD and NORTHCOM.

The USCG evaluated capabilities, including biometrics sensors combined with boarding-team communications. Voice, video, and data streams from the boarding team were passed through the DOJ Project SeaHawk Joint Operations Center in Charleston, SC, and then onto the CWID network for integration with common operational pictures, and for command-and-control decision making. Figure 3 illustrates the data and information flow.

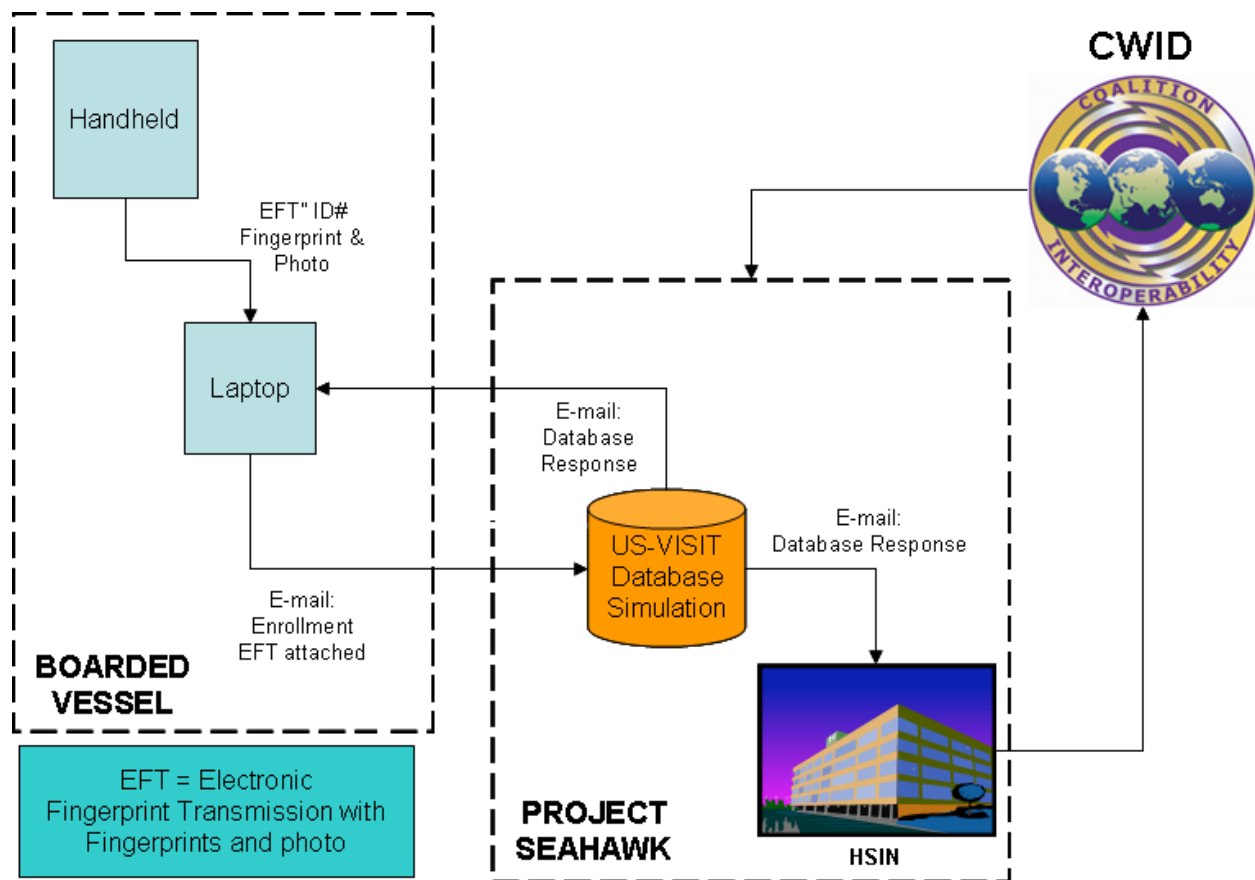


Figure 3. Data flow diagram for Trial IT 3.58.

The overall objective of the USCG Trial IT 3.58 at CWID 2007 was to demonstrate effective sharing of voice, video, and data between all Homeland Security entities and stakeholders in Homeland Security missions. The USCG required DOD Architecture Framework compliant architectures and mission threads supporting this trial. The purpose of the mission threads was to clearly articulate and depict operational processes and information exchanges for scenarios being exercised in CWID 2007. This initiative assisted the USCG in developing, consolidating, and validating operational concepts, architectures, and requirements. It also provided the first opportunity to use the Biometric Identification System in conjunction with the Boarding Team Communications System. Figure 4 shows a graphical representation of USCG Trial IT 3.58 at CWID 2007.

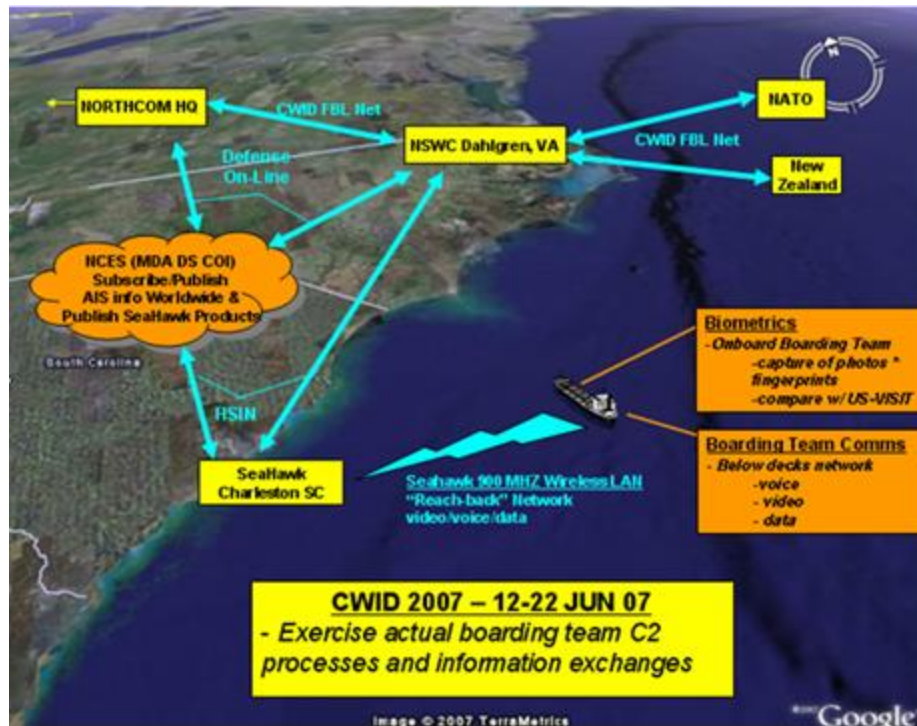


Figure 4. Operational overview for USCG Trial IT 3.58.

4. FINDINGS

This section summarizes the findings derived from the CWID 2007 evaluation.

4.1 Watchstander Comments

This section provides a brief description of each technology evaluated in this trial, followed by the respective lessons learned, and the recommendations made.

Note: To reduce the possibility of misrepresenting any participant's comments, most comments were copied directly from participant reports and emails. Occasionally, comments were paraphrased slightly to capture two or more similar thoughts.

4.1.1 NORTHCOM Comments

- The watchstanders found it difficult to monitor and understand the many different systems and chat programs provided, including HSIN Chat and CWID Chat.
- When the CWID Portal wasn't working, the watchstander had to find workarounds to receive and pass information.
- Watchstander was unable to forward the video clip sent to her, because the size of the clip (23 Megabytes) exceeded limits on the email system. She was able to transfer it with the use of a memory stick and walking it to the user.

- The watchstanders benefited through their involvement in CWID and recommend continued involvement.
- The maritime scenario seemed realistic.
- Two watchstanders were sufficient to support CWID at NORTHCOM.
- Late assignment of the two watchstanders resulted in them working hard to catch up. Recommend the watchstanders be selected early and be involved earlier.
- Recommend that USCG continue participation in future CWID exercises.
- Recommend that USCG Reserve unit commanding officer in Colorado Springs evaluate whether that unit should continue to provide watchstanders to CWID.

4.1.2 Dahlgren Comments

- Biometrics demonstration was very well received by many visitors. The equipment that was provided at Dahlgren was especially beneficial for briefings and demonstration of how the equipment was used.
- The senior watchstander at Dahlgren was sometimes uninformed about the status of the trial, often due to non-trial distractions.
- There was some initial confusion on the first day of training when another trial (ID Map with General Dynamic's Information Technology) was expecting to use a USCG watchstander. This appeared to be a misunderstanding and was resolved when they got someone from the U.S. Navy to work with them.
- Technical representatives from SAIC and equipment specialists were very useful for answering questions and keeping the equipment working.
- R&D Center found a conflict when the role players were busy being trained on general CWID trials. This made it difficult to find time to train the USCG watchstanders and they didn't have enough time to be fully trained.
- It was suggested that in the future, general CWID training be done in the morning and keep the afternoon clear for USCG training.
- Consider training off site to allow training to be done without interruption.
- After considerable discussion about the USCG watchstanders, it was suggested that more reservists be used in the future. It was pointed out also that many reservists can only serve a maximum of two weeks and therefore could not be available for the full three-week period. It was agreed that using reservists has both pro's and con's.
- It was recommended that more discussions be held with the other trials to find out what they would need from the watchstanders to reduce surprises during the exercise.
- It was agreed that the USCG gained goodwill and credibility with other services and vendors from our participation in the exercise.
- MDA-DS-COI didn't demonstrate well and wasn't used by the role players.

- USCG used CWID to prove that a collection of systems could be interconnected and used to make a larger system.
- There were too many different chat networks used (3–5); it was confusing to the watchstanders, and they were confused about which ones they should use.
- It was unclear to the watchstanders when the exercise began and ended each day.
- VIP tours interfered with the role players in their exercise play.
- The watchstanders wanted more MSEL activities.
- Security clearances were a major problem with multiple submissions often required to Dahlgren.
- A question was posed: Why doesn't USCG participate in the DOD Clearance Verification System Joint Personnel Adjudication System?
- USCG doesn't have a clear sponsor for CWID.
- The Dahlgren site had problems with security and training.
- It was suggested to consider evaluating the new Mobile Command Center project at CWID 2008.
- The video showing how the BT Comms equipment is used aboard ships was very helpful as a means to explain the operation to visitors.
- The Dahlgren watchstanders did an excellent job, especially with the briefings to the visitors.
- The lack of DHS participation took away from the realism of certain scenarios where contact with various agencies within DHS would have been beneficial.
- Sharing MDA information with the community of interest project appeared to be a duplication of effort. Spiral one development was to provide AIS data within the community, something that Web-based Common Operational Picture (WEBCOP) should be able to deliver within a couple of months. The symbology the R& D Center came up with is nonstandard as opposed to DOD, but may provide a simplified version needed for Port Partners.
- Recommend that two complete groups of watchstanders be trained and available to rotate through watch stations.
- Recommend future involvement of other DHS agencies: Transportation Security Agency, Customs and Border Protection, and Customs and Immigration Enforcement.
- Recommend that training provided is only for trials that USCG participates in. It was recommended that role players be selected by the USCG office that owns the system being tested.
- Recommend finding the right role players with the proper skills.
- Recommend the VIP brief be presented to the role players during the first week of training so they could become familiar with it before the exercise began.

- HSIN did not effectively support local information sharing. Users were confused and frustrated without clear guidance on HSIN's role or how to use the system to share information effectively.

See APPENDIX P for more details.

4.1.3 SeaHawk Comments

- SeaHawk was a good site for CWID because there were multiple large ships in the area to use for testing the equipment.
- The BT Comms equipment was difficult to keep operating reliably. We were able to transmit voice but not data.
- The interface into the SeaHawk command center required a large amount of time and effort to get connected.
- The boarding teams found it hard to actually use the BT Comms gear; the red lights on the routers needed to be watched while walking the ship passageway and could be a safety concern.
- Each router and PDA in BT Comms needed to be provided with encrypted passwords. This requirement was awkward and time consuming.
- It was difficult to get all the software working together with the BT Comms gear.
- The use of a couple of rooms at SeaHawk was greatly appreciated and provided room to store and test all the equipment.
- MDA data sharing quality problems were discovered that the providers were originally unaware of.
- The size and weight of the routers, and the manner of use, were found to be a source of frustration; the size and weight need to be reduced.

4.2 Overall Impressions

This section includes personal observations, USCG-specific observations, and CWID general observations. Each of the comments made here would be addressed during the planning and execution of a USCG participation in CWID 2008.

4.2.1 Personal Observations

- CWID 2007 was a worthwhile and positive experience for the USCG. It took two different R&D Center projects (BT Comms & Biometric At Sea) and demonstrated that they could work together and provide a solution to a thorny communications problem for USCG boarding teams.
- The BT Comms part of the trial was impressive when watchstanders in Dahlgren were able to talk directly to role players in the engine room of the ship in Charleston harbor and even see live pictures transmitted.

4.2.2 USCG Observations and Recommendations

- One of the larger questions for the USCG to answer, if they want to continue to participate in CWID, is: Is the cost of CWID – in terms of time, personnel, and money – worth the benefit of participating?
- The commitment of the USCG R&D Center personnel and contractors helped ensure a successful trial.
- Thanks go to SeaHawk in Charleston, SC including the IT staff, watchstanders, and personnel from Sector Charleston, and to the watchstanders at NORTHCOM.
- CWID seems to be invisible to most USCG Headquarters personnel and programs. Recommend work on ways to provide higher visibility.
- It is unclear if there would be any impact if the USCG didn't participate in CWID in the future.

4.2.3 CWID General Observations and Recommendations

- Of the 33 interoperability trials at Dahlgren, the USCG Information Sharing and Communication trial was one of the top six selected by NSWC-DD in their After Action report.
- The presence of the various contractors providing the equipment for this trial was a critical success factor for the exercise.
- Recommend all players get involved early in the CWID planning cycle to help make the trial better.
- Consider using active duty USCG personnel that are assigned and working at NORTHCOM.
- Recommend scheduling more MSEL activities throughout day to keep the watchstanders more engaged.
- Recommend additional efforts be made to directly involve DHS and other DHS organizations in the CWID exercises.
- Recommend that a brief be provided to all flag officers at USCG Headquarters to make them aware of the program and the week of involvement from other offices and programs.

5. CONCLUSIONS

The CWID 2007 evaluation demonstrated that the BT Comms system and the Maritime Biometric Identification System can work together effectively in a real-world setting. Many knowledgeable observers were impressed with the ability of these systems to transmit voice, data, and video.

The Maritime Biometric Identification System worked extremely well during the CWID 2007 trial – the best of the three technologies evaluated. This level of success was not surprising, because a prototype of this system is currently being used successfully in the waters of the Mona Pass between the Dominican Republic and Puerto Rico.

The IBIS portable fingerprint collection device worked without any problems. Occasionally, the fingerprint data being transmitted with the BT Comms system wasn't able to get through, but the problem was found to be with the BT Comms System or the SeaHawk 900 MHZ wireless system. This system would be very useful to any cutters involved in situations where positive verification of a person being on a watchlist could enhance crew safety and potentially lead to USCG apprehension of wanted persons.

The BT Comms system also worked well during the CWID 2007 trial. Although the software did not work when there were multiple host identifications, a workaround to this problem was quickly found. This workaround required all the routers to be turned off and then turned back on, to force a proper connection. In addition, the size and weight of the routers, and the manner of use, were found to be a source of frustration for the boarding team members. This system could have wide applicability throughout the USCG with improvements to the routers.

The MDA-DS-COI System was once again a very good test of a capability service. As the first real consumers of the data being provided, CWID 2007 discovered several issues with the quality of the data. However sharing of data across the network with multiple consumers was effective.

The general consensus among all the planners and participants was that CWID 2007 was worthwhile and provided an excellent opportunity to evaluate new USCG technologies. However, the systems that were tested were not far enough along in their development for full scale testing. It is recommended that systems be tested only if they are truly ready for full scale testing.

Issues to be addressed include: (1) whether the benefit from participating on CWID is worth the full cost required when time out of the office, per diem, and travel are included; (2) which office(s) should own or are responsible for CWID; and (3) how to get broad support and visibility for CWID from a variety of program offices.

6. RECOMMENDATIONS

The following recommendations are made on the basis of an analysis of the results of this evaluation:

- The R&D Center should consider participating in CWID 2008 as a means of evaluating other new technologies close to being deployed or ready for field testing. The only caution is that the systems be fully prepared for field testing.
- The USCG should consider deploying both the BT Comms system and the Biometric Identification System to the field.
- The MDA-DS-COI System should be further developed to continue to improve the scale of data sharing, and improve the quality of the data.

APPENDIX A. BOARDING TEAM SUPPORT/COMMUNICATIONS PROGRAM

BOARDING TEAM SUPPORT/COMMUNICATIONS PROGRAM

U.S. DEPARTMENT OF
HOMELAND SECURITY



UNITED STATES COAST GUARD RESEARCH & DEVELOPMENT CENTER

Safe and Effective Maritime Security



A boarding team from the Coast Guard Cutter ADAK climbs aboard a cargo vessel in Iraq. Coast Guard photo.

As the lead Federal agency for maritime homeland security, the U.S. Coast Guard conducts vessel boardings and inspections, both at sea and at the pier.

These boardings hold challenges and dangers for Coast Guard boarding teams. Boarding team members may have difficulty communicating within commercial vessels, crew members may lack proper identification, fully inspecting large vessels is time consuming and wrought with missed

opportunities, and boarding team members must be constantly aware of the safety of all members.

New techniques and technologies provide Coast Guard boarding teams with the ability to perform these duties more effectively, efficiently, and safely.

The **USCG Research & Development Center** (R&D Center) launched the Boarding Team Support/Communications Program to:

- Support the development of technology that will increase the safety and effectiveness of boarding teams,
- Identify gaps in capabilities that affect accomplishment of boarding team missions, and
- Promote appropriate interagency coordination and ensure that research is not being duplicated.

R&D Center Strengths:

- Wide breadth of scientific, engineering, and operational field expertise
- Modeling and Simulation (M&S)
- Human Systems Integration
- Operational Effectiveness Assessment
- Test & Evaluation (T&E)

What Can the R&D Center Provide?

The R&D Center can provide a business strategy that will take your program from identifying a problem to acquiring the solution. We provide technical knowledge, Coast Guard operations experience, and contracting expertise. Working with other government agencies and vendors, the R&D Center devises workable Coast Guard solutions.

How Can We Work Together?

The Boarding Team Support/Communications Program can:

- Define performance gaps,
- Translate user wants/needs into requirements,
- Identify emerging technologies,
- Provide an unbiased assessment of potential solutions,
- Leverage other government agency development efforts to benefit the Coast Guard,
- Plan development strategy, and
- Plan and execute T&E in support of acquisitions.



Container vessel awaits boarding. Coast Guard photo.

Recent Reports

User Evaluation of the Tactical Ballistic Survival System for the Enhanced Maritime Safety and Security Team analyzed the efficacy of a load carriage/ballistic protection vest system that integrates emergency flotation, level 3 ballistic protection, and configurable load carriage.

Performance Evaluation of the Pulsed Elemental Analysis with Neutron (PELAN) System evaluated the performance of a technology that could detect contraband behind bulkheads and walls in vessels and shipping containers.

Maritime Biometrics Identification at Sea Requirements Study identified and documented Coast Guard biometric requirements for identifying individuals during vessel boardings or alien migrant interdiction operations.

Boarding Team Support/Communications POC: James Fletcher 860-441-2659, James.E.Fletcher@uscg.mil

www.rdc.uscg.gov <http://cgweb.rdc.uscg.mil> 1082 Shennecossett Road Groton, CT 06340-6048 p: 860-441-2600 f: 860-441-2792
Approved for public release May 2007

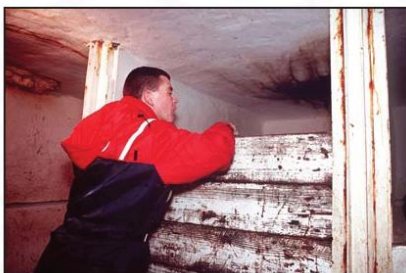
BOARDING TEAM SUPPORT/ COMMUNICATIONS PROGRAM

SAMPLE OF CURRENT PROJECTS



Today's vessels make communication difficult.
Coast Guard illustration.

Digital Assistants (PDA) as communication devices and smart wireless repeaters that are deployed throughout the vessel to form a secure, self-healing network in critical areas on a boarded vessel. This network can transmit voice, data, and video. The solution can also integrate with legacy handheld radios. Phase one development included a first generation engineering prototype that validated the proof of concept. The second phase development focused on size reduction, increased transmitter power, increased ruggedization, and human factors analysis of the design.



Vessel inspection challenges. Coast Guard photo.

collects and focuses back-scattered x-rays onto a screen. The image is captured using a digital camera, enhanced using real-time image processing software, and displayed on a small flat-panel display. The low power makes it safe for users. The trade-off is its limited ability to penetrate sheet metal. Sponsored by Homeland Security Advanced Research Projects Agency (HSARPA), the initial evaluation is nearing completion. After which, the prototype will be lab tested and if successful, the R&D Center will conduct an independent user-field test to verify the prototype's performance in an operational environment. The goal is to determine the efficacy of this technology in searching for hidden contraband on vessels.

Boarding Team Connectivity seeks to provide reliable, secure communications among boarding team members while dispersed throughout a large vessel. The candidate technical solution uses Personal

Vessel Compartment Inspection is evaluating the Lobster Eye X-ray Inspection Device (LEXID). It is an x-ray imaging device that uses a low power, hard x-ray source. A focusing array



Mobile biometrics identification system. Coast Guard photo.

Maritime Biometrics Identification at Sea implements a proof of concept for a mobile biometrics identification system that is being used by 110-foot patrol boat crews for positive identification of illegal migrants interdicted in the Mona Passage between the Dominican Republic and Puerto Rico. In the proof of concept, a maritime system has been designed and built that collects fingerprint and digital facial images with handheld devices. This data is integrated with biographic data for search and enrollment in the Department of Homeland Security's (DHS) United States Visitor and Immigrant Status Indicator Technology program (US-VISIT). The first phase used an on-board database of 800,000 biometric templates on a laptop computer and the data searches were done onboard. The second phase leverages a newly deployed 110-foot patrol boat-based satellite communications system to send biometric data back to DHS for comparison with the full US-VISIT database of 80 million records.



BT member evaluates Ionscan swipe for drug detection.
Coast Guard photo.

Multi-mode Detection is evaluating four commercially available, enhanced trace narcotics and explosives detection systems. These systems have a simultaneous narcotics and explosives detection capability and will replace the aging Ionscan 400B trace narcotics detector. The evaluation will consist of performance testing in a controlled laboratory environment and a controlled field environment.

If the candidate devices successfully pass testing in controlled environments, they will be evaluated in an operational field environment.



APPENDIX B. MARITIME BIOMETRIC IDENTIFICATION

MARITIME BIOMETRIC IDENTIFICATION

U.S. DEPARTMENT OF
HOMELAND SECURITY



Identifying the Dangerous At-Sea



Undocumented migrants stopped at sea. Coast Guard photo.

The U.S. Coast Guard is tasked with keeping the nation's maritime borders secure from illegal immigration. Due to the inability to identify citizenship for large numbers of undocumented passengers, the Coast Guard boarding teams have had little choice but to return intercepted foreign nationals to their respective homelands—potentially returning convicted criminals and suspected terrorists for another try at illegal entry.

The Coast Guard's Research and Development Center (R&D Center) has been working with partnering agencies to provide at-sea boarding teams with real-time access to national and international biometric databases. The Coast Guard's Maritime Biometric Identification At Sea pilot program at Mona Passage has tested an alternative to the current cycle of interdiction and return by use of a stand-alone portable database supplied by US-VISIT as an on-board reference for biometric data taken during boardings. The R&D Center has assessed the pilot program and has developed deployment scenarios tailored to the needs of the Coast Guard, and of partnering agencies.

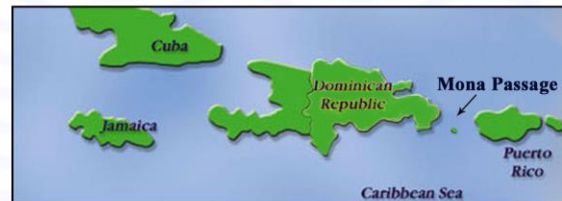
Partner Agencies:

- Department of Homeland Security US-VISIT
- Department of Homeland Security Science and Technology
- U.S. Navy
- Customs & Border Patrol
- Biometrics Fusion Center
- Science Applications International Corporation (SAIC)

R&D Center Maritime Biometrics Project Support

- Inter-agency coordination and dissemination
- Project management
- Testing and evaluation
- Analysis and assessment

Biometrics offers a means to positively identify an individual, regardless of disguise or alias. The Coast Guard's Biometrics program places the enormous resources necessary to cross-reference biometric data with existing U.S. and international databases in the hands of the boarding officers at every interdiction.



Initial results at Mona Passage are encouraging. During Phase I, 20 percent of interdicted undocumented passengers have been found to possess a criminal background, and prosecutions have increased dramatically from two successful prosecutions per year to 22 in three months. Implementation of Phase II will provide a real-time link between USCG boarding officers and the full reference capacity of US-VISIT—including coordination of biometric data with other U.S. and international agencies.



Undocumented migrant is checked for weapons as he boards the U.S. Coast Guard Cutter OAK. Coast Guard photo.

Maritime Biometric Identification POC: Dr. Thomas Amerson 860-441-2894, Thomas.L.Amerson@uscg.mil

www.rdc.uscg.gov <http://cgweb.rdc.uscg.mil> 1082 Shennecossett Road Groton, CT 06340-6048 p: 860-441-2600 f: 860-441-2792
Approved for public release May 2007

(This page intentionally left blank.)

APPENDIX C. CWID TRIAL 3.58 DETAILED DATA SUMMARY

Interoperability

Trial Tracking Number: IT 3.58

System Name: USCG Information Sharing and Communications

System Acronym: USCG IS&C (Previous 2.58)

Trial Creator: Buddy Hartberger

System Description: This trial is designed to demonstrate a combination of information and communication systems that should effectively support U.S. Coast Guard mission execution and our interaction with other DHS and DOD agencies. The USCG Boarding Team Communications System (CG BT Comms) is a rapidly deployable communications system used to support all CG boarding team operations, such as the boarding of deep draft merchant vessels, fishing vessels, etc. The BT Comms System provides a high-speed secure broadband wireless network capable of supporting sensitive voice, data and video communications. The BT Comms System is capable of interfacing military or commercial satellites as well as terrestrial wireless systems to provide capability for communications to reach back to shore or parent cutter commands. The BT Comms System is transport independent and can interface with a variety of types of networks (PSTN, VHF, HF, MILSATCOM, EV-DO, etc) allowing boarding teams multiple paths for communication.

Coalition Partners

Coalition Partners:

Partner Name: NZ

Sponsor? No

Points of Contact

Govt POC

Command/Agency:

PMO does support this Trial.

Interoperability Trial Information

Name:	Albert Hartberger
Email:	albert.w.hartberger@uscg.mil
Phone:	202-475-3488
Company:	U.S. Coast Guard (CG66)
Program Management Office Code:	USCG (CG-66)
Contact Allowed?	Yes
Should this Point of Contact be contacted (via email) of all changes made to the trial?	Yes
POC Type(s):	Government, Homeland Security/Defense, Program Management Office,

Describe POC's experience with CWID, the CWID SWG's operations, or entering MSEL events into CWID MSEL software:

Technical,
Third year coordinating
USCG participation ... USCG
is planning to use CWID 07 to
evaluate several
developmental systems that
USCG expects to deploy
USCG wide ... the CWID
evaluation will help us
identify existing shortcomings
so that follow-on development
can be completed if necessary.

Name:

John Davin

Email:

john.j.davin@uscg.mil

Phone:

(202) 372-2629

Company:

U.S. Coast Guard

Program Management Office Code:

Contact Allowed?

Yes

Should this Point of Contact be contacted (via email) of all changes made to the trial?

Yes

POC Type(s):

Government, Homeland
Security/Defense, Program
Management
Office, Technical,

Describe POC's experience with CWID, the CWID SWG's operations, or entering MSEL events into CWID MSEL software:

CWID Objectives Supported

Objectives Supported:

CWID Objective:

Enhance the commander's capability to command, control and coordinate across joint and coalition forces, government agencies, NGOs, and first responders.

Is this the primary objective of this trial? Yes

List each system capability to be demonstrated by your Trial (in priority order):

Objective 3 INTEGRATED OPERATIONS 3:a Demonstrate new technology or enhancement to existing technology that streamlines the operational decision-making process throughout the spectrum of military and civil operations, including GWOT contingencies and crisis response. 3.c. Situational awareness using advanced visualization technologies.

Describe how this Objective is met through use of this trial:

The USCG Information Sharing and Communication Solution provides a rapid and secure means of communicating from vessels off shore, to the local command center and anywhere. It solves a long standing problem maintaining communications with boarding teams. It works even when the boarding team is deep within a large ship. It will also provide rapid and secure transmission of biometric data. A portable fingerprint scanner collects biometric data, downloads to a laptop and is securely transmitted

via an encrypted wireless network to a command center. From there it can be passed to higher level operational commanders, other federal government agencies, state and local agencies. The data is then transmitted to a secure fingerprint database and the results will be quickly sent back to the boarding team. This trial will provide a substantial improvement in situational awareness to appropriate command and control entities through a Net centric community of interest (COI).

CWID SubObjective:

Homeland Security

Trial is submitted in support of Homeland Security.

Benefits Provided

This trial demonstrates capabilities that are not currently available within the USCG. It will provide the ability to communicate with boarding teams even when they are deep inside a large ship where normal communications fail. It will also allow boarding teams to collect photos and fingerprints of suspects while on a boarding of a vessel at sea and send them to a shore command over a secure network. This biometric data will then be sent to a large database of data like USVISIT. The results can then be sent back to the boarding team, giving them identification data as well as alerting them if there are any people that are wanted or dangerous. This will enable USCG boarding teams to reduce their reliance on crew manifests which can easily be falsified.

Interoperability

U.S. Trial Partners:

HSIN - Homeland Security Information Network will be used to provide communications between SeaHawk in Charleston and the CWID network. The Homeland Security Information Network is a computer-based counterterrorism communications system connecting all 50 states, five territories, Washington, D.C., and 50 major urban areas. The Homeland Security Information Network (HSIN) allows all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism.

Coalition Trial Partners:

Trial will support additional partners if requested.

(This page intentionally left blank.)

APPENDIX D. CWID TRIAL 3.58 DATA FLOW DIAGRAM

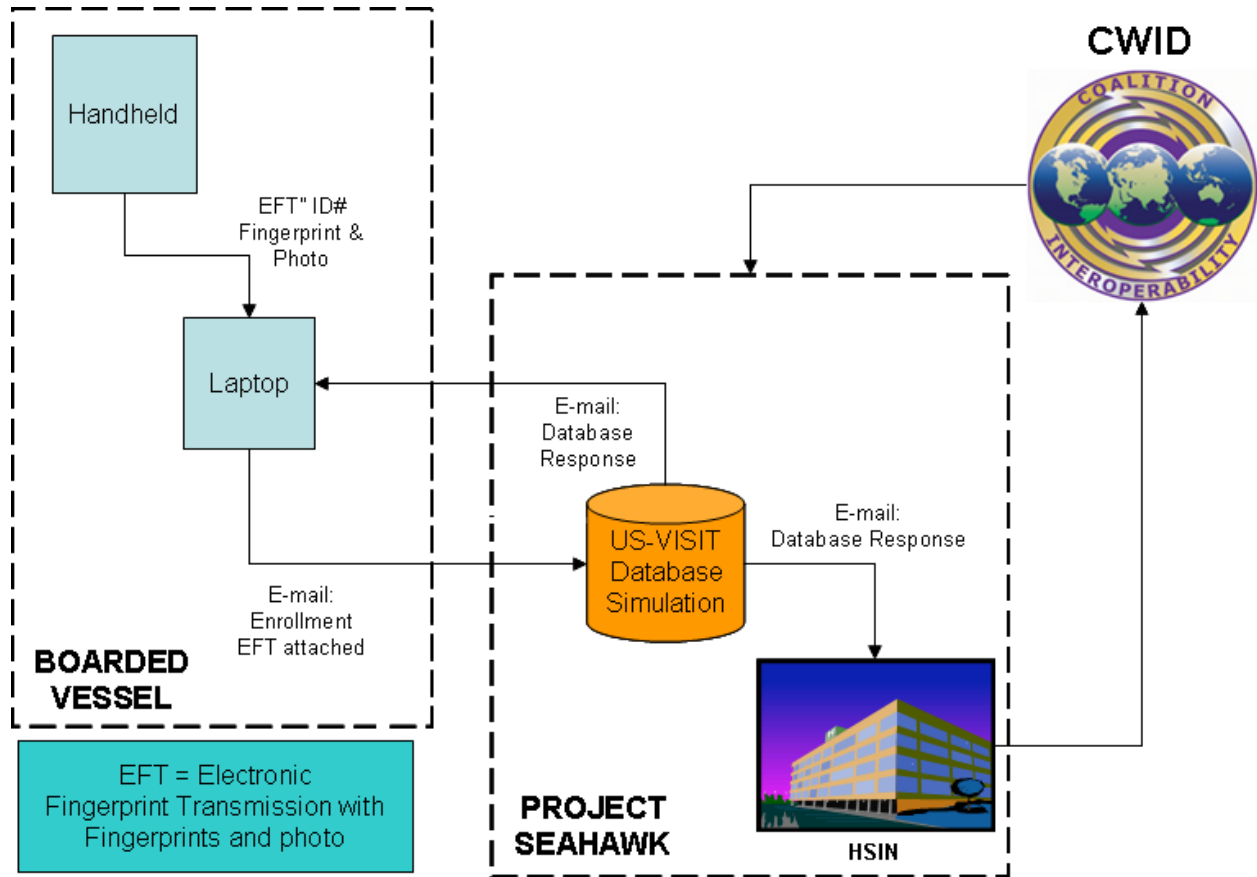


Figure D-1. Data flow diagram: IT 3.58.

(This page intentionally left blank.)

APPENDIX E. CWID TRIAL 3.58 OPERATIONAL OVERVIEW

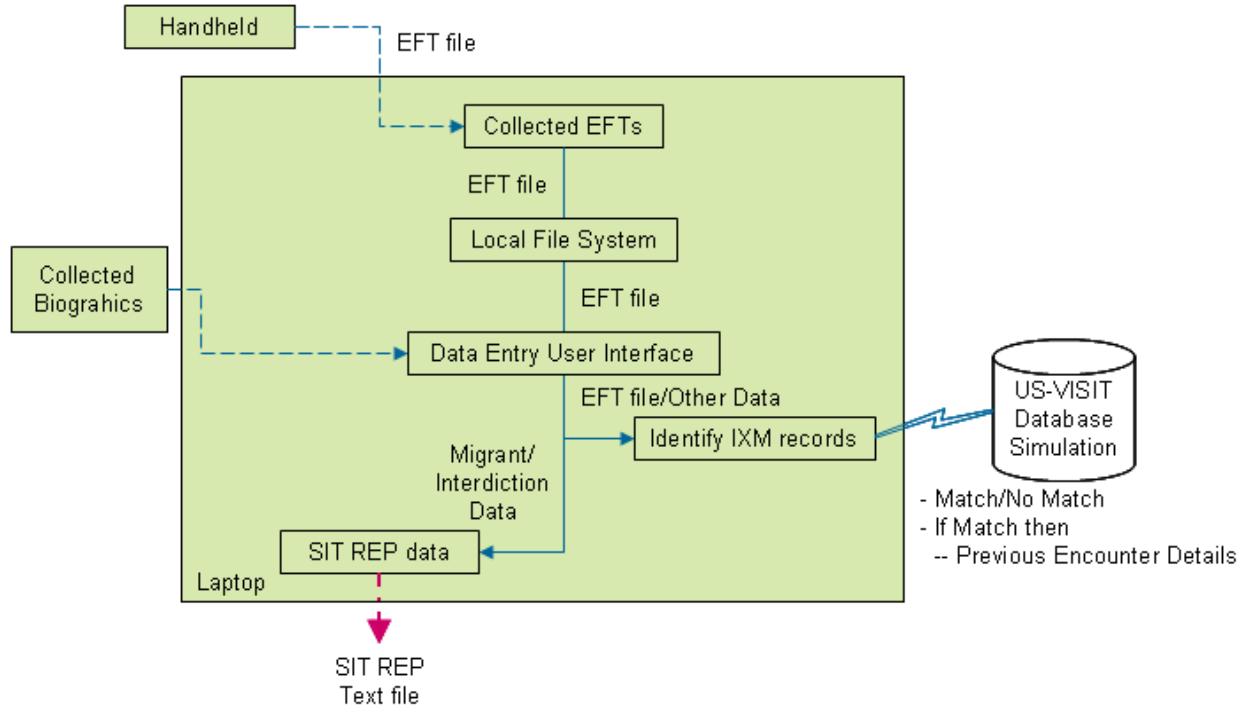


Figure E-1. Operational view-1: IT 3.58.

(This page intentionally left blank.)

APPENDIX F. CWID TRIAL 3.58 PROCESS FLOW

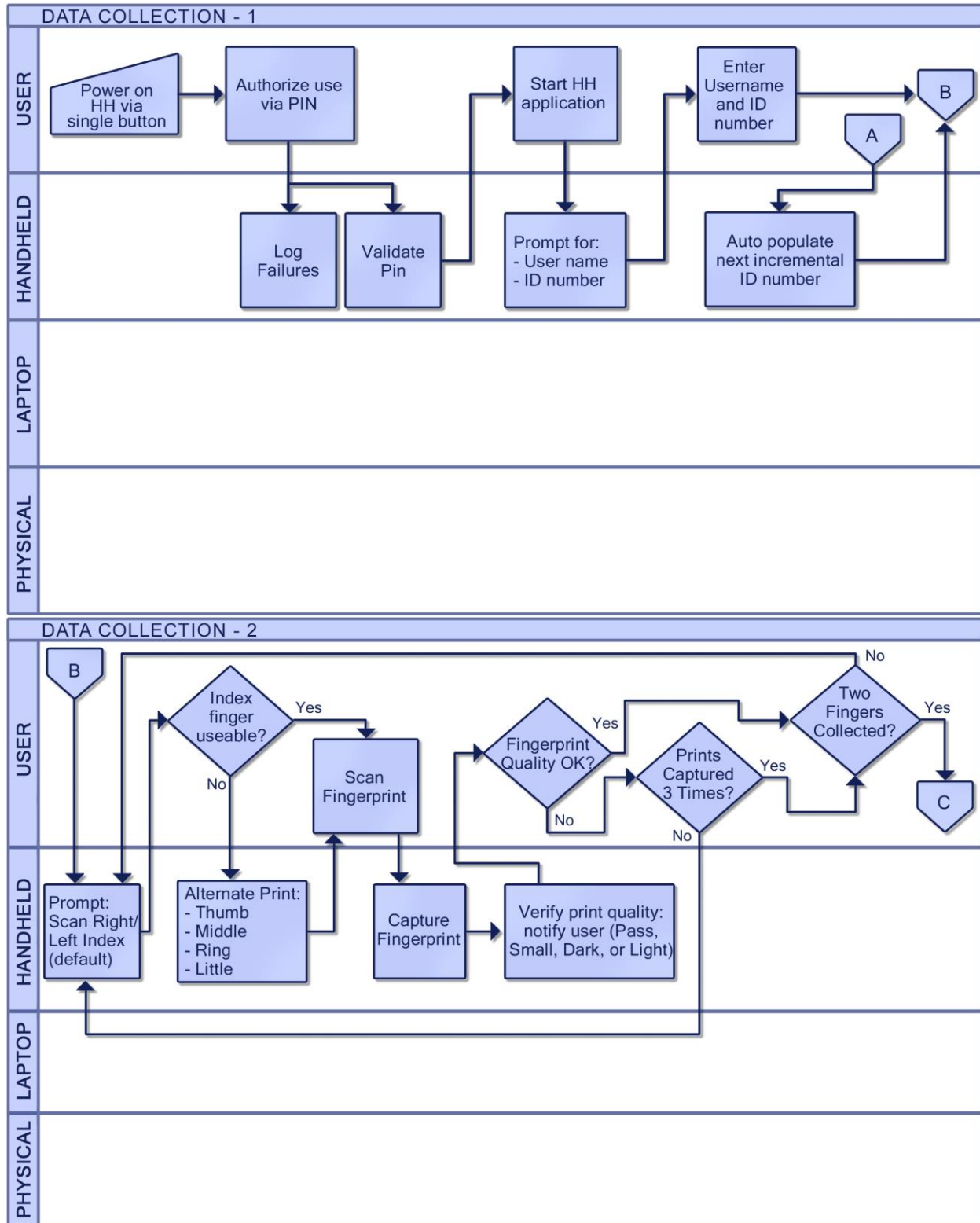


Figure F-1. Operational view-5: IT 3.58 process flow.

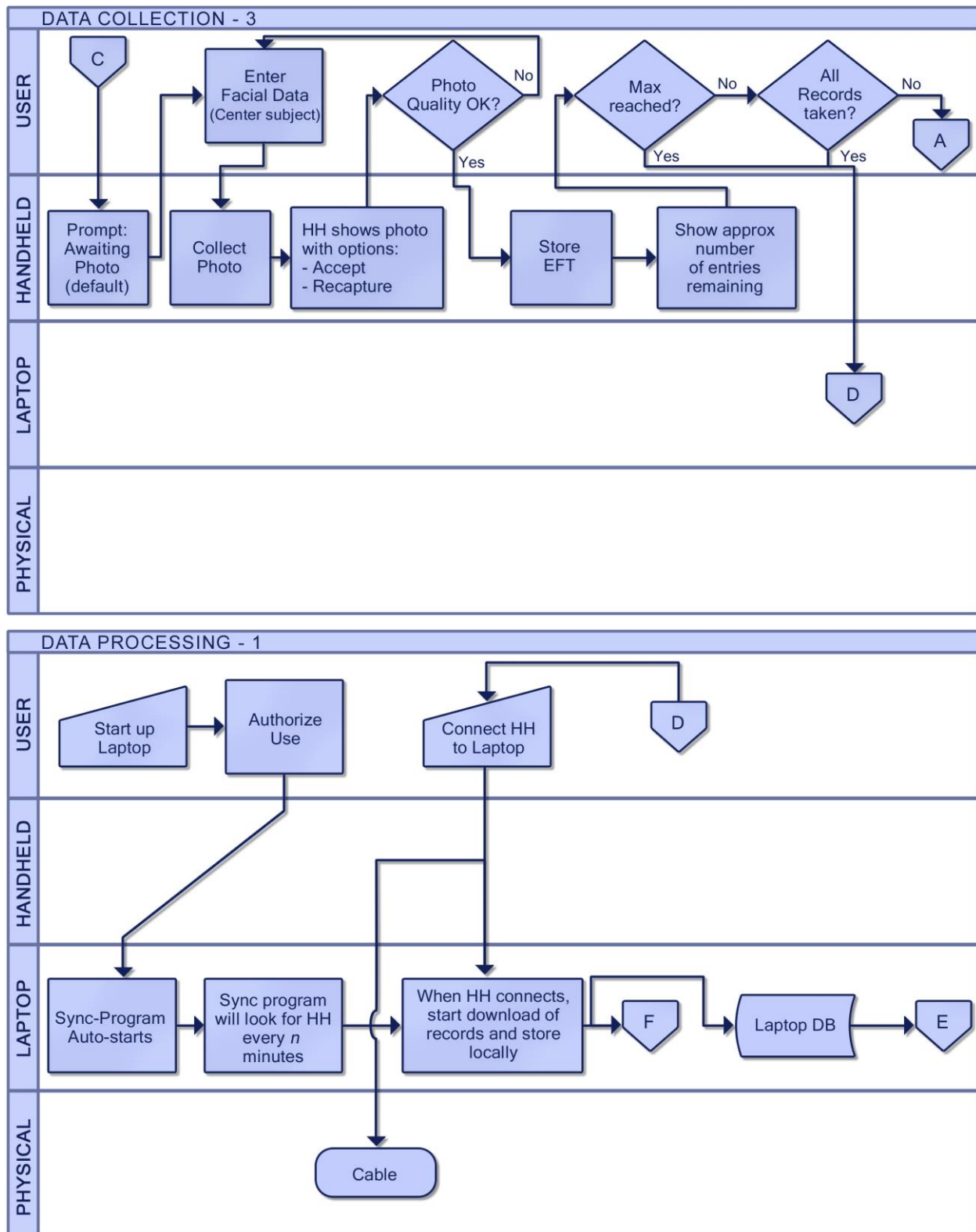


Figure F-1. Operational view-5: IT 3.58 process flow (continued).

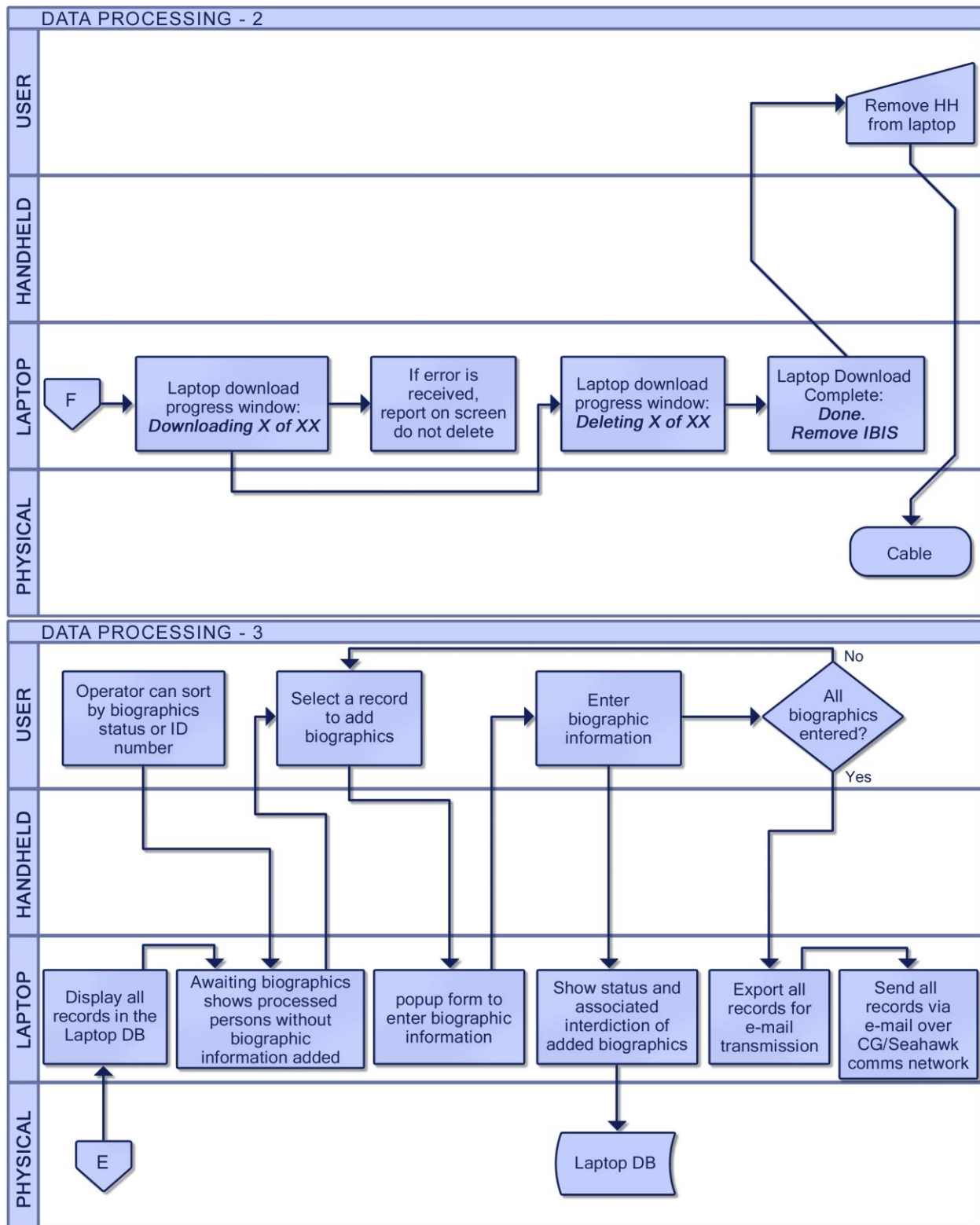


Figure F-1. Operational view-5: IT 3.58 process flow (continued).

(This page intentionally left blank.)

APPENDIX G. CWID TRIAL 3.58 BIOMETRICS ARCHITECTURE

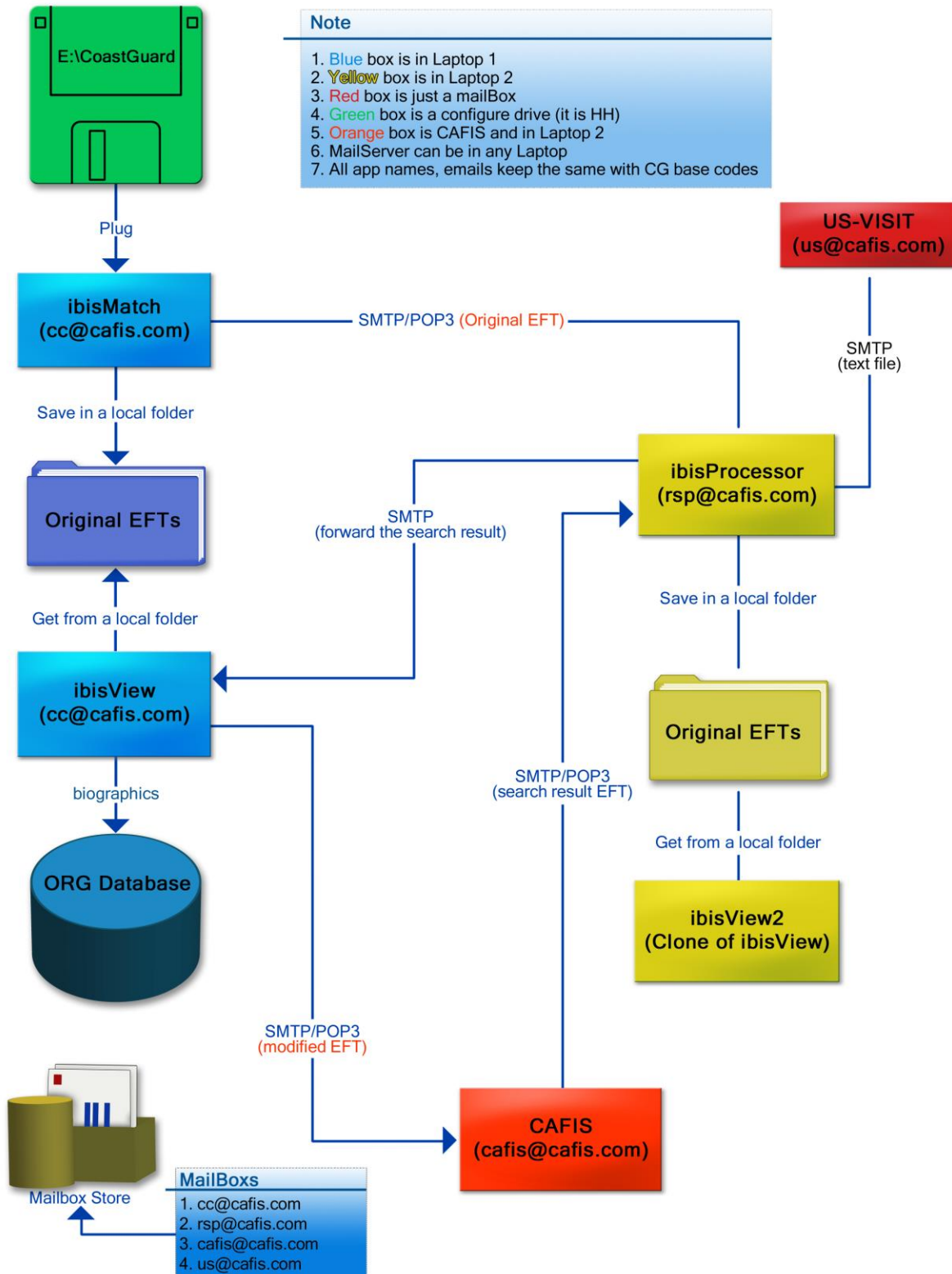


Figure G-1. Biometrics architecture: IT 3.58.

(This page intentionally left blank.)

APPENDIX H. CWID TRIAL 3.58 CAPABILITIES & FUNCTION WORKSHEET

H.1 Capabilities

The Trial Capabilities are the expected Government or agency benefits which the Interoperability Trial intends to demonstrate. Trial Capabilities are the essence of Warfighter evaluation (i.e., capabilities = sub-objectives documented in the Federal Business Opportunity). Trial capabilities are demonstrated through the execution of the Trial's functions. Every Master Scenario Event List (MSEL) event will directly map to specific Trial Capability.

H.2 Function

A Trial Function refers to tasks that a trial must perform in order to completely demonstrate a capability. To properly demonstrate a capability a trial operator may be required to perform several sequential "Functions" to create products or provide services that will fully demonstrate the trials capabilities.

Enter the CWID Objective that your trial is addressing as it appears in the Federal Business Opportunity (FBO announcement (use a separate workbook for each objective)		
Objective 3 INTEGRATED OPERATIONS Enhance the commander's capability to command, control and coordinate across joint and coalition forces, government agencies, NGOs, and first responders.		
Capability # 1: Identify each capability (i.e., subobjective) that your trial will demonstrate to properly satisfy the CWID Objective identified above. <i>Note: A trial may need to demonstrate one or more capabilities to adequately address the CWID Objective. Each capability should be addressed associated to the CWID Objective listed above. Use Additional worksheets as required.</i>		
3:a Demonstrate new technology or enhancement to existing technology that streamlines the operational decision-making process throughout the spectrum of military and civil operations, including GWOT contingencies and crisis response.		
Functions required to demonstrate the capability listed above. List the system functions that must be performed to demonstrate the capability listed above. Add additional Function entries as necessary	Data Characteristics: If the function being performed requires or results the exchange of information (data) between your trial and an external entity, identify each type of data being transferred in support of this function (i.e., email, email with attachment, imagery, MS Word Documents, track data (land maritime, air), Graphics, briefings, Voice Over IP (VOIP), etc.	Number of repetitions of this function required to adequately assess
Function # 1:		
Use Ad Hoc Wireless Mesh Network to transfer voice communications and E-mails with or without attachments from teams located beyond radio contact.	Voice / E-mail with MS Word, JPEG, EFT, and WAV/MPEG attachments	5

Function # 2:		
Post MSWord Situation Report and attachments to MDA Community of Interest (MDA COI) page in Homeland Security Information Network (HSIN) for review by CWID network.	MSWord report with MS Word, JPEG, WAV/MPEG, EFT, and Voice attachments	5
Function # 3:		
Post Automatic Identification System (AIS) tracks to MDA Community of Interest (MDA COI) page in Homeland Security Information Network (HSIN) for viewing by CWID network.	E-mail / Track Data (Maritime)	2
Function # 4:		
Use biometric technology to collect photo and fingerprints.	EFT and JPEG files	2
Function # 5:		
Add biographic data to collected biometrics	RTF files	2
Function # 6:		
Transmit biometric and biographic data to simulated USVisit database	E-mail with EFT, JPEG, & RTF attachments	2
Function # 7:		
Receive HIT/NO HIT E-mail from simulated US Visit database	E-mail with JPEG & RTF attachments	2
Function # 8:		
Function # 9:		
Function # 10:		
Capability # 2: Identify each capability (i.e., subobjective) that your trial will demonstrate to properly satisfy the CWID Objective identified above. <i>Note: A trial may need to demonstrate one or more capabilities to adequately address the CWID Objective. Each capability should be addressed associated to the CWID Objective listed above. Use Additional worksheets as required.</i>		

3.c. Situational Awareness using advanced visualization technologies.		
Functions required to demonstrate the capability listed above. List the system functions that must be performed to demonstrate the capability listed above. Add additional Function entries as necessary	Data Characteristics: If the function being performed requires or results the exchange of information (data) between your trial and an external entity, identify each type of data being transferred in support of this function (i.e., email, email with attachment, imagery, MS Word Documents, track data (land maritime, air), Graphics, briefings, Voice Over IP (VOIP), etc.	Number of repetitions of this function required to adequately assess
Function # 1:		
Post report and video attachments to MDA Community of Interest (MDA COI) page in Homeland Security Information Network (HSIN) for viewing by CWID network.	MSWord or E-mail with JPEG and WAV or MPEG attachments	2
Function # 2:		
Function # 3:		
Function # 4:		
Function # 5:		
Function # 6:		
Function # 7:		
Function # 8:		
Use HSIN Maritime COI on Portal to coordinate cooperation for response and consequence management of SD truck bomb. (MSEL 267)	Transfer between: USCG cutter, LNO, and District and anyone on portal Data transferred: IM, email(s), messages, reports Method used for transfer: HSIN	2
Function # 9:		
Function # 10:		

Capability # 3: Identify each capability (i.e., subobjective) that your trial will demonstrate to properly satisfy the CWID Objective identified above.

Note: A trial may need to demonstrate one or more capabilities to adequately address the CWID Objective. Each capability should be addressed associated to the CWID Objective listed above. Use Additional worksheets as required.

Functions required to demonstrate the capability listed above. List the system functions that must be performed to demonstrate the capability listed above. Add additional Function entries as necessary	Data Characteristics: If the function being performed requires or results the exchange of information (data) between your trial and an external entity, identify each type of data being transferred in support of this function (i.e., email, email with attachment, imagery, MS Word Documents, track data (land maritime, air), Graphics, briefings, Voice Over IP (VOIP), etc.	Number of repetitions of this function required to adequately assess
Function # 1:		
Function # 2:		
Function # 3:		
Function # 4:		
Capability # 4: Identify each capability (i.e., subobjective) that your trial will demonstrate to properly satisfy the CWID Objective identified above.		
<i>Note: A trial may need to demonstrate one or more capabilities to adequately address the CWID Objective. Each capability should be addressed associated to the CWID Objective listed above. Use Additional worksheets as required.</i>		
Function # 1:		
Function # 2:		
Function # 3:		
Function # 4:		
Function # 5:		

APPENDIX I. CWID TRIAL 3.58 TRAINING PLAN



Prepared by: John Davin

Potomac Management Group, Inc.,
a division of Advanced Technology Systems, Corp.
7915 Jones Branch Drive
McLean, VA 22102

I.1 SCOPE

The purpose of the warfighter/operator training plan is to identify the Coalition Warrior Interoperability Demonstration (CWID) 2007 training objectives, present the training curriculum, time estimates for execution of the training curriculum, and the persons who require training.

I.2 OBJECTIVE

The training program will train the warfighter/operator on how to access the email system that will be used to receive the information and will be able to execute Master Scenario Event Lists (MSEL) with ease and full comprehension. The training during execution will cover familiarization with the trial capabilities so participants can effectively and efficiently perform their assigned duties and responsibilities (i.e., execute MSELs with ease and full comprehension).

I.3 TRIAL OVERVIEW

The Information Sharing and Communications Solution provides a rapid and secure means of communicating from vessels off shore, to the local command center and anywhere via the internet. It solves a long standing problem maintaining communications with boarding teams. It works even when the boarding team is deep within a large ship. It will also provide rapid and secure transmission of biometric data. A portable fingerprint scanner collects biometric data, downloads to a laptop and is securely transmitted via an encrypted wireless network to a command center. From there it can be passed to higher level operational commanders, other federal government agencies, state and local agencies. The data is then transmitted to a secure fingerprint database and the results will be quickly sent back to the boarding team. This trial will provide a substantial improvement in situational awareness to appropriate command and control entities through a Net Centric Community of Interest (COI). The trial will be observed at three locations: NORTHCOM, Dahlgren, and Wellington, NZ.

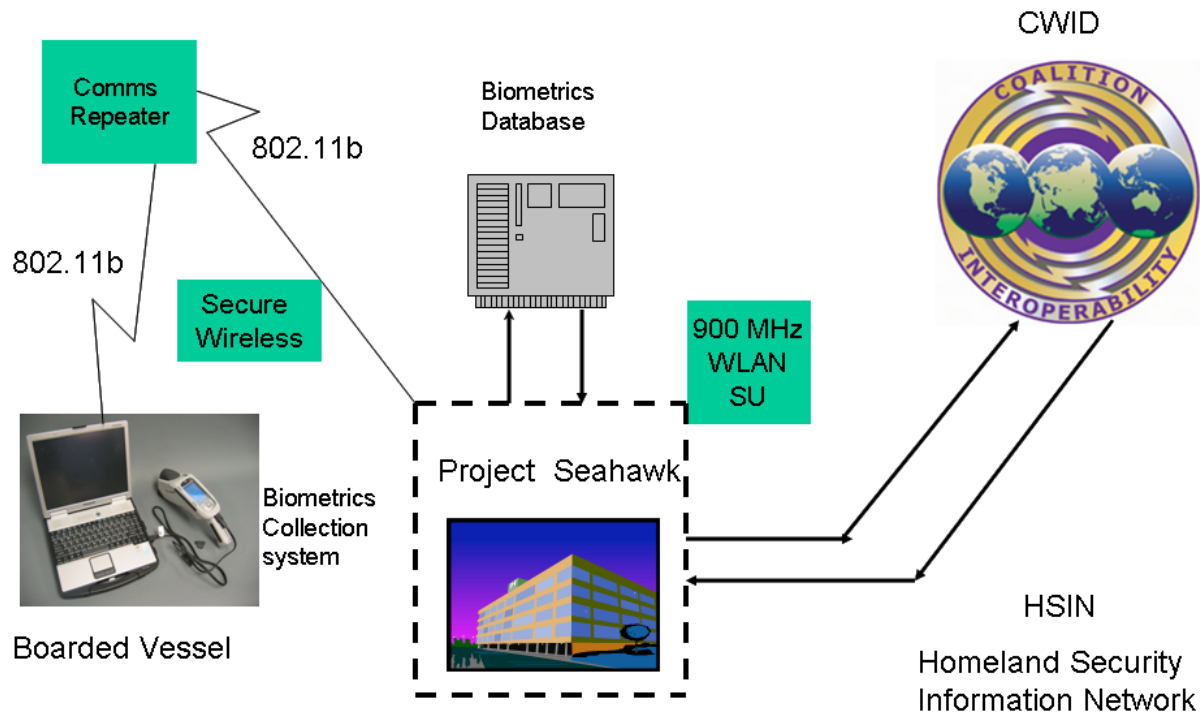


Figure I-1. USCG information sharing and communication solution.

I.4 TRAINING TEAM AND PARTICIPANTS

Training will be provided by the U.S. Coast Guard (USCG) Information Sharing & Communication (IS&C) Team. Operator and Warfighter will be provided at Dahlgren for the role players from Dahlgren and NORTHCOM during the training and set up period. This training will also be provided to remote participants in Wellington by written instructions sent via email and land line telephone call.

I.4.1 Target Population

One to two hours of operator training for warfighters and role players at Dahlgren, NORTHCOM and Wellington is expected. Role players to be trained will include:

- U.S. Coast Guard Liaison Officer NORTHCOM
- U.S. Coast Guard Area CDO – Dahlgren
- U.S. Coast Guard District CDO – Dahlgren
- DHS NOC Duty Officer – Dahlgren
- SeaHawk CDO – SeaHawk Charleston, SC
- USCG Boarding Team Leader - SeaHawk Charleston, SC

I.4.2 Warfighter/Operator Recommendations and Limitations

Warfighters/operators and role players need only to possess basic computer operational skills and understand computer security requirements.

I.5 INSTRUCTIONAL STRATEGY

Training will be over the shoulder (hands-on) type using the actual data provided for the demonstration. Training for New Zealand personnel will be via PowerPoint presentation.

I.6 COURSE CONTENT

Course content will consist of a theory of operations, a brief demonstration by the instructor, and a hands on session with the instructor present. Level of instruction will be the same for all operators.

I.6.1 Teaching Points

Operators will not perform any analysis of the files. Operator is only required to access files. File transfer will take place using email.

I.6.2 Training Materials

Training material will include power point slides and hands-on exercises.

I.7 REQUIRED RESOURCES

Existing CWID workstations (hardware/software) will be used to provide training. No additional hardware or software will be required.

I.8 TECHNICAL SUPPORT

On-site technical representatives will be present during integration (set-up), training and 2 weeks of execution.

APPENDIX J. CWID 2007 PARTICIPANTS

USCG IT 3.58 Information Sharing and Communications

J.1 USCG Participants

NAME AFFILIATION	SITE	ROLE
CDR Jim Marchese USCG NORTHCOM	NORTHCOM	USCG LNO
LCDR Stacie Fain USCG NORTHCOM	NORTHCOM	USCG LNO
CDR Rich Guba, USN Department of Homeland Security	NSWC-DD	DHS NOC
LCDR Rich Sundland USCG COMDT (CG-37RCC-2)	NSWC-DD	JHOC USCG
LT Josh Jarrell USCG COMDT (CG-37RCC-2)	NSWC-DD	USCG Area/District CDO
LT Andre Whidbee USCG COMDT (CG-37RCC-2)	NSWC-DD	USCG Sector CDO
Buddy Hartberger USCG COMDT (CG-926)	NSWC-DD	USCG CWID Sponsor
Hank Blaney USCG COMDT (CG-523)	NSWC-DD & SeaHawk Charleston	Scenario & Master Scenario Event List (MSEL) development USCG CWID Coordinator
Jack Davin USCG COMDT (CG-523/ATS Inc.)	NSWC-DD & SeaHawk Charleston	USCG CWID Coordinator
OSC Timothy Clutter USCG Sector Charleston	SeaHawk Charleston	SeaHawk CDO
OSC Charlie Hinds USCG Sector Charleston	SeaHawk Charleston	SeaHawk CDO
PS1 William Simpson USCG Sector Charleston	SeaHawk Charleston	SeaHawk CDO
BM1 Gerald Shirmer USCG Sector Charleston	SeaHawk Charleston	SeaHawk Boarding Team 2 Leader
GM2 Torre Vickers USCG Sector Charleston	SeaHawk Charleston	SeaHawk Boarding Officer Team 1
MK2 Michael Sellers USCG Sector Charleston	SeaHawk Charleston	SeaHawk Boarding Officer Team 1
GM3 Ryan Anderson USCG Sector Charleston	SeaHawk Charleston	SeaHawk Boarding Officer Team 2

J.2 USCG Research and Development Center (R&D Center) Participants

NAME AFFILIATION	SITE	ROLE
Kathy Shea USCG R&D Center	NSWC-DD	RDC Coordinator
Jim Fletcher USCG R&D Center	SeaHawk Charleston	Boarding Team Comms
Jay Spalding USCG R&D Center	SeaHawk Charleston	MDA/COI
Dr. Joan Silver USCG R&D Center	SeaHawk Charleston	Boarding Team Comms
David Beene USCG R&D Center	SeaHawk Charleston	Boarding Team Comms
LT Mike Chien USCG R&D Center	SeaHawk Charleston	Boarding Team Comms
LTjg Mario Teixeira USCG R&D Center	SeaHawk Charleston	Biometrics
Dr. Thomas Amerson USCG R&D Center	SeaHawk Charleston	Biometrics
John Mcleod USCG R&D Center	SeaHawk Charleston	Boarding Team Comms

J.3 Project SeaHawk Participants

NAME AFFILIATION	SITE	ROLE
Capt Scott Beeson USCG	SeaHawk	Support
John Buechele SeaHawk	SeaHawk	Support
Bart Coghill SCRA	SeaHawk	IT Support
Alistair Nicole SAIC	SeaHawk	IT Support
Ethan Walker SeaHawk	SeaHawk	IT Support
Lane Melton SeaHawk	SeaHawk	Support
Buddy Mcalister SCRA	SeaHawk	IT Support
Ed Phumphrey SeaHawk Charleston	SeaHawk Charleston	SeaHawk Boarding Team 1 Leader
Earl Graham SeaHawk Charleston	SeaHawk Charleston	SeaHawk Boarding Team 2 Leader

J.4 Contractor Participants

NAME AFFILIATION	SITE	ROLE
Randy Sundberg SAIC	SeaHawk	Contractor Coordinator
Mohammed Kaloko SAIC	SeaHawk	Biometrics
Stephen Rigdon SAIC	SeaHawk	Support
Matthew O'Brien SAIC	SeaHawk	MDA
Christina O'Loughlin SAIC	SeaHawk	Biometrics
Sang An SAIC	SeaHawk	Biometrics
Zora Siemasko SAIC	Washington, DC	Biometrics
Mike Doyle TKC Technology	SeaHawk	Boarding Team Comms
Alex Remoly SAIC	SeaHawk	Biometrics
Babak Amin SAIC	Washington, DC	MDA
Dick Shaw SAIC	SeaHawk	Support
Wally Reddington SAIC	SeaHawk	Boarding Team Comms & Biometrics
Jim Harmon SAIC	SeaHawk	MDA
Matt Moraux SAIC	SeaHawk	Boarding Team Comms
Brian Hannagan SAIC	Washington, DC	Portal
Beth Gorko GDIT	USCG Headquarters	HSIN Support
Guy Varlund SI International	Washington, DC	Software Animation

(This page intentionally left blank.)

APPENDIX K. SAIC TRIP REPORT FOR DAHLGREN, VA



28 June 2007

Commanding Officer
U.S. Coast Guard
Research and Development Center
1082 Shennecossett Road
Groton, CT 06340-6096
(ATTN: Ms. Kathleen Shea, kathy.k.shea@uscg.mil)

Subj: Trip Report for Dahlgren VA for CWID Execution and VIP demonstrations.

Dear Ms. Shea,

The Dahlgren VA trip report is forwarded in accordance with the requirements of Delivery Order HSCG32-07-J-100024 under Contract HSCG32-05-D-R00010.

The Coalition Warrior Interoperability Demonstration (CWID) Dahlgren set up, execution, and VIP demonstrations were conducted June 7, June 13-15 and June 18-21, 2007 in the Dahlgren CWID facilities.

The following people participated in these trips:

USCG R&D Center: Kathy Shea, LT Michael Chen, and LTJG Mario Teixeira.

USCG Headquarters: Hank Blaney

SAIC: Christy O'Loughlin and Matt Regan. (Subject Matter Experts (SME))

COCO: Mr. Chung

PMG: Jack Davin

The following is a summary of the CWID Dahlgren set up, execution, and VIP demonstrations:

Thursday June 7, 2007, CWID Dahlgren set up and training day.

- Successfully delivered all BT Comms, Biometrics, and MDA equipment to Dahlgren and the appropriate laptops were scanned for network connection.
- Set up Dahlgren staging area, all laptops were connected to the Dahlgren internet connection, and assigned static IP addresses.

- Worked with the Coast Guard operational personnel performing the CWID MSEL activities and conducted the VIP briefings during the two weeks of demonstrations.
- Using the training materials SAIC developed, we trained the CG operational personnel on the proper operation of the biometrics equipment.

Wednesday June 13, 2007, first day of Dahlgren demonstrations and VIP briefings.

- Prepared and set up biometrics equipment for VIP tours and demonstrations.
- Pre-populated biometrics equipment screen to facilitate the short time frame of the VIP briefings (Only allowed 5 minutes for MDA, Biometrics and BT Comms combined).
- The BT Comms was set up at Dahlgren and received voice and some video from CWID Charleston.
- VIP demonstrations were conducted at 0830, 1030, and 1230 throughout the day according to schedule. The last tour did not arrive in the Dahlgren CWID CG Operations Center until 1430.
- All VIP presentations went smooth with minor SME support necessary.

Thursday June 14, 2007, second day of Dahlgren demonstrations and VIP briefings.

- Ensured all equipment was still configured for demonstrations.
- Answered basic SME questions and answered all CG operators' questions as they used the biometrics system.
- Tours were initiated as scheduled with the last one entering the Dahlgren CWID CG Operations Center at 1445.

Friday June 15, 2007, third day of Dahlgren demonstrations and VIP briefings.

- Answered basic SME questions and answered all Coast Guard operators' questions as they used the system.
- The CG operators were able to comfortably give the demonstrations and all equipment functioned properly.
- Tours were initiated as scheduled with the last one entering the Dahlgren CWID CG Operations Center at 1445.

Monday June 18, 2007, forth day of Dahlgren demonstrations and VIP briefings.

- SAIC SMEs were not requested at Dahlgren this day. LTJG Teixeira filled the Biometrics SME position.
- Posters of each technology and slick/informational sheets were delivered to and displayed at CWID Dahlgren.
- VIP demonstrations were initiated at 0830, 1030, and 1230 throughout the day according to schedule.

Tuesday June 19, 2007, fifth day of Dahlgren demonstrations and VIP briefings.

- Before the SAIC SME representative relieved LTJG Teixeira, they took the tour to examine what other technologies were being displayed during CWID.
- Answered basic SME questions for VIPs touring Dahlgren.
- Gathered information on other project participating in CWID. This information was also collected in hard copy and can be provided to the RDC upon request.

Wednesday June 20, 2007, sixth day of Dahlgren demonstrations and VIP briefings.

- Answered all SME questions for VIPs touring Dahlgren.
- ADM Parker and ADM Glen (CG Flag officers) toured Dahlgren to see CG Operations Center demonstrations. The Admirals were able to see live video and audio from the BT Comms system from CWID Charleston.
- Answered specific CG flag officer questions and gave more detailed information on the various technologies during their tour.
- Provided detailed information to those VIPs that requested additional information.

Thursday June 21, 2007, final day of CWID Dahlgren demonstrations and VIP briefings.

- No SAIC SME representation at Dahlgren. All CG operators were comfortable with the biometrics presentation and they were able to perform all VIP briefings independently.

Please contact me should you have any questions or require any additional information.

Very Truly Yours,

A handwritten signature in black ink, appearing to read "Stephen Rigdon". The signature is fluid and cursive, with the first name "Stephen" written in a larger, more prominent script than the last name "Rigdon".

Stephen Rigdon, Program Manager

(This page intentionally left blank.)

APPENDIX L. SAIC TRIP REPORT FOR CHARLESTON, SC SITE SURVEY



25 May 2007

Commanding Officer
U.S. Coast Guard
Research and Development Center
1082 Shennecossett Road
Groton, CT 06340-6096
(ATTN: Ms. Kathleen Shea, kathy.k.shea@uscg.mil)

Subj: Trip Report for Charleston SC Site Survey and Boarding Team (BT)
Communications/Biometrics Test & Evaluation (T&E)

Dear Ms. Shea,

The Charleston SC trip report is forwarded in accordance with the requirements of Delivery Order HSCG32-07-J-100024 under Contract HSCG32-05-D-R00010.

The Coalition Warrior Interoperability Demonstration (CWID) site survey and Boarding Team Communications/Biometrics Test and Evaluation (T&E) was conducted May 14-18, 2007 on the Federal Law Enforcement Training Center's (FLETC) training ship *CAPE CHALMERS* and at the Department of Justice's (DOJ) *SEAHAWK* Task Force offices in Charleston South Carolina.

The following people participated in this trip:

USCG R&D Center: Jim Fletcher and Dave Beene

SAIC: Randy Sundberg, Sang An, Mohamed Kaloko, Lihua Shen, Dick Shaw, Alistair Nicol, and Mat Moraux.

TKC: Mike Doyal

COCO: Joel Reiter

The following is a summary of the CWID Charleston site survey and BT Comms/Biometrics T&E:

- **Monday May 14, 2007**, the out of town people traveled to Charleston SC.
- All BT Comms and Biometrics equipment was successfully scanned by SeaHawk.
- The SeaHawk staging area was established and all equipment was placed on chargers.

- We worked with the SeaHawk Planning Officer to identify the SeaHawk Task Force Officers (TFO's) who will also participate in the CWID boarding. They identified (2) TFOs to participate during the June activities.
- We borrowed some XTS-5000 secure radios from the Coast Guard SeaHawk Vessel Boarding Search Team (VBST) and in the process they volunteered to be the CG boarding team during CWID. They're going to provide (4) Coasties for the CWID Training June 6-7 and then (2) will participate June 13-14 and the other (2) will participate June 20 & 21.
- **Tuesday May 15, 2007**, everyone gathered at the SeaHawk staging area and we conducted a safety/planning meeting before moving to the *CAPE CHALMERS*.
- Once on the ship we showed everyone the locations we would be using and established a staging area in the Captain's Lounge.
- The BT Comms repeaters were deployed in the ship's bridge wing, bridge stairwell, main passageway, engine room stairwell, engine room, shaft alley, aft steerage, aft main deck, center main deck, and on the pier next to the ship.
- The BT Comms mesh network was up and running before noon.
- The BT comms had problems linking into the SeaHawk 900 MHZ Wireless network, but most of the problems were corrected by 1800 and the remaining problems were fixed by 1000 Wednesday morning.
- **Wednesday May 16, 2007**, we re-deploy the BT Comms network and the Biometrics Team successfully passed finger print files to the Toughbook in SeaHawk through the SeaHawk 900 MHZ wireless system.
- Wednesday afternoon we tried to send the fingerprint files again, but it didn't work and it was determined the Cogent software doesn't work if the system has multiple Host ID's (Laptop's, Wireless Card's, etc.).
- We tried to use a third laptop to act as a jumper so the system only sees one Host ID, but it still didn't work.
- **Thursday May 17, 2007**, the teams were able to get the systems operating properly if they used a specific activation sequence so Cogent can properly identify the Toughbook's Host ID.
- Thursday afternoon we deployed the BT Comms and Biometrics system on the ship and successfully transmitted the fingerprint files, received a match, and transmitted the results back to the Toughbook on the ship using the BT Comms and SeaHawk 900 MHZ wireless system.
- We held a CWID debrief to identify lessons learned and action items when we return to Charleston June 5-8 for the final set-up and training.
- The SeaHawk staging area was packed up, cleaned, and the BT Comms equipment was shipped back to the R&D Center using the Naval Engineering Support Unit's (NESU) shipping and receiving.
- During the week we also identified some MDA Data Sharing reliability problems and the subject matter experts (SMEs) are not sure if they can be corrected before the June CWID demonstration. Jay Spalding, Matt Regan, and Alistair Nicol are all working on solutions to the problems. SeaHawk personnel's big concern is things will stop once CWID is over.

- We identified (3) CWID role players who will participate in our June activities. We provided CPO Charlie Hines, CPO Tim Clutters, and PO1 Bill Simpson with the HSIN registration instructions and briefed them on the June CWID activities.
- We also met with the Global Personnel Recovery System (GPRS) CWID trial personnel that CDR Chris Bartz (G-RCC) told us about in April. They now want to move from Sector Charleston to SeaHawk so the VIPs only have one place to visit. They are going to join our SeaHawk staging area and will plug a laptop with FalconView™ into SeaHawk's network system too. (There can only be (4) computers plugged into the SeaHawk network and with the GPRS laptop we now have (3) computers connected to their system.)
- **Friday May 18, 2007**, the personnel from out of town traveled back to their respective locations and started working on their action items.

Please contact me should you have any questions or require any additional information.

Very Truly Yours,

A handwritten signature in cursive script that reads "Stephen Rigdon".

Stephen Rigdon, Program Manager

(This page intentionally left blank.)

CWID 2007 US COAST GUARD TRIAL 3.58: INFORMATION SHARING AND COMMUNICATIONS



USCG OBJECTIVES

- 1. Demonstrate ability to exchange a variety of data/information between USCG assets (ships) with sector command (SeaHawk) and external to USCG (DHS, NORTHCOM, CWID) by transmitting:
 - Voice
 - Biometric data (fingerprints)
 - Video

USCG OBJECTIVES

2. Demonstrate ability to exchange AIS track and vessel information between sector command (SeaHawk) and external to USCG (DHS, NORTHCOM, CWID) to increase Maritime Domain Awareness.

USCG LOCATIONS

SeaHawk Charleston, SC – equipment deployed for trial

Role player watchstanders:

NSWC Dahlgren, VA

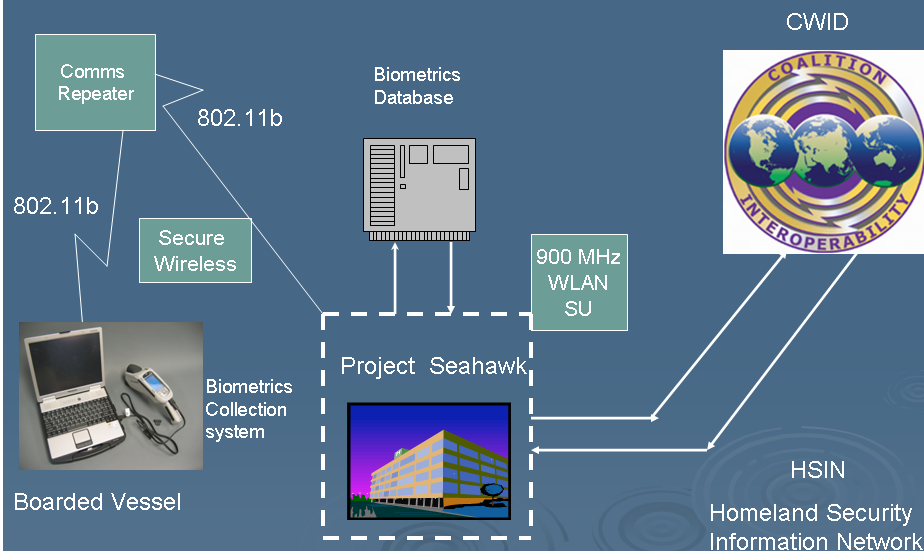
NORTHCOM, Colorado Springs, CO

Wellington, New Zealand

USCG PARTNERS

- USCG Headquarters – CG-66 & CG-523
- USCG Research & Development Center (RDC), Groton, CT
- SeaHawk Charleston, SC
- USCG Sector Charleston, SC

USCG Information Sharing and Communication Solution



Laptop

- Panasonic Toughbook-74's as a standalone system running Cogent fingerprint matching software. Migrants will be identified as "hit"/ "no hit" against biometric datasets that are on the laptop.



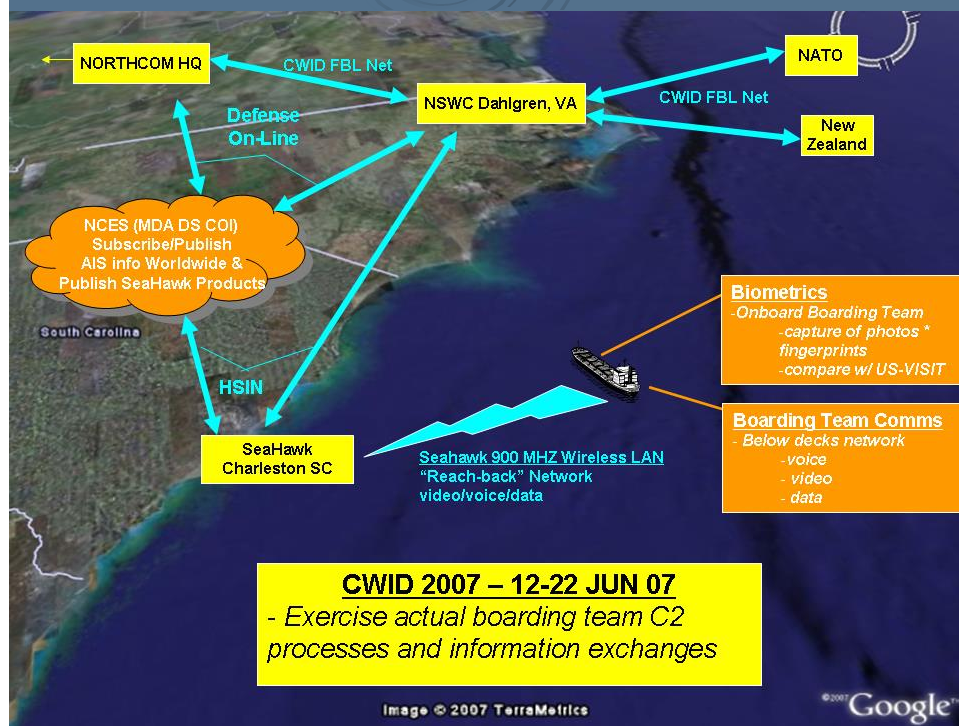
Handheld

- The Identix IBIS is the collection device to be used on each of the cutters.



Wireless Network

- Wireless network 802.11B
- Secure - encrypted with mCRG w/EV-DO
- Connected to SeaHawk 900 MHz LAN



(This page intentionally left blank.)

APPENDIX N. SAIC CWID BIOMETRICS TEST PLAN

Laptops:

Handheld:

N.1 Introduction

The execution of this Test Plan and Descriptions will be used by SAIC to demonstrate that the USCG Coalition Warrior Interoperability Demonstration Proof of Concept System meet requirements and functions as proposed and have been correctly implemented. The test plan is used to define, organize, and schedule the upcoming test effort while the test descriptions include details of functions to be tested by the SAIC team during the test execution period during system updates.

N.2 Test Descriptions

N.2.1 USCG handheld tests

Test #	Test Name	Test Description
4.1.1	Capture Validation	Demonstrate ability to capture required data on handheld device
4.1.2	Additional feature Validation	This test will confirm the handheld devices ability to ensure the ID used is the proper length, the correct finger selected is stored in EFT file and the device conducts rudimentary image quality checks of the fingerprint images

N.2.2 CWID laptops pre Tests with COCO software installed

Test #	Test Name	Test Description
3.2.1	COCO Team will configure COCO software in both Laptops	COCO Team will configure software
3.2.2	IP configuration on both laptops with COCO configuration	IP address will be assigned by COCO Software installation Team. Team will update Encryption key every 12 days after updating IP address will change.
3.2.3	Start up Laptops without wireless card inserted	Test to Validate host ID. Laptop host ID is first by using Cogent Host id Utilities to meet CAFIS host ID requirements. Make sure all Application is running properly
	Insert Linksys Wireless interface card	COCO software will establish communication link between the two laptops.
	Open a CMD window to send a ping to the other Laptop.	If COCO channel is working properly both Laptops will communicate with each other.

N.2.3 CWID laptops Test

After laptops pre test successful, and e-mail communication is established. There are three ways of communication from the cutters to the shore.

- *One by sending e-mail from one laptops by suing e-mail address cwid1@cafis.com and cwid2@cafis.com*
- *Push to talk by using COCO communication software*
- *Using personal cell phones*

Test #	Test Name	Test Description
3.3.1	ibisProcessor in laptop on the shore office laptop	Application for processing match
3.3.2	ibisView2 on the shore laptops	Same application in Ibis view in the cutter to see what information the cutter is sending for matching on shore.
3.3.3	IbisMatch application on the cutter laptops	Visible on the screen. Application for downloading eft files
3.3.4	IbisView application on the cutter laptop.	Visible on the screen

N.3 Test scripts

The following tests shall be executed within the lab; and as possible, on-board a USCG 110 cutter.

N.3.1 USCG handheld Test

Step	Description	Expected result	P (pass) / F (fail)	Comment
4.1.1 Capture Validation				
1	Power on handheld device	Prompts the user for a PIN		- If device already logged in reset it
2	Enter 4 digit pin (1234)	The Desktop screen will now be accessible for the user to start the application		

Step	Description	Expected result	P (pass) / F (fail)	Comment
3	Start the CG Application, START -> COAST GUARD	The Coast Guard home screen requesting a user log in. (this process should take less than 5 minutes)		
4	Enter a username (Test 1)	Test 1 populates the username field, is logged in the handheld log, and wristband ID screen appears. The bottom of the screen displays 200 transactions remaining.		
5	Enter 5 digit wristband ID # (12345)	The numbers should populate the window and be visible to the user.		
6	Start Timer			
7	Using only one hand: Press the center button (or click CAPTURE next to the ID Number) to continue to the capture process	The right index fingerprint capture screen appears.		
8	Using only one hand: Have subject place their right index finger on platen	The fingerprint should be visible in the user's window for capture.		
9	Using only one hand: When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the captured image is visible and screen will indicate PASS RIGHT_INDEX in green upon capture of an acceptable print		
10	Using only one hand: Press the center button (or click ACCEPT) when the fingerprint passes the quality check	The left index fingerprint capture screen appears		
11	Using only one hand: Have subject place their left index finger on platen	The fingerprint should be visible in the user's window for capture		

Step	Description	Expected result	P (pass) / F (fail)	Comment
12	Using only one hand: When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the captured image is visible and the screen will indicate PASS LEFT_INDEX in green upon capture of an acceptable print		
13	Using only one hand: Press the center button (or click ACCEPT) when the fingerprint passes the quality check	The FRONT facial capture screen appears		
14	Using only one hand: Center subjects face in camera display	The facial image of subject is visible in the capture screen		
15	Using only one hand: Press center button (or click CAPTURE to save image)	The captured image is visible on the screen for review		
16	Using only one hand: If this image looks clear (i.e. not blurry) press the center button (or click ACCEPT to save the data and create an EFT file).	EFT file (12345_'TCN'.EFT) saved to memory in folder (Storage Card\Coast Guard\). Display changes to main screen with Wristband ID # populated and incremented to (12346) and the total transactions remaining should read 199		
17	Stop Timer	Timer <= 30 seconds		
18	Confirm the image was saved properly, START->PROGRAMS. In the programs window open FILE EXPLORER. In the FILE EXPLORER window, open the STORAGE CARD->COASTGUARD	Displays a single EFT file (12345_'TCN'.EFT)		
19	Close FILE EXPLORER and close PROGRAMS window	The Coast Guard home screen displays requesting a wristband number. The bottom of the screen displays 199 transactions remaining.		

Step	Description	Expected result	P (pass) / F (fail)	Comment
20	Accept 5 digit generated wristband ID # (123456790) by pressing the center button (or clicking CAPTURE next to the ID Number)	The right index fingerprint capture screen appears.		
21	Have subject place their right index finger on platen	The fingerprint should be visible in the user's window for capture.		
22	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the captured image is visible and the screen will indicate PASS RIGHT_INDEX in green upon capture of an acceptable print		
23	Press the center button (or click ACCEPT when the fingerprint passes the quality check)	The left index fingerprint capture screen appears		
24	Have subject place their left index finger on platen	The fingerprint should be visible in the user's window for capture		
25	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the captured image is visible and the screen will indicate PASS LEFT_INDEX in green upon capture of an acceptable print		
26	Press the center button (or click ACCEPT when the fingerprint passes the quality check)	The front facial capture screen appears		
27	Center subjects face in camera display	The facial image of the subject is visible in the capture screen		
28	Press center button (or click CAPTURE to save image)	The facial image of subject is visible in the capture screen		

Step	Description	Expected result	P (pass) / F (fail)	Comment
29	If this image looks clear (i.e. not blurry) press the center button (or click Accept) to save the data and create an EFT file.	EFT file (12346_ 'TCN'.EFT) saved to memory in folder (Storage Card\Coast Guard\). Display changes to main screen with Wristband ID # populated and incremented to (12347) and the total transactions remaining should read 198		
30	Confirm the image was saved properly, START->PROGRAMS. In the programs window open FILE EXPLORER. In the FILE EXPLORER window, open the STORAGE CARD->COASTGUARD	Displays a single EFT file (123456_ 'TCN'.EFT)		
31	Close FILE EXPLORER and close PROGRAMS window	The Coast Guard home screen displays requesting a wristband number. The bottom of the screen displays 198 transactions remaining.		
32	Exit COAST GUARD application by clicking EXIT in the lower left corner	Display changes to Desktop		
4.1.2 Additional Feature Validation				
ID Number Length				
33	Start the CG Application, START -> COAST GUARD	The Coast Guard home screen requesting a user log in.		
34	Enter a username (Test 1)	Test 1 populates the username field, is logged in the handheld log, and wristband ID screen appears. The bottom of the screen displays 198 transactions remaining.		

Step	Description	Expected result	P (pass) / F (fail)	Comment
35	Enter a 3 digit ID Number (123)	The number should populate the window and be visible to the user.		
36	Press the center button (or click CAPTURE)	The ID Number Validation Message should appear stating the ID Number must be 5 digits in length		
37	Click OK on the message box	Message box disappears and the ID remains as entered		
38	Add two more digits to make the ID number (12345)	The number should populate the window and be visible to the user.		
39	Press the center button (or click CAPTURE)	The ID Number Validation Message should appear stating the ID Number must be 5 digits in length		
40	Click OK on the message box	Message box disappears and the ID remains as entered		
41	Press the BACK button to remove the last digit making the number (12345)	The numbers should populate the window and be visible to the user.		
42	Press the center button (or click CAPTURE)to continue to the capture process	The right index fingerprint capture screen appears.		
43	Click on ABORT to cancel the capture	Screen resets back to ID number screen with ID number (123456789) displayed		
Fingerprint Choice				
44	Change the 5 digit ID Number for test subject to(12346)	The numbers should populate the window and be visible to the user.		

Step	Description	Expected result	P (pass) / F (fail)	Comment
45	Press the center button (or click CAPTURE)	The right index fingerprint capture screen appears.		
46	Click the Alternative Print button	A selection of fingers list should appear (e.g. RIGHT_THUMB, RIGHT_MIDDLE, etc.)		
47	Select RIGHT_MIDDLE	The header at the top of the screen should change from RIGHT_INDEX to RIGHT_MIDDLE		
48	Have subject place their right middle finger on platen	The fingerprint should be visible in the user's window for capture.		
49	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the captured image is visible and the screen will indicate PASS RIGHT_MIDDLE in green upon capture of an acceptable print		
50	Press the center button (Click ACCEPT) when the fingerprint passes the quality check	The left index fingerprint capture screen appears		
51	Click the Alternative Print button	A selection of fingers list should appear (e.g. RIGHT_THUMB, RIGHT_MIDDLE, etc.)		
52	Select LEFT_MIDDLE	The header at the top of the screen should change from LEFT_INDEX to LEFT_MIDDLE		
53	Have subject place their left middle finger on platen	The fingerprint should be visible in the user's window for capture		

Step	Description	Expected result	P (pass) / F (fail)	Comment
54	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the captured image is visible and the screen will indicate PASS LEFT_MIDDLE in green upon capture of an acceptable print		
55	Press the center button (or click ACCEPT) when the fingerprint passes the quality check	The front facial image capture screen appears		
56	Center subjects face in camera display	The facial image of test subject is visible in the capture screen		
57	Press center button to save image (or click CAPTURE)	The facial image of subject is visible in the capture screen		
58	If this image looks clear (i.e. not blurry) press the center button (or click Accept) to save the data and create an EFT file.	EFT file (12345_'TCN'.EFT) saved to memory in folder 'STORAGE CARD\COAST GUARD'. Display changes to main screen with Wristband ID # (12346) populated and incremented by 1 and the total transactions remaining should read 197		
59	Repeat this process for the thumb, ring and little fingers	Same results as listed above for each step creating EFT files 12347_'TCN'.EFT, 12348_'TCN'.EFT, and 12349_'TCN'.EFT		
Image Quality Check				
Small				

Step	Description	Expected result	P (pass) / F (fail)	Comment
60	The 5 digit ID Number for test subject (12345) is displayed	The number should populate the window and be visible to the user.		
61	Press the center button (or click CAPTURE)	The right index fingerprint capture screen appears.		
62	Have subject place their right index finger on platen (ensure their finger is barely touching the platen, i.e. creating a “small” image)	The fingerprint should be visible in the user’s window for capture.		
63	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Small RIGHT_INDEX in red upon capture of an unacceptable print		
64	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
65	Have subject place their right index finger on platen (ensure their finger is barely touching the platen, i.e. creating a “small” image)	The fingerprint should be visible in the user’s window for capture.		
66	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Small RIGHT_INDEX in red upon capture of an unacceptable print		
67	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
68	Have subject place their right index finger on platen (ensure their finger is barely touching the platen, i.e. creating a “small” image)	The fingerprint should be visible in the user’s window for capture.		
69	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Small RIGHT_INDEX in red upon		

Step	Description	Expected result	P (pass) / F (fail)	Comment
		capture of an unacceptable print		
70	Upon receiving Small RIGHT_INDEX for the third time Click the ACCEPT button	The left index fingerprint capture screen appears		
71	Have subject place their left index finger on platen (ensure their finger is barely touching the platen, i.e. creating a “small” image)	The fingerprint should be visible in the user’s window for capture.		
72	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Small LEFT_INDEX in red upon capture of an unacceptable print		
73	Press the center button (or click RECAPTURE)	The left index fingerprint capture screen appears		
74	Have subject place their left index finger on platen (ensure their finger is barely touching the platen, i.e. creating a “small” image)	The fingerprint should be visible in the user’s window for capture.		
75	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Small LEFT_INDEX in red upon capture of an unacceptable print		
76	Press the center button (or click RECAPTURE)	The left index fingerprint capture screen appears		
77	Have subject place their right index finger on platen (ensure their finger is barely touching the platen, i.e. creating a “small” image)	The fingerprint should be visible in the user’s window for capture.		
78	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Small LEFT_INDEX in red upon capture of an unacceptable print		

Step	Description	Expected result	P (pass) / F (fail)	Comment
79	Upon receiving Small LEFT_INDEX for the third time Click the ACCEPT button	The front facial capture screen appears		
80	Center subjects face in camera display	The facial image of test subject is visible in the capture screen		
81	Press center button to save image (or click CAPTURE)	The facial image of subject is visible in the capture screen		
82	If this image looks clear (i.e. not blurry) press the center button (or click Accept) to save the data and create an EFT file.	EFT file (12351_ 'TCN'.EFT) saved to memory in folder 'STORAGE CARD\COAST GUARD'. Display changes to main screen with Wristband ID # (12352) populated and incremented by 1 and the total transactions remaining should read 193		
Dark				
83	The 5 digit ID Number for test subject (12353) is displayed	The number should populate the window and be visible to the user.		
84	Press the center button (or click CAPTURE)	The right index fingerprint capture screen appears.		
85	Have subject place their right index finger on platen (ensure their finger is wet and firmly placed on the platen)	The fingerprint should be visible in the user's window for capture.		
86	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Dark RIGHT_INDEX in red upon capture of an unacceptable print		
87	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
88	Have subject place their right index finger	The fingerprint should be		

Step	Description	Expected result	P (pass) / F (fail)	Comment
	on platen (ensure their finger is wet and firmly placed on the platen)	visible in the user's window for capture.		
89	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Dark RIGHT_INDEX in red upon capture of an unacceptable print		
90	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
91	Have subject place their right index finger on platen (ensure their finger is wet and firmly placed on the platen)	The fingerprint should be visible in the user's window for capture.		
92	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Dark RIGHT_INDEX in red upon capture of an unacceptable print		
93	Upon receiving Dark RIGHT_INDEX for the third time Click the ACCEPT button	The left index capture screen appears		
94	Have subject place their left index finger on platen (ensure their finger is wet and firmly placed on the platen)	The fingerprint should be visible in the user's window for capture.		
95	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Dark LEFT_INDEX in red upon capture of an unacceptable print		
96	Press the center button (or click RECAPTURE)	The left index fingerprint capture screen appears		
97	Have subject place their right index finger on platen (ensure their finger is wet and firmly placed on the platen)	The fingerprint should be visible in the user's window for capture.		
98	When satisfied with the image on screen press the center button (or click on the	When the print is captured the screen will indicate Dark		

Step	Description	Expected result	P (pass) / F (fail)	Comment
	CAPTURE button)	LEFT_INDEX in red upon capture of an unacceptable print		
99	Press the center button (or click RECAPTURE)	The left index fingerprint capture screen appears		
100	Have subject place their right index finger on platen (ensure their finger is wet and firmly placed on the platen)	The fingerprint should be visible in the user's window for capture.		
101	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Dark LEFT_INDEX in red upon capture of an unacceptable print		
102	Upon receiving Dark LEFT_INDEX for the third time Click the ACCEPT button	The front facial image screen appears		
103	Center subjects face in camera display	The facial image of test subject is visible in the capture screen		
104	Press center button to save image (or click CAPTURE)	The facial image of subject is visible in the capture screen		
105	If this image looks clear (i.e. not blurry) Press the center button (or click Accept) to save the data and create an EFT file.	EFT file (12353_'TCN'.EFT) saved to memory in folder 'STORAGE CARD\COAST GUARD'. Display changes to main screen with Wristband ID # (12353) populated and incremented by 1 and the total transactions remaining should read 192		
Light				
106	The 5 digit ID Number for test subject (12354) is displayed	The number should populate the window and be visible to the user.		

Step	Description	Expected result	P (pass) / F (fail)	Comment
107	Press the center button (or click CAPTURE)	The right index fingerprint capture screen appears.		
108	Have subject place their right index finger on platen (ensure the fingerprint sensor is exposed to a lot of direct light)	The fingerprint should be visible in the user's window for capture.		
109	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Light RIGHT_INDEX in red upon capture of an unacceptable print		
110	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
111	Have subject place their right index finger on platen (ensure the fingerprint sensor is exposed to a lot of direct light)	The fingerprint should be visible in the user's window for capture.		
112	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Light RIGHT_INDEX in red upon capture of an unacceptable print		
113	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
114	Have subject place their right index finger on platen (ensure the fingerprint sensor is exposed to a lot of direct light)	The fingerprint should be visible in the user's window for capture.		
115	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Light RIGHT_INDEX in red upon capture of an unacceptable print		
116	Upon receiving Light RIGHT_INDEX for the third time Click the ACCEPT button	The left index fingerprint capture screen appears		
117	Have subject place their left index finger on platen (ensure the fingerprint sensor is	The fingerprint should be visible in the user's window for		

Step	Description	Expected result	P (pass) / F (fail)	Comment
	exposed to a lot of direct light)	capture.		
118	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Light LEFT_INDEX in red upon capture of an unacceptable print		
119	Press the center button (or click RECAPTURE)	The right index fingerprint capture screen appears		
120	Have subject place their left index finger on platen (ensure the fingerprint sensor is exposed to a lot of direct light)	The fingerprint should be visible in the user's window for capture.		
121	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Light LEFT_INDEX in red upon capture of an unacceptable print		
122	Press the center button (or click RECAPTURE)	The left index fingerprint capture screen appears		
123	Have subject place their left index finger on platen (ensure the fingerprint sensor is exposed to a lot of direct light)	The fingerprint should be visible in the user's window for capture.		
124	When satisfied with the image on screen press the center button (or click on the CAPTURE button)	When the print is captured the screen will indicate Light LEFT_INDEX in red upon capture of an unacceptable print		
125	Upon receiving Light LEFT_INDEX for the third time Click the ACCEPT button	The front facial capture screen appears		
126	Center subjects face in camera display	The facial image of test subject is visible in the capture screen		
127	Press center button (or click CAPTURE) to save image	The facial image of subject is visible in the capture screen		

Step	Description	Expected result	P (pass) / F (fail)	Comment
128	If this image looks clear (i.e. not blurry) press the center button (or click Accept) to save the data and create an EFT file.	EFT file (12354_ 'TCN'.EFT) saved to memory in folder 'STORAGE CARD\COAST GUARD'. Display changes to main screen with Wristband ID # (123) populated and incremented by 1 and the total transactions remaining should read 191		
129	Exit COAST GUARD application by clicking EXIT in the lower left corner	Display changes to Desktop		

N.3.2 USCG laptop Test

Step	Description	Expected result	P (pass) / F (fail)	Comment
Laptop Validation				
4.2.1 Process Biometric searches				
1.	When the laptop starts up, login using "cwid2/cwid2" for shore laptop	This will log into the computer as an administrator		
2.	Lunch the ibisProcessor			
3.	Lunch the ibisView2			
4.2.2 EFT download and Biometric searches				
IBISMatch				
4.	When the laptop starts up, login into cutter laptop	This will log into the computer as an admin		

Step	Description	Expected result	P (pass) / F (fail)	Comment
5.	Enter username and password Username: cwidl Password: cwidl	Windows desktop displays (wait 5 minutes to allow all background services to start up)		
6.	For testing purposes, clean all data off the machine (run C:\coastguard\cleanup.bat	This removes all EFT files form the system		
7.	The IBISMatch and IBISView applications start up by user	IBISMatch window displays “ Waiting for IBIS ”		
8.	Ensure IBISMatch is looking in the correct location	IBISMatch window source (Source: e:\CoastGuard)		
9.	Connect the handheld to laptop via Active Sync (USB) cable	IBISMatch displays Connected “date and time”		
10.	IBIS Match retrieves EFT search files sequentially from handheld	IBIS match displays count of files downloaded “Downloading XX of XX”		
11.	IBISMatch deletes files from Handheld	IBISMatch displays count of files deleted “Deleting XX of XX” Verify delete files by checking “COAST GUARD” directory on handheld. Use file explore (My Device/Storage Card/CoastGuard)		
12.	IBISMatch states “Done, disconnect the handheld”. Remove the USB cable that is connected to the laptop	IBISMatch application returns to searching for the IBIS, The window displays “ Waiting for IBIS ”		

Step	Description	Expected result	P (pass) / F (fail)	Comment
13.	Reconnect the same handheld to the laptop via the USB cable	IBISMatch states that there are no EFTs on the handheld Connected “date and time” (No EFT Files Found)		
14.	IBISMatch save the EFT files in the folder “c:\CoastGuard\running\Laptop1_Efts”	Files are ready to display by ibisView		
IBISView				
15.	ibisView gets the original EFT file which was download from Handheld device by ibisMatch	Information can be display in the ibisView window		
16.	IBISView moves the EFT files from “c:\CoastGuard\running\Laptop1_Efts” to “c:\CoastGuard\running\Laptop1_Efts\oriViewedEfts”	Downloaded EFT files are located in the folder “..\oriViewedEft”		
17.	ibisView displays the original EFT records	All downloaded EFTS are visible in the Status Window and display the Armband number, the time of last update, the Match type, the Encounter type, and the Add Biographics button		Note: some of the downloaded EFTs are designed to be MATCHES
18.	Click the button “Add Biographics”, see the section below Addition of biographic data	Biographical pop window display		
19.	User enter the biographics data for this record			

Step	Description	Expected result	P (pass) / F (fail)	Comment
20.	User click the save button in Biographics window	The biographies window close and below action will be taken 21, 22, 23 for current writing		
21.	ibisView add the biographics into the original EFT file			
22.	ibisView saves this EFT file with biographics added in the folder “c:\CoastGuard\running\Laptop1_Efts\modifiedEfts”			
23.	ibisView sends the modified EFT to CAFIS for search			
24.				
25.				
26.				
27.	CAFIS should respond within a matter of minutes to and IBISView displays the results	Those files which match should display Match – See Alert... Those files that do not match should display NO MATCH The responses from CAFIS are located in the C:\responseEFT folder		

Step	Description	Expected result	P (pass) / F (fail)	Comment
28.	All files that match and display Match – See Alert... should be located in the Alert Window	The Alert window should display the Armband number, the time of last update, check box when completed, and Alert Details (Match from (encounter type) with FIN number		
29.	By clicking the row on the Alert Window	The hit person information window will be pop		
30.				
4.2.3 User Interface				
Interaction within system (window size, interface actions, reload)				
31.	Ensure that the IBISMatch window is static to the user Attempt to physically resize the window (see if the arrows appear when hovering over the edges of the window), Try to maximize the window using the buttons at the top right corner of the window, etc.)	The window should not be configurable by the user		
32.	Ensure that the IBISView window is static to the user Attempt to physically resize the window (see if the arrows appear when hovering over the edges of the window), Try to maximize the window using the buttons at the top right corner of the window, etc.)	The window should not be configurable by the user		
33.	Ensure that the user is not able to resize the height of the rows within the IBISView application (resizing a row could be confusing during operations)	The rows should not be configurable by the user		
34.	Ensure that the user can change the size (within limitations) or switch the order of the columns in the display window	The column size or order should be configurable by the user		Note: this is not in the requirements

APPENDIX O. CWID TRIAL 3.58 INFORMATION ASSURANCE FINAL SCAN RESULTS

IT3.58, USCG IS&C

O.1 Purpose

The purpose of this Coalition Warrior Interoperability Demonstration (CWID) Information Assurance (IA) Assessment was to provide a high-level analysis of a trial's security architecture for the trial vendors and sponsors. In order to receive this assessment, a trial had to meet two criteria:

- 1) Trial had to have some IA functionality—either the trial had to perform an IA service as its function or it had to use IA service(s)
- 2) Trial had to have United States (U.S.) involvement—either the trial must have been sponsored by the U.S. or and to be executed at a U.S. site

While CWID 2007 was primarily focused on making information available to war fighters and first responders, products that are going to be fielded needed to demonstrate that data/information that it processes was adequately protected. It was intended that CWID's IA Assessment process encouraged the trial's vendor and sponsor to consider IA functions and how to achieve an appropriate level of IA. This assessment considered both technical and administrative functions that contributed to the protection of information.

O.2 Background

CWID is the Chairman of the Joint Chiefs of Staff's (CJCS') annual event that enables the U.S. Combatant Commands and international community to investigate command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) solutions that focus on relevant and timely objectives for enhancing coalition interoperability. CWID conducts trials of C4ISR capabilities, which can then be moved into operational use within 6–12 months following the execution period. The scenario for CWID 2007 incorporated aspects of Homeland Defense (HLD) and Homeland Security (HLS) in addition to traditional Coalition operations. USNORTHCOM intends to use CWID as a proving ground for emerging C4ISR technologies relevant to HLD and HLS. International participants included Australia, Canada, New Zealand, United Kingdom (UK), and the North Atlantic Treaty Organization (NATO), to include several constituent nations. CWID 2007 was conducted in a simulated operational environment.

All vulnerabilities were found using network scanners only. Actual "hands-on" assessment would be required for validation of each one of the vulnerabilities, to include port openings. Some of the port openings may have resulted in false finding in the application/service that was found talking back to the tool. Most of the tools, if unable to get a definitive answer, gave a "best guess" on what was talking back. If another application protocol/service was actually on

that port, port redirection would be validated. Port redirection is unauthorized on any DOD network, and should be corrected immediately.

O.3 IA Principles

There are three common security principles/services that should be considered by a developer or risk acceptor when deciding the appropriate level of assurance a product must demonstrate. These are confidentiality, integrity, and availability. Some have included other principles such as authentication and non-repudiation when listing the principles.

- Confidentiality – information is available only to the authorized recipients
- Integrity – information has not been changed while stored or in transit
- Availability – information is available to the person/information system that needs it

Frequently, it seems that security services are at odds with each other. A battlefield commander might feel that it is more important to have information available than to keep information confidential—knowing the location of high-value targets (availability) might be more important than protecting the location of a sensor or information source (confidentiality). Or, a decision maker might feel that data integrity is the dominant service. For systems that process classified information, confidentiality is typically the dominant service.

O.4 Certification and Accreditation Methods

Information systems inherently have some level of risk to the security services. The government officially appoints someone as a risk acceptor/accreditor. When a system is accredited, the accreditor is stating that the system provides an acceptable level of risk for the environment in which it is operating. Accreditors consider all aspects of a system. They consider specific hardware and software, configuration, system administration, physical security, information assurance tools, product integration, foreign involvement, known threats, operating environment, and a number of other factors. Typically, the risk acceptor has broad programmatic knowledge. Often, they will rely upon a technical expert or certifier to technically assess whether or not the system's security mechanisms are adequate. When the risk acceptor considers the certifier's recommendation and knowledge regarding the malicious and non-malicious threats anticipated in the system's operating environment, they are able to make an informed decision regarding whether or not to accredit a system.

There are a number of certification and accreditation processes that the government uses for information systems. Some of these are:

- Department of Defense (DOD) Information Assurance Certification and Accreditation Process (DIACAP), for DOD Information Technology Systems
- National Information Assurance Certification & Accreditation Process (NIACAP)
- Joint Air Force, Army, Navy 6/3 for systems that process Special Access Required or Special Access Programs data
- Director of Central Intelligence Directive 6/3 for systems that process Intelligence data

Depending on the type of data being processed, other authoritative directives might apply. Each of these processes describes the activities that must be accomplished and the roles of the players involved with accrediting an information system.

O.5 Product Certification

According the National Secure Telecommunications and Information Systems Security Policy No. 11, IA products and IA-enabled products must be evaluated. Commercial cryptographic products are evaluated against the Federal Information Protection Standard (FIPS). National Information Assurance Partnership (NIAP) laboratories evaluate other commercial IA products. NIAP labs evaluate products against standards presented in the Common Criteria Evaluation and Validation Scheme. The data and operating environment will determine the Evaluation Assurance Level (EAL) that is required. The amount of evidence that a vendor must supply to the NIAP labs depends on the required EAL. More information is available at the common criteria portal and the NIAP website (<http://niap.bahialab.com/cc-scheme>).

O.6 Recommendations

From both the scan results and trial interviews, it was seen that the machines scanned had not completed the DOD Security Technical Implementation Guidelines (STIG) implementation. Follow the STIG for each operating system/device. STIG checklists can be found at <http://iase.disa.mil/stigs/stig/index.html>.

Follow the DOD Ports and Protocols Category Assignments List. Close unnecessary ports and stop unnecessary services and protocols from being used. A program used in Windows, TCPView, found at <http://www.microsoft.com/technet/sysinternals/Networking/TcpView.msp>, can be used to verify service running on each Windows machine to validate these results.

Periodic scanning your own products, using free tools (Nessus, NMAP, etc.), as well as fee based tools (Retina, WebInspect, etc.) with the intent of trying to find any possible security flaw, and patching those vulnerabilities, should be the focus of every DOD system, as well as in-coming DOD system to ensure all possible avenues of entry for malicious intruders are blocked. Conforming to minimum DOD standard will make it easier to enter service/agency specific networks, which will most likely have additional security implementations for each system.

O.7 Detailed Findings for the Boarding Team Communications System

HLD

Table O-1. Transportation Protocol X.X.4.63.

Port Number	State	Transportation Protocol	Application Protocol
443	Open	TCP	HTTPS

Vulnerabilities found:

- The installation of HSQLDB on the remote host has the default 'sa' account enabled without a password. An attacker may use this flaw to execute commands against the remote host, as well as read any data it might contain.

Table O-2. Application Protocol X.X.4.233.

Port Number	State	Transportation Protocol	Application Protocol
23	Open	TCP	TELNET
80	Open	TCP	HTTP

Vulnerabilities found:

- Anonymous FTP is enabled.
- ICMP Timestamp request is allowed from arbitrary hosts.
- The CMOS configuration does not conform to DISA requirements.
- Installed FTP server is configured to allow access to the system drive.
- Media Player is configured to allow automatic CODEC downloads.
- Reversible password encryption is not disabled.
- Unnecessary services are running on the system.

APPENDIX P. CWID 2007 NSWC DAHLGREN AFTER ACTION REPORT

Date: 26 July 2007

From: Dennis Warne, Dahlgren CWID Site Lead

To: CWID JMO

Via: COL Howard Thomas, HQMC C4

CAPT William Sposato, NAVSEA SEA Trial Program Manager

Subj: COALITION WARRIOR INTEROPERABILITY DEMONSTRATION 2007 (CWID 07) DAHLGREN SITE AFTER ACTION REPORT (AAR)

1. Introduction:

Naval Surface Warfare Center (NSWC) Dahlgren, Virginia hosted 33 Interoperability Trials (ITs) demonstrated on both the Coalition and Homeland Security venues in seven separate Operational Centers. CWID 2007 executing from 8–22 June 2007 as the Senior Warfighters for the Coalition Forces Land Component Commander (CFLCC), 1ST Marine Expeditionary brigade (MEB), 31ST Marine Expeditionary Unit (MEU), 15TH MEU, National Guard Bureau (NGB), Naval Sea System Command (NAVSEA) Sea Trials unit, and US Coast Guard (CG) participated here.

2. Significant Accomplishments:

The NSWC Dahlgren site successfully integrated/demonstrated 33 Interoperability (ITs). There were 11 ITs on the CTF Domain and 12 on the HLS Domain, there were also 9 trials common on both domains, and 1 on the 4 Eye Domain.

The following ITs are highlighted from NSWC Dahlgren that obtained successful Warfighters assessment that could identify useful technologies with future value:

1.01 Compartmented High Assurance Information Network (CHAIN) was well received and extensively used by the war fighters. **This IT met its CWID objectives.**

IT 3.09 Global Recovery System (GPRS), generated a lot of interest with DVs with its ability to recover downed Pilots and other recovery operations. **This IT was very successful and accomplished all its CWID objectives.**

IT 3.14 COSMOS, was well received by Coalition visitors and should be continued to be developed/improved for CWID 08. **This IT was extremely successful and accomplished its CWID objectives**

IT 3.58 USCG Information Sharing and Communication, demonstrated the ability to create a human Bio metric based tracking system to identify hostiles. A system like this would be

invaluable to Physical Security and Intelligence personnel in Iraq and Afghanistan. **This IT met its CWID objectives.**

IT 3.71 Mobile Keys, next generation will include CAC Card capability with their portable stick. With the DOD requiring CAC Cards this new capability should return next year for assessment. **This IT met its CWID objectives.**

IT 5.12 ID-Map: Situational Awareness, Visualization and Collaboration, demonstrated superb capabilities for Command and Control Centers. **This IT met all its CWID objectives.**

3. CWID 07 Execution at NSWC Dahlgren:

This year the USMC supplied a portable Command Operational Center (COC) that was set up outside the CWID building (BLDG 1450T) to simulate an actual operational center used by forward deployed units (Iraq and Afghanistan). This provided additional realism to the Dahlgren site and provided additional insight to actual conditions Trials would encounter should they be forward deployed. The USMC plans to expand this capability next year.

With the addition of the COC at Dahlgren the USMC simulated the 15TH and 31ST MEU to the Dahlgren MBAT role player lists. Since these Units supported amphibious landings they fit into the CWID Scenario extremely well, add realism, and are planned to be used again next year.

The NAVSEA unit LCS and DDG 1000 Operational Center used several fires systems (i.e., NFCS, JADOCS, and AFATDS) to execute precision strike and calls for fire from Dahlgren using GCCS threads. Target Missions were processed and executed involving systems across the CFBL network such as AFATDS, NFCS, JADOCS, UK-JETTS (JETTS was at Dahlgren) and GE-ADLER (Simulated German Artillery). This effort was in support of JETTS and JADOCS initiative at UK and EUCOM sites. NSWC Dahlgren plans to continue using AFATDS, NFCS, and JADOCS as infrastructure and looking into additional fire systems for next year.

This year Dahlgren added a separate US Coast Guard (CG) Operational Center with CG Role players where the CG based ITs were assessed. This break out placed new emphasis on the CGs role and technology needs. Dahlgren plans to pursue expanding the CG role in CWID through coordination with NORTHCOM.

The NGB Room was very effective but tightly packed with numerous ITs. We need to look at possibly limiting some of the amount of unclassified IT/Trials in this Ops Center or expanding this space. We're planning on discussing this with NORTHCOM to improve CWID at Dahlgren.

NSWC Dahlgren provided tours for 331 visitors which included 23 DVs (O7 / SES 1 and above) and 6 media outlets

4. Operational Comments:

IT training at NSWC Dahlgren was a challenge this year. The ITs fit into two different categories, those that had a good presence here during set up and execution and provided excellent training to the role players (were here to answer questions and walk them through the

IT) and those that limited their presence due to funding or programmatic constraints and provided very limited role players training and no direct Site support during execution.

The NAVSEA unit LCS and DDG-1000 Operational Center was well organized, trained up, and manned. Dahlgren has the capability to supply a solid infrastructure to support SPAWAR's CFMCC Scenario and plans to pursue a closer relationship with SPAWAR regarding NAVSEA unit LCS and DDG-1000 involvement for CWID 08.

JMO assessors working out of NSWC Dahlgren integrated extremely well with the Site Technical Staff. They had many challenges with IT software/hardware and MSEL execution, but they were quickly identified and resolved as a team. NSWC Dahlgren plans to improve this teaming process to identify issues quicker and hopefully resolved them faster to ensure MSELs are not missed or executed improperly in CWID 08.

5. 2007 Lessons Learned:

CWID Test Schedule – In past CWID's the Network Working Group, along with several other supporting JMO WGs generated a very detailed site and services test schedule to valid backbone services and to assist the sites in CWID preparations. This testing was for both the US Sites and Coalition participants on each of the various Domains. The testing usually involved the months of April and May as a validation and run-up to execution in June. For CWID 07 there did not seem to be a rigorous test schedule established which lead to several problems during set up week and the first week of execution. This item should be addressed prior to CWID 08 IPC.

CWID Demonstration – Demonstrations in CWID 07 were very taxing here at NSWC Dahlgren. In CWID 06 the demos (e.g., Mediator) performed better than many of the Site ITs. In CWID 07 this was not the case with the exception of very few (e.g., Mediator). Including demonstration in CWID 08 will need to be looked at very closely by the Service Leads due to the fact that they are draining the Site's limited resources and takes away from the approved ITs.

IT challenges – Some of the IT/Trials were very complex. The IT technicians that arrived on site were technically competent, however many lacked CWID indoctrination. Site personnel had to review configuration requirements, Site/Working Group responsibilities as well as train the technicians on CWID methodology.

JMO introduction video – The CWID JMO video should be produced and delivered to the Sites at least one week prior to execution.

6. Conclusion:

I have just recently returned as the CWID Dahlgren Site Lead and I and my team look forward to working with the JMO, other Sites, Coalition partners, and the various CWID working groups to make CWID 2008 the best ever.

Dennis Warne

CWID Dahlgren Site Lead

(This page intentionally left blank.)