2003-08

ASOCC capabilities to meet MTAC current and future requirements

Schacher, G. E. (Gordon Everett)

Monterey, California. Naval Postgraduate School

NPS-97-03-007

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

ASOCC Capabilities to Meet MTAC Current and Future Requirements

Gordon Schacher and Shelley P. Gallup

Wayne E. Meyer Institute of Systems Engineering

August 2003

Prepared for: Navy Warfare Development Command

This page intentionally left blank.

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RADM David R. Ellison, USN
Superintendent

Richard Elster
Provost

This report was prepared for: Naval Criminal Investigative Service

This report was prepared by: Wayne E. Meyer Institute of Systems Engineering

Authors:

_____
Gordon Schacher

_____
Shelley P. Gallup

Reviewed by:

_____
Phil DePoy, Director
Wayne E. Meyer Institute of Systems Engineering

Released by:

_____
Leonard A. Ferrari, Ph.D.
Associate Provost and
Dean of Research

REPORT DOCUMENTATION PAGE

Form approved

OMB No 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	20 July 03	Technical Report

4. TITLE AND SUBTITLE
ASOCC Capabilities to Meet MTAC Current and Future Requirements

5. FUNDING
Office of Naval Research for Naval Criminal Investigative Service

6. AUTHOR(S)
Gordon Schacher and Shelley P. Gallup

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Wayne E. Meyer Institute of Systems Engineering
Naval Postgraduate School
777 Dyer Rd., Room 100D, Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Criminal Investigative Service
Naval Yard
Washington, DC

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words.)

The Area Security Command and Control System (ASOCC) has been designed to support Command and Control information and decision making during a terrorist event. It is being installed in a number of DoD facilities, including the Multi-Threat Alert Center in NCIS. This work has determined the support ASOCC can provide for current and possible future MTAC missions.

14. SUBJECT TERMS
Force Protection, Network Information Systems, Homeland Security

15. NUMBER OF PAGES
92

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	

NSN 7540-01-280-5800
(Rev. 2-89)
Std 239-18

Standard Form 298
Prescribed by ANSI

Table of Contents

This page intentionally left blank.

1.0 EXECUTIVE SUMMARY

This report addresses whether the Area Security Operations Command and Control (ASOCC) system can adequately support the full range of the Naval Criminal Investigative Service's (NCIS) Multi-Threat Alert Center (MTAC) information processes. It also examines whether MTAC's mission should expand to become more directly involved in Homeland Security (HLS).

1.1 BROAD SUMMARY

Currently MTAC's major function is ingesting and analyzing intelligence information to produce assessments and provided them to naval units. Much of the work is long range, fusing and assessing information from a variety of sources to determine the threat background. Less frequent is providing warnings of immediate danger.

ASOCC is designed to support information processes for Crisis and Consequence Management. The information provided is local and real-time, from human observations and a variety of sensors. There is a heavy emphasis on information display and collaboration to support situational awareness and decision-making. There is a mismatch between MTAC's basic mission and the operations ASOCC is designed to support, but a match in some of the functionalities needed for both. A system designed for real-time information, and associated user-friendly displays, can provide considerable support for MTAC analysts if the proper information can be made available.

The major ASOCC drawbacks for supporting MTAC activities are:

1. lack of capability to support TS/SCI information and
2. it will be available only to major commands.

Thus, much of the information used by MTAC cannot be on the system and it cannot be used for widespread information dissemination to the naval community.

The existence of ASOCC in MTAC opens the possibility of close collaboration with those units participating in HLS, including real-time assessments and C2 during a terrorist event. This would be a major addition to MTAC responsibilities, but could be warranted as DoD becomes increasingly involved in this activity.

- ASOCC would provide the capabilities needed for this mission.
- Standard Operating Procedures (SOPs) would have to be written for supporting this mission, and for using ASOCC in conjunction current information processes.

1.2 CORRELATION BETWEEN ASOCC DESIGN and MTAC PROCESSES

MTAC and NCIS Field Agents have responsibilities for:

- Providing assessments to naval units.
- Collaboration with other agencies to develop assessments.
- Collaboration with Operations Centers.
- Interaction with local authorities for naval unit Force Protection.

ASOCC is designed to provide information for the following operational and tactical actions:

- Collaborative course-of-action planning.
- Crisis and Consequence Management execution.
- Situation monitoring.
- Response asset monitoring.
- ID through engagement of specific threat objects.

The system uses an internet based approach, with considerable graphic display and collaboration capabilities . It is designed for real-time information during a terrorist event, primarily for Crisis and Consequence Management.

ASOCC provides information input, access, display, and dissemination, and collaboration for decision-making. MTAC's principal activities are similar processes.

- ASOCC's collaboration capabilities could improve the workflow of both MTAC watchstanders and analysts.
- ASOCC's capability to display large amounts of diverse information for easy comprehension could aid MTAC near-term and real-time analyses.

The ASOCC CONOPS specifically address requirements for, and the system has solutions for:

speed of information access,
information fusion (presentation for fusion, not the process),
situation assessment,
widespread information dissemination, and
speed of collaboration.

- The system fully meets these requirements for real-time Consequence Management.

ASOCC does not meet MTAC operations requirements for:

- Automatic generation of Navy messages and/or e-mail.
- Field Agent connectivity to SIPRNET when ASOCC is not available to them.
- Availability at all naval units.
- TS/SCI information sources and collaboration.

The first two requirements could be accomplished within ASOCC with some additional system development. The second two are unrealistic. This implies

- ASOCC cannot replace existing MTAC process means. It would have to work in parallel with them.
- This is not a serious restriction. Regardless of the support provided by the system, the requirement to use existing means will remain.

1.3 ASOCC USE FOR MTAC PROCESSES SPECIFICS

Providing Assessments to Naval Units: MTAC has the responsibility to provide a variety of assessments and warnings to naval units, ranging from Threat Assessments to Blue Darts.

- ASOCC can provide a distribution means to those units that have the system.

- Current means, primarily message traffic, will continue to be required.
- Having parallel means for distribution is an advantage. Redundant paths will be needed when one path is unavailable.

Collaboration With Other Agencies To Develop Assessments: A significant portion of MTAC's information input comes from other agencies. Most of this information is at the TS/SCI level.

- ASOCC cannot support information nor collaboration at the TS/SCI level.
- ASOCC Chat collaboration tools at the Secret level would benefit assessment operations.

Collaboration With Operations Centers: MTAC currently coordinates with a number of centers, e.g. ROCs, JITTF. This is currently done to both obtain and provide threat information.

- AOCC will be at many centers and can implement instant, multi-person collaboration for operational and tactical purposes.
- Assessments could be speeded with use of the system.
- Availability of side-by-side Secret and Unclassified collaboration could aid fusing both types of information.

Interaction With Local Authorities: I&W and real-time Force Protection information can come from a variety of sources, including unclassified such as local police or even civilians. Current NCIS interaction with local authorities is primarily through Field Agents and Field Offices.

- ASOCC being located in EOCs could speed access to local threat information.
- Field agents will most often not have direct access to the system.
- Local information is filtered through a Field Office (first-level assessment by subject-matter experts), which will not have ASOCC.
- There is no process for direct MTAC access to locally produced information.
- It is unclear how local information, vetted for assessment, would be placed in ASOCC, when, and by whom.

ID Through Engagement Of Specific Threat Objects: ASOCC has capabilities to identify and track threat objects and to distribute that information. Tracking such objects in real-time is not an MTAC responsibility, but it is an MTAC responsibility to monitor and assess the threat environment and knowledge of anything that contributes to that environment is of high interest.

- ASOCC's presentation of threat tracks could aid assessing the threat environment.
- ASOCC may not be in operation and presenting tracks during the pre-event phase.

Field Agents: NCIS Field Agents will probably not have access to ASOCC. Agents are an important source of information, both I&W and real-time. They also provide information directly to ships and installations and play a key role in overseas ship Force Protection. Because of these responsibilities, and their possible need for rapid communications, consideration must be given to how they carry out their duties when ASOCC is in use.

- There are no means determined for Agents inputting information to ASOCC.
- There are no processes for ASOCC distribution of SIRs and Spot Reports.
- There is no process for Field Office or MTAC verification of information in ASOCC.

1.4 RECOMMENDED ACTIONS

Parallel Paths: The requirement to disseminate information from MTAC to naval forces via message traffic will remain regardless of other means being put into place. E-mail is also extensively used for alerting. If ASOCC and existing means are to operate in parallel:

- Single-point-entry is needed.
- If there is no automatic means for creating messages and e-mail from single-point-entry, the amount of work to be done in MTAC will be increased by inclusion of ASOCC paths.

Benefits to MTAC from having the ASOCC path also available are:

- Use of ASOCC and associated alerting could speed the information processes.
- Availability of ASOCC could provide an alternate path when current means are down.

Personnel Requirements: ASOCC manning requirements are unclear. Manning depends on how it will be used. It is expected that decisions on how ASOCC will be used will depend on whether needed manning can be supported.

- Determine ASOCC manning requirements for various use configurations.
  - Full 24/7 support for MTAC daily operations.
  - Support for only new HLS operations.
  - Use of the collaboration capabilities for daily analyst operations.
  - Use of the collaboration capabilities by watchstanders.

System Improvements, Fusion of Real-Time and I&W Information: Pre-terrorist-event I&W information can be valuable for evaluating the current situation. This could be information acquired and processed for as long as several months before an event. Such information needs to be fused with that obtained during the event. There is no ASOCC process for doing this.

- Develop a means for ASOCC fusion of long-term I&W information.
  - A permanent archive.
  - A classification scheme so that pertinent information can be identified.
  - A means for extracting information that applies to the current situation.
  - A means for displaying information that applies to the current situation.
- Develop SOP for fusing I&W and current event information for real-time analysis.

System Improvements, Alerting Naval Units to Threats: The current alerting system in ASOCC needs modification and additional capabilities:

- A means to go directly from an alert to pertinent information.
- Visible alert status for the sender, e.g. has it been opened and acted on.
- Visual time of entry and status for all ASOCC users
- Prioritization scheme.
- Direct alert to the recipient for directed information.
- A separate special section for official information, such as SAR, SIR, Blue Dart.

SOP Development: The current ASOCC CONOPS and contained SOPs are fairly complete for Crisis and Consequence Management. They do not address many MTAC requirements.

- Develop new MTAC SOPs
  - For use of ASOCC in parallel with current means for current processes.

  - HLS responsibilities.
- Develop ASOCC SOPs specific to how it provides NCIS support.
  - For placing SIRs, Spot Reports, SARs, etc. in ASOCC.
  - Field Agent access and use.

1.5 ASOCC IN A SYSTEM OF SYSTEMS

No single current system is designed to support the broad spectrum of information processes from MTAC's I&W to terrorist-event real-time sensors and C2. A combination of systems, preferably existing systems, is needed.

The Navy currently has systems that, collectively, can meet many requirements, with ASOCC adding the needed COP and SA at the local level. For example:

- Joint Fires Network (JFN)
- Tactical Exploitation System- Navy (TES-N)
- Collaboration at Sea (CaS)
- Global Command and Control System (GCCS)

These are noted (there are others) as examples because the first two support Navy Fires and the last two provide access throughout the Fleets. Navy Fires processes have correspondence to HLS processes and Navy Force Protection operations. Compatibility of ASOCC with JFN would be needed and is not technically difficult.

Much of MTAC's information and collaboration is at the TS/SCI level. If network solutions are to be used for information dissemination at the Secret level, a means is needed to move information between these levels. JFN includes TES-N (TS/SCI) for image exploitation and ADOCS (SECRET/NOFORN) for target execution.

- TES-N processes TS/SCI information and passes Secret target information to ADOCS for target exploitation.
- TES-N can also pass information to GCCS for situational awareness.

Thus, technical solutions for the exchange of information across classification levels exist. It is germane that

- ASOCC has capabilities for import of information from GCCS.

The need to provide information to all naval units is a significant consideration for any system supporting MTAC operations. ASOCC will not be available at all locations with which MTAC is required to exchange information. Most challenging are small ships at sea, which have intermittent internet connectivity and limited bandwidth. The CaS system exists on essentially all Navy ships. Updates by replication occur frequently, with files being updated whenever a ship logs on.

- CaS is not directly compatible with ASOCC, JFN, or its variants and it would be somewhat cumbersome to use for this application without modifications.
- However, it illustrates that network solutions to widespread distribution are available without starting from scratch.

This page intentionally left blank.

2.0 INTRODUCTION

The purpose of the study reported here is to determine contributions the Area Security Operational Command and Control (ASOCC) system can make to the mission of the Multi-Threat Alert Center (MTAC) and to its parent organization, the Naval Criminal Investigative Service (NCIS). We focus on MTAC and NCIS Field Agents because ASOCC has, potentially, the most direct applicability to their operations.

It is planned that ASOCC will be installed at Homeland Security (HLS) operating centers and at major Navy facilities such as Regional Operating Centers. An ASOCC server is already located in MTAC but there are no CONOPS or Standard Operating Procedures (SOP) for how it will be used. The ASOCC developer has written Draft CONOPS that can provide an initial review of the support that can be expected for MTAC information processes and collaboration with other organizations. This is not an evaluation of ASOCC capabilities, rather the support it can provide to MTAC's mission.

The ASOCC CONOPS states (italics) that the current, draft version "*exclusively focuses on Navy employment and, in particular, the current Phase 1 employment strategy (e.g. San Diego and Norfolk fleet concentration areas)*." Thus, the CONOPS is appropriate to Navy use at operating centers that support a regions installations. This is not necessarily the same support needed for MTAC's mission to provide assessments for the whole of naval forces.

Perhaps the first organizations MTAC will interact with that have ASOCC installations are East and West Coast Joint Harbor Operating Centers (JHOCs), which are primarily combined Navy and Coast Guard organizations. A Draft CONOPS for the San Diego JHOC has been prepared. That CONOPS has been reviewed as part of this study.

During a crisis event appropriate Emergency Operating Centers (EOC) are stood up to manage the situation. Their operations and how MTAC will operate with them are an important consideration. MIDLANT Regional Operating Center (ROC) personnel have been interviewed in order to understand how MTAC now interacts with that Center and how it might interact through the use of ASOCC.

A primary ASOCC goal is to provide shared Situational Awareness (SA) amongst local organizations and between them and national organizations during an emergency. For this purpose it is planned to have the system at local-, regional-, and national-level EOCs. NCIS Field Agents duties include interaction with a variety of people and organizations at the local level as well as their being a part of NCIS operations at the Field Office level. There is the possibility that access to ASOCC would enhance Field Agent interaction with local organizations and with MTAC. Thus, Field Agent processes are included in report as a component in understanding potential ASOCC use.

Three general types of information exchange must be considered:

1. Long-range Indications and Warning (I&W).
2. Urgent information that needs assessment and fusion with other information.
3. Immediate threats.

The first type of information is processed and transmitted at a relatively slow pace. Building Threat Assessments is an example. Most information that is dealt with by the intelligence community is of this type. Multi-agency collaboration for evaluation and producing products is frequent.

The second type of information is less frequent but of high priority when it appears. It requires in-depth evaluation in order to assess the level of the threat. It can lead to an assessment of imminent danger and warnings to units that might be affected must be sent out.

For the third type, by immediate threat we mean information is in hand that "the Huns are coming over the hill". The information is such that immediate action is required. NCIS deals with this type of information infrequently. It is this type of information ASOCC is designed to carry, information that produces situational awareness during a terrorist event for both Crisis and Consequence Management.

This report does not provide a complete presentation of all NCIS information processes. As noted above, the purpose of this report is to determine what ASOCC can contribute to MTAC processes and the processes described are only as complete as needed for this purpose. Even with this restriction, a considerable breadth of information exchange processes is covered.

3.0 FITNESS ANALYSIS

Determining support that ASOCC can provide for MTAC processes is done by determining "fitness" between that system's capabilities and MTAC's information input and dissemination requirements. Fitness is multivariate, requiring examining several aspects of both the system and requirements. We have developed a set of elements to facilitate this comparison. They are:

- Broad purpose, objectives
- Who participates
- High-level functions
- Operational/tactical actions
- Command and personnel relationships
- System/process requirements
- System/process capabilities

Fitness comparisons of the type reported here are best made at the Standard Operating Procedures (SOPs) and Tactics Techniques and Procedures (TTPs) level. The ASOCC Draft CONOPS contains many SOPs and TTPs even though they are not identified as such.

For a Fitness comparison, each element is broken down into a set of attributes, which are shown in the following table. The table then shows whether that attribute is required by MTAC and provided by ASOCC. There are two columns for MTAC, the first for current requirements and the second for MTAC expanding its mission to fully support HLS. Fitness between MTAC and ASOCC is determined by looking for Xs in the same rows. Fitness is higher for MTAC transitioning to HLS support because ASOCC was designed for such support.

Fitness Element	MTAC Current	ASOCC	MTAC HLS
Broad Purpose			
Indications and Warnings	X		X
Multi-Agency Situational Awareness		X	X
Multi-Agency COA Planning		X	
Threat Assessment	X		X
Incident Management		X	
Participants			
NORTHCOM	X	X	X
JITTF	X		X
ROC		X	X
EOC		X	
JHOC		X	X
Local Law Enforcement		X	
First Responders		X	
Field Offices	X		X
Field Agents	X		X
Navy Bases	X	X	X
Ships	X		X
High-Level Functions			

Collaborative COA Planning		X	
Crisis Management		X	X
Consequence Management		X	
Operational Situational Awareness	X	X	X
Tactical Situational Awareness		X	X
Threat Asssessment	X		X
Threat Warnings	X	X	X
Operational/Tactical Actions			
Asset Monitoring		X	
Asset Management		X	
Detect to Engage		X	
Sensor Management		X	
Information Management	X	X	X
Information Alerting	X	X	X
Action Alerting	X	X	X
Tactical Collaboration		X	X
System Requirements/Capabilities			
Internet Based		X	X
Message Traffic	X		X
Collaboration Capabilities	X	X	X
TS/SCI Capable	X		X
Secret Level Capable	X	X	X
Unclassified Capable	X	X	X
Automatic Trans-Classification			X
Connectivity to All Bases	X		X
Connectivity to All Ships	X		X
Connectivity to Field Offices	X		X
Field Agent Accessible	X		X
Ingest Sensor Data		X	
Map Overlays		X	X
Import Agency Databases		X	X
WMD/HAZMAT Predictions		X	
Incident Reporting		X	X
Warning Direction and Coordination		X	X
Threat Warning	X	X	X

Discussions of these attributes are found throughout this report. Discussions of the Fitness elements are found in the Conclusions in Section 8.

Summary Fitness between MTAC requirements and ASOCC capabilities, using aggregate elements are as follows:

Aggregate Element	Fitness
Intelligence Agency collaboration	Low
Reach all naval units	Low
Coordination with Operations Centers	High
Real-time situation awareness (MTAC with HLS)	High
Real-time threat alerting	High

4. MTAC PROCESSES AND REQUIREMENTS

MTAC's primary duty is threat reporting from I&W information. Information comes from CIA, State, FBI, other DoD, and Navy sources. Information comes in on JWICS and CT Link, which is operated by the CIA. These are TS/SCI sources and normally contain raw information. CT Link is the primary source and CIA controls its content. The Watch Officer checks these inputs every 15 min and determines whether there is information that requires action, decides what action to take, and initiates the proper processes.

Information also comes into MTAC from NCIS Field Agents, field offices, ships, and other Navy units. The MTAC information situation presents an interesting challenge. The organization is to ingest information that has a wide range of attributes, ingest, fuse, and assess it, and provide information outputs with a similarly wide range of attributes. Attributes are:

Geographic -specific location to broadly applicable.
Time -immediate interest to uncertain time of threat action.
Quality -highly credible to unknown veracity; - recent to aged information.
Level - severe threat to generalized danger.

If a piece of information comes into MTAC that is

- credible
- immediate interest (e.g., near-term threat)
- location known
- significant danger

the watch will take immediate action to warn the affected unit through appropriate means.

If these criteria are not met, different actions can be taken. E.g., [General interest, not imminent > send to analyst and archive] or [Significant threat, unknown location > general alert].

The situation is often not clear-cut and nor from a single piece of information. It is often one of piecing together information that has a range of attributes, some separated in time, and possibly from a location that is not that where the current threat exists. One of the main functions of MTAC analysts is to fuse information from many sources to build a coherent threat picture and provide appropriate warnings.

Fusing dissimilar types of information to present an accurate picture of a current threat is challenging. For example, say the following information were available:

1. A terrorist group X had received scuba training on underwater demolition techniques at a camp within the last year (information in an archive).
2. Local dissidents at port city Y recently purchased scuba gear (Field Agent report).
3. Van of unknown ownership intercepted bringing explosives Port Y country.
4. Local contacts report excitement within local dissidents about an approaching event (recent information obtained from friendly by agent arranging a port visit).
5. A U.S. DDG is planning a Port Y visit in two weeks.

The sources for this information are varied, the contents are of various ages, and different means were used for their transmission to MTAC. They need to be fused into a coherent picture.

What information should MTAC output, and to whom, based on these inputs? It could be:

a general warning of underwater threats to all Navy units.
an increase in threat level for that country and modified Threat Assessment.
a specific warning to the DDG not to go into port A.
a combination of the above.

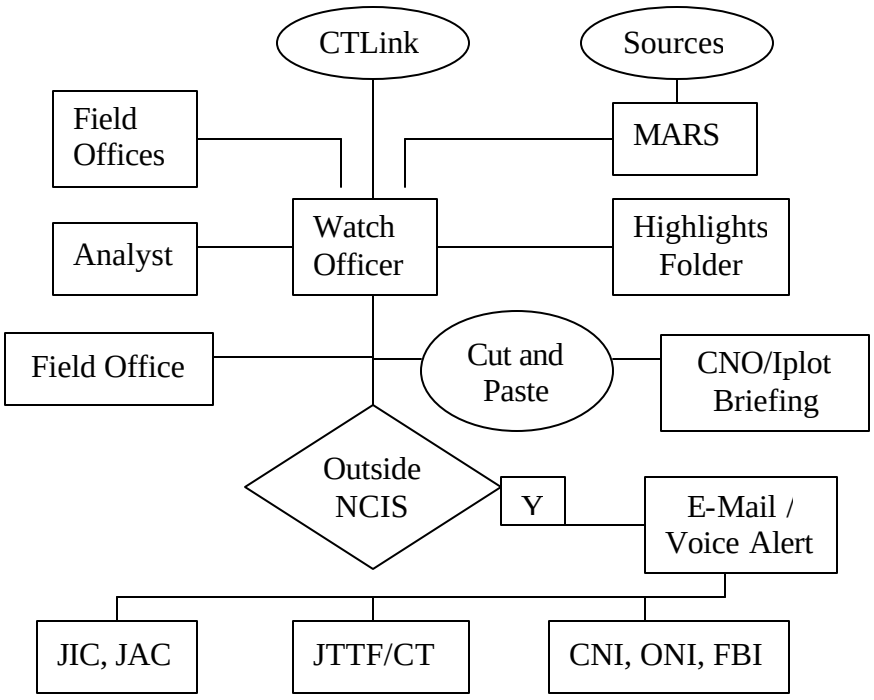
In this contrived situation it is easy to see correlations between various pieces of information. For many of the situations being examined it is not so easy. It is NCIS's/MTAC's job to piece together information and provide outputs to the Navy that enable adequate Force Protection postures. A thrust of this project is to determine what types of information systems are needed to accomplish this job in the current and future environments.

There is an urgency spectrum to both information input and output. They can roughly be categorized as:

Long-range - used with other information to build assessments.
Timely - forward to Navy units and other organizations for their consideration.
Urgent - immediate threat knowledge or belief, issue appropriate warnings.

4.1 LONG-RANGE I&W INFORMATION

The MTAC watch is continually monitoring input information from a variety of sources. Information for which immediate action is not needed is sent to analysts, placed in "folders", and used to prepare briefings. Such information is also shared with other intelligence agencies and Navy units. The following diagram shows the basics of long-range information flow.



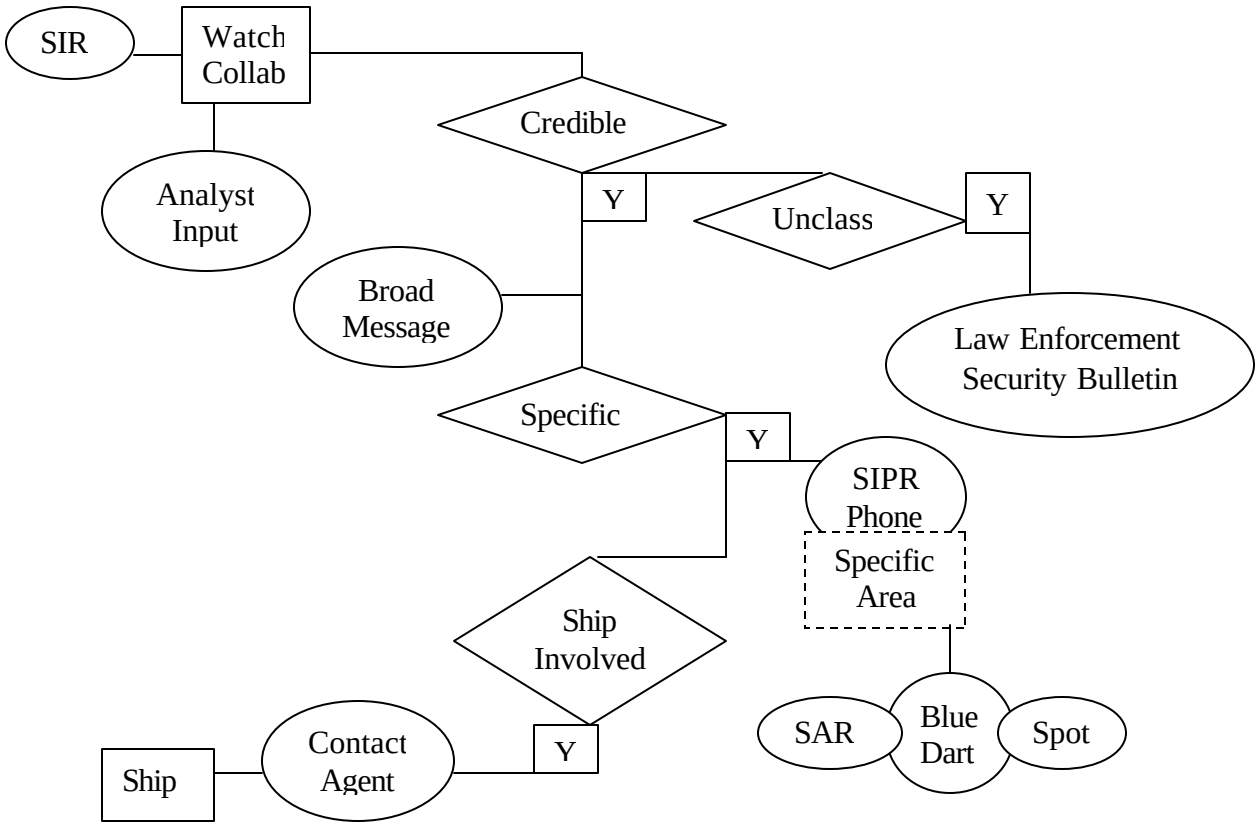
MTAC Long-Range Information Flow

Much of the input information is on the high side, TS/SCI. If classified (Secret) information is sent out, it is put on a disk and taken to a computer with the proper classification. If needed, voice is by STU.

Collaboration paths are not shown. IRC Chat is available on the high side. Secret level Chat is not available and would be useful for many situations.

4.2 TIME-SENSITIVE INFORMATION FLOW

The following figure shows examples of time-sensitive information flow. It is a composite of the things that can occur and information that can be sent out, not flow for a particular situation.



Time-Sensitive Information Flow

Message traffic is currently the primary means of transmitting information.

Nothing above indicates the speed with which various types of information should be accessed, evaluated, and transmitted. Message traffic is slow, and phone calls are also subject to availability of the person on the receiving end and possible need to leave messages for call back.

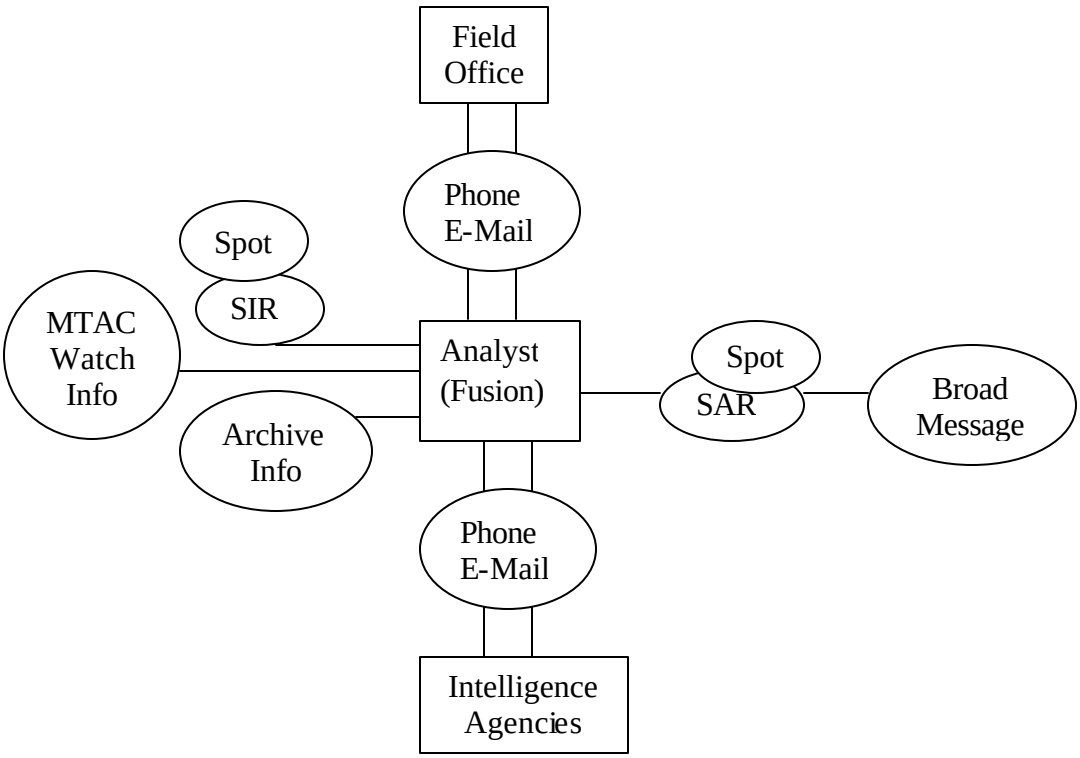
An evaluation of speed requirements is beyond the scope of this study, except to indicate in the comparisons with ASOCC where it might be a factor.

4.3 ANALYST PROCESSES

MTAC Analysts have available information from several sources. Their source of criminal information is MARS. They can pull information from there or the Watch may push information to them. They are experts for a particular geographical area and subscribe to daily summaries that pertain to that area. E.g., for the Pacific area: JIC/PAC, PACOM, NSA/East Asia. JITTF/CT would be a source for all analysts. Analysts also have available information that is archived at NCIS, and area information "drawers" are being implemented.

Analysts also work directly with the NCIS Field Office for their area. This is done through e-mail and phone calls. In some cases a Field Office does not have communication facilities for high classification levels and information has to be transmitted through an embassy. E-mail is used for asynchronous group-chat and a SIPR internet capability to carry out collaboration would be of benefit.

In the course of producing their product, Analysts acquire and evaluate a broad range of information and participate in quite a bit of collaboration. Most Analyst output is SARs but they can also produce Spot reports. They can send a SAR with no other endorsement. The following diagram shows the essential elements of their information input and output.

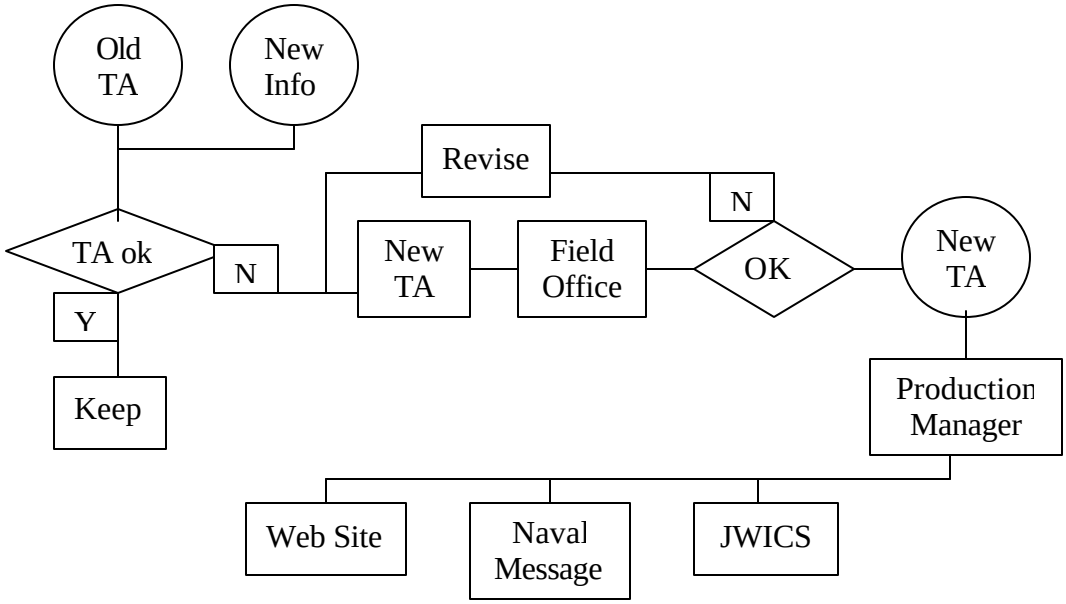


MTAC Analyst Information Processes

4.3.1 Threat Assessments

Producing Threat Assessments is a new task for MTAC Analysts. The information used to produce these assessments is obtained in the same manner as noted above, with a focus on piecing together various types of information, mainly long-term, to provide a complete picture.

Assessments are coordinated with the appropriate field office using the process illustrated in the following diagram.



Analysts Threat Assessment Production Process

This page intentionally left blank.

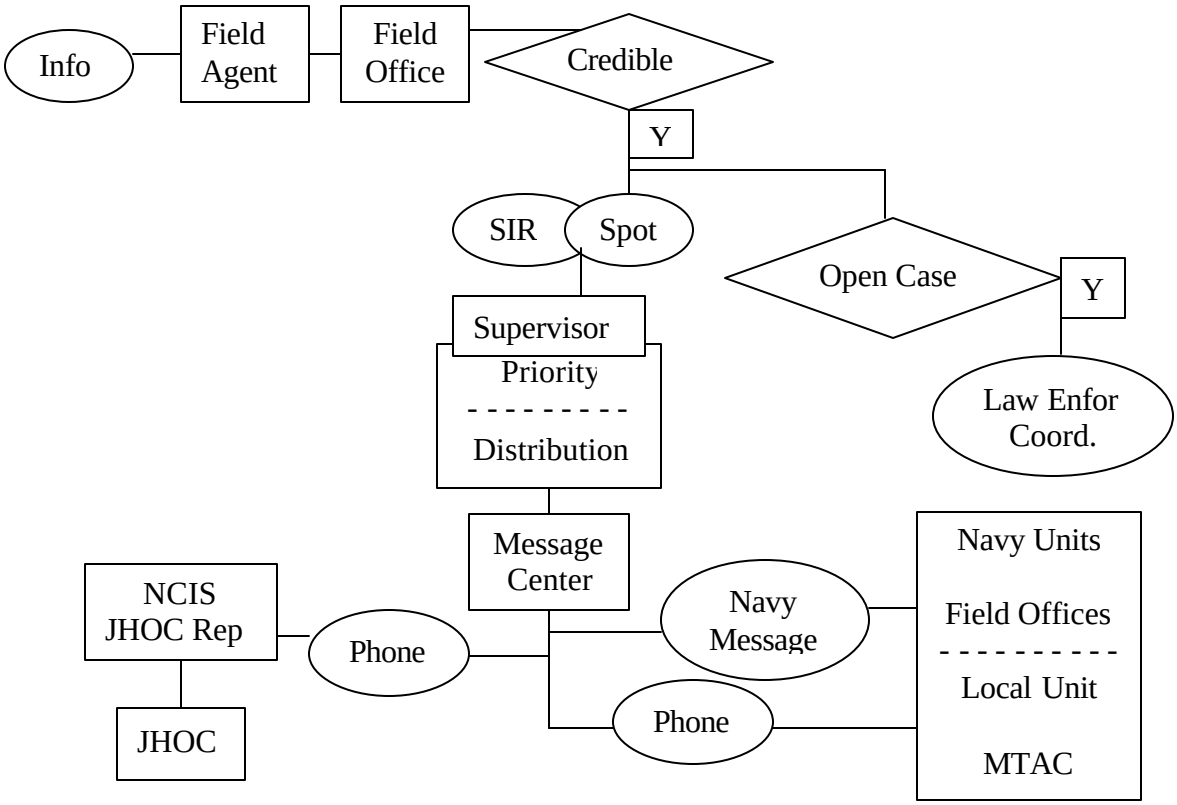
5. FIELD AGENT PROCESSES AND REQUIREMENTS

NCIS Field Agents have a wide range of law enforcement responsibilities, few of which are covered here. We have chosen to focus on those responsibilities that illustrate types of information exchange where ASOCC can provide and not provide support:

1. Interaction with Operations Centers
2. Interaction with MTAC
3. Foreign port operations

Interactions with Operations Centers and with MTAC are similar in that they are multi-person activities. Agents on the ground coordinate with their Field Office. The Field Office has agents assigned to coordinate with regional Operations Centers. It also has an administrative center where communications with outside the office are cleared, prioritized, and executed. Foreign port operations are different because the Field Agent has more individual information exchange responsibilities, e.g. communications with a ship while it is in port.

NCIS Field Agents are not authorized to provide information directly to other units. The Agent uses an authorization process at Field Headquarters, which involves a supervisor and the administration message center. If the information will go to an Operations Center, the NCIS agent assigned as coordinator with the Center will also be involved. Regardless of whether information goes to a Center, a coincident path to Navy units will also be used. The following is a diagram of the process.



Field Agent Information Processes

5.1 FOREIGN PORT OPERATIONS

Foreign ports vary widely in the capabilities that are available. We discuss here the worst case so that the full range of communications options used and needed are discussed. It can be the case that there is no embassy available, no NCIS support facilities, no communication other than by cell phone. This does not directly address evaluation of ASOCC use in the continental U.S., but does provide additional insight into the full range of NCIS communication needs ASOCC may need to support.

We describe the common situation of an Agent supporting a Navy ship going into a foreign port. Before leaving the home station for the foreign location, the Agent takes the following actions:

- Pull the current Threat Assessment for the area.
- Pull the current PIVA for the location.
- Check out a cell phone that will work in the area.
- Obtain the ship's Force Protection Plan.

If lucky, they may have the Force Protection Plan before leaving the office. Getting the Plan 2 weeks ahead is a wonder, may get it 2 days ahead, or it may not be available until in-transit or on site.

On site, the agent's first actions are:

- Contact the Defense Attaché.
- Contact the ship.

If there are difficulties reaching the ship because of local conditions, the home Station is contacted to have them relay information to the ship. When the ship is in port:

- Deliver the Threat Assessment personally to the ship's Commanding Officer and Force Protection Officer.
- Meet with the ship daily to communicate updates and, if the ship desires, participate in daily planning.

Prior to the ship's arrival, and while it is in port, the Agent is:

- Working with local law enforcement to assess threats and available local support.
- Working with local information sources, if such contacts exist.
- Working with the port administration to determine facilities support available.
- Comparing the ship's Force Protection Plan to current conditions.
- Communicating needed information updates to the ship, its superior, and the home office.

The result is that the Agent spends much time on-the-ground and may have a need to communicate from various locations. Communications can be with all of the entities noted above. The Agent's primarily communication means are:

- Phone.
- Face-to-face.

The need to communicate sensitive or classified information often arises and this can be delayed until proper facilities can be reached. NCIS is in the process of acquiring RASP, a portable computer system that will allow secure communications by satellite link from any location.

The work described above is a mixture of real-time coordination and longer-term situation assessment. Being successful at assessing the local situation requires developing local relationships so that information sources are available. During an "event", on-the-street activities must still occur if the Agent is to be effective.

ASOCC will not play a role in foreign operations because it will not be available. Several systems with similar capabilities are being proposed for HLS. The Navy is improving its ability to collaborate during operational situations by various means, such as Joint Fires Network, Collaboration at Sea, Global Command and Control System. A spectrum of capabilities is in place, being improved, and becoming available. It is important to examine whether a similar tool would be of benefit to an Agent for foreign operations. In essence, one is asking whether a tool developed for real-time situation awareness during an event, and in the ASOCC case designed to meet the needs of first responders and consequence managers, will be of aid to Agents longer-term operations.

Field Agent operations in CONUS are similar to those described above so this question also applies to CONUS activities. A significant difference is that communication capabilities are better. Another difference is that working with local authorities is more reliable and smoother.

The position of an NCIS Field Agent in CONUS is unlike other law enforcement officers because they are part of DoD and laws with regard to the military operating in the U.S. apply. The Agent can work low-level civilian sources but can't investigate U.S. citizens; that is an FBI responsibility and such information has to be obtained from them. They provide a support role during an event to base security forces and local police, who have the primary responsibility. For example, during an event, an agent might provide near-term information to gates for the type of activity to expect, but would not be responsible for manning the gates and protecting the base. In essence the responsibilities are somewhat longer-range predictions. An agent is unlikely to need the speed of an ASOCC for communicating such information.

This page intentionally left blank.

6. JHOC FUNCTIONS

JHOC is included here because of the emerging importance of Homeland Security (HLS) and because JHOC San Diego being stood up, with NCIS participation, as an HLS center. It is also important because it is a prototype for Navy participating in direct coordination with other activities during a crisis event, i.e. Navy Region, U.S. Coast Guard, base security, local law enforcement, City EOC, etc.

Interactions with JHOC depend on how that organization functions. Pertinent JHOC characteristics are:

- Manned full-time to manage harbor operations.
- Exists within the Coast Guard Operating Center.
- Three watchstanders: Coast Guard, Navy, and Harbor Police.
- NCIS Agent will be assigned to JHOC (for coordination, not as a watchstander).
- Navy OS/E5 will be in the EOC permanently to monitor IWCCS.
- Will contain an ASOCC terminal.

The JHOC situation awareness architecture is complex. Characteristics of this architecture pertinent to this study are:

- Multi-node, with sensor inputs at various places.
    - Harbor cameras feed into SPAWAR EOC and Regional Police EOC.
    - IWCCS feed to ASOCC will be in CG EOC (at JHOC).
    - GCCS will feed into IWCCS (I&W tracks) then be fed into ASOCC for C2.
- ASOCC is the backbone that will distribute sensor imagery and information.
    - An ASOCC terminal will be needed at SW Region to input these feeds.
    - Bases will need an ASOCC node of security is to have this information.

This architecture means that information from a variety of sensors in the harbor area can be available to all area participants, and to remote locations properly equipped. The same is true for any other type of information exchange.

The architecture makes possible single point-of-entry for information an NCIS Field Agent wishes to provide to NCIS, the Navy Region, law enforcement, etc. Even though JHOC will be in operation all of the time, the same is not true for other centers. They will be in operation during a crisis, with a defined process for which center is primary, with an alternate primary in case one is down. The following considerations apply to whether or not an Agent can use this system for transmitting information to required locations:

- Some units requiring the information may not have ASOCC capabilities.
- The system may not be manned (non-crisis situations).
- It may not be desired to give the information widespread distribution.

We provide here a review of the Draft JHOC CONOPS as a baseline to compare how MTAC can coordinate with that organization and how ASOCC might be part of that process. This is not a review of the CONOPS itself, only its applicability to MTAC operations.

6.1 JHOC CONOPS ELEMENTS

The 24 Mar Draft CONOPS (see Appendix B) contains all of the elements outlined in the Fitness Analysis Methodology Section, but not arranged as shown there. The following are elements extracted from that document and placed in the suggested arrangement. These elements are not described for the sake of brevity and because the meanings are well understood.

Broad purpose, objective

- Improve common Situational Awareness and responsiveness across multi-agencies.
- Improve C2 and coordination of multi-agency efforts to deter, detect and defend against asymmetrical terrorist threats offshore and within the Port of San Diego.
- Enhance coordination of Incident Management and Consequence Management.
- Leverage collective efforts and limited resources to optimize their use.
- Enable coordinated interagency actions.

Who participates

- United States Coast Guard, San Diego Operations Center
- Commander, Naval Region South West, Emergency Operations Center
- Commander, Third Fleet

High-level functions supported

- Collaborative course-of-action planning
- Situation analysis
- Crisis and Consequence Management execution
- Situation monitoring
- Response asset readiness monitoring
- Destroy/thwart asymmetric threats

Operational/tactical actions supported

- Identify
- Track
- Target
- Interdict
- Engage and re-engage

Command and personnel relationships

- One watchstander from each participating organization
- Two options for authority:
    - JHOC Watch Commander has assigned coordination authority
    - All watchstanders equal

Use rules

- Participating agencies will retain Tactical Control (TACON) of their assets.
- Participating agencies operate under their existing ROE.

- Diverting USN assets should be avoided to ensure continuous protection of vessels and facilities.
- Requests for USCG assets will go directly to the Activities Operations Duty Officer.
- Requests for Harbor Police assets will go directly to Harbor Police Dispatch.
- Requests for Navy Security assets will go directly to Regional Dispatch Center EOC.

System/process requirements

- Timely
- Interoperability within the Incident Command System
- Information architecture
    - server-based intranet link to integrate
        - sensors,
        - agency databases,
        - intelligence information
- Databases
    - National Criminal Information Center (NCIC)
    - Automated Regional Justice Information System (ARJIS)
    - Marine Information Safety and Law Enforcement (MISLE)
    - Joint Maritime Information Element (JMIE), SEALINK, ELINT query
    - Global Command and Control System Marine/Joint(GCCS-M/J)

System/process capabilities

- Interoperable secure communications
- Tactical decision aids
- Information
    - collection
    - processing
    - fusion
    - dissemination
- Geographically separated sensors
- Static information sources (dynamic is not mentioned)
- Sensors
    - video
    - radar
    - thermal imaging
    - sonar
    - ACTD Direction Finding System (position localization)
    - Automatic Identification System (AIS)
    - Blue Force Locating System

6.2 JHOC TASKS

The Draft CONOPS lists a large number of tasks in its Section III, “Concept of Operations”. These tasks are breakdowns of the elements listed above into actual activities to be performed. For example, the following tasks listed under A, “Daily Operations”, are Track tasks:

Track

#2 Monitor, track and record deep draft vessel traffic including moored and anchored vessels.
#3 Monitor and track other vessel activity for suspicious and/or anomalous activity.
#8 Compare actual vessel arrival information with scheduled arrival information.
#10 Establish, maintain dialogue with local pilots associations concerning vessel movements.
#12 Maintain continuous MDA (commercial vessels in port, cargo operations, Blue Force activities, channel clearings, special events, HVA/HIVs, and boardings).

In order to compare adequately JHOC CONOPS and MTAC information processes, it is necessary look at tasks as well as the CONOPS elements. In Results, Section 8, we discuss correlations between CONOPS elements and tasks and MTAC processes.

The JHOC CONOPS contains a large number of tasks that are not included in the elements listed above. A number of them overlap with MTAC responsibilities. A list follows immediately with code numbers (A1, B1b, etc) that refer to the subsection and number in Section III "Concept of Operations"

A1 – Maintain situational awareness of current activities.
A4 – Receive and coordinate initial investigations of suspicious and/or anomalous activities.
A5 – Monitor radios for voice traffic.
A3 – Monitor and track other vessel activity for suspicious and/or anomalous activity.
A12 – Maintain continuous MDA of Blue Force activities, special events, HVAs, and boardings.
A16 – Respond to requests for information from federal, state, and local authorities.
B1b – Divert/launch the most appropriate law enforcement asset(s) to investigate or intercept threats/targets of interest.
B1c – Alert all participating agencies threats/targets of interest.
B1f – Requests for Navy Security assets will go directly to the Regional Dispatch Center.
B1g – All participating agencies will agree to comply with JHOC requests whenever feasible.
B1j – Provide tactical coordination between available law enforcement and protective (USN Force Protection) assets.
B5 – Coordinate information dissemination to appropriate commands and stakeholders.
D1 – Utilize an informational technology architecture that will integrate sensors, agency databases, and intelligence information to provide common situational awareness for decision-makers and security assets…

This is an interesting list. It ranges from information dissemination that is clearly within the MTAC area of responsibility (B1c), to how NCIS Field Agents might be assigned (B1g), to new coordination tasks (D1). There is, as yet, no indication of how these tasks would be shared between MTAC and a JHOC. This needs to be clarified as SOP are developed for all phases of terrorist events.

7. ASOCC CAPABILITIES

The Draft ASOCC CONOPS is contained in Appendix A. It presents good descriptions of system components and capabilities in the initial sections, which are not discussed here. Rather, we discuss proposed use of the system to support HLS processes. System performance is adequate to support this use. System improvement suggestions are in Section 8 of this report.

7.1 ASOCC CONOPS ELEMENTS

The 12 May ASOCC Draft CONOPS contains all the elements presented above in Section 3, but not arranged in the manner shown there. The following are elements extracted from that document and placed in the desired arrangement. The entries are not described for the sake of brevity and because the meanings are well understood.

Broad Purpose, Objective

In the section "Coordination/Support, Command and Control Strategy", the CONOPS states "*...provide commanders with mission-critical capabilities to plan, coordinate, integrate and manage AT/FP operations by integrating the efforts of the Joint Maritime Component Commander (JFMCC), CPF/CLF, C2F/C3F, other U.S. Combatant Commanders, Navy Regional Commanders, U.S. Coast Guard activities, and local/State/Federal law enforcement partners*". This breaks down into the following objectives:

- Provide common Situational Awareness across multi-agencies.
- Provide collaborative course-of-action planning across multi-agencies.
- Provide cooperative decision-making across multi-agencies
- Provide a platform for threat assessment, operational and tactical support, and response to the presence of WMD devices during all aspects of a terrorist incident including both crisis and consequence management.

Who Participates

The CONOPS defines two organization levels: Incident Level is first responders and Multi-Echelon Level is the collection of organizations that provide screened information to responders and command organizations. They contain:

Incident Level:

- Joint Harbor Operations Center
- Emergency Operations Center
- Joint Operations Center
- Navy Regional Command Center or Navy Regional Operations Center

Multi-Echelon Level

- US NORTHCOM/ECH 1 Commands/LFA
- NAVNORTH/JFMCC
- CPF/CLF

High-Level Functions Supported

- Collaborative course-of-action planning

- Crisis and Consequence Management execution
- Situation monitoring
- Response asset readiness monitoring

Operational/Tactical Actions Supported

The following actions are specifically included.

- Shared situational awareness
- Information management
  - Unclassified and Secret
  - Transfer across classification levels
  - Push and pull as local situation and threat demands
  - Alerting to insure information awareness
- Information fusion
  - Sensors
  - Intelligence (threat)
  - Real-time law enforcement
  - Asset availability

The I&W phase of an operation is noted but the CONOPS does not provide specifically for it.

These information processes directly support military and civilian actions to identify and interdict terrorist activities. In military terms, the spectrum of these actions is:

- Identify
- Track
- Target
- Interdict
- Engage and re-engage

Command and Personal Relationships

No command relationships are specified. The CONOPS states " *Since ASOCC is a peer-to-peer network, allowing permissive/approved access to all users for information being assimilated on the net, the concept of a command and control process, with strict hierarchies for reporting and communication, is not entirely applicable*.". Thus, there is no way to specify how ASOCC fits within a command structure or supports structured interrelationships between organizations. It is flat and whatever structure or relationships exist must be imposed external to ASOCC.

Operational personnel are not listed. Personnel needed for system operation are designated. It is not specified at what locations these people are needed. It would not be at each location where there is an ASOCC system, so the total number is uncertain. The responsibilities of the two positions are:

- System Administrator
  - Monitor the status of ASOCC nodes and adjust peer-to-peer relationships as required,
  - Provide Tier II maintenance support to ASOCC workstations in the AOR,
  - Maintain a database on the configuration and ASOCC software version at each node,
  - Perform or coordinate installation of new software releases,
  - Perform ASOCC user and local administrator training,

- Operations support
  - Configure the XIS tool to access locally designed and remote databases for all nodes in the AOR,
  - Assist all nodes in developing or modifying and sharing of local databases for ASOCC access,
  - Provide quality control for local databases used as sources for ASOCC,
  - Identify remote databases of interest to ASOCC users and arrange for ASOCC access to them,
  - Identify and demonstrate mapping sources that may be of interest to ASOCC users,
  - Assist ASOCC nodes in developing and sharing overlays, shape files, etc. that could be used in ASOCC,
  - Assist in the training of ASOCC users.

7.2 STANDARD OPERATING PROCEDURES

The ASOCC CONOPS does not use the term Standard Operating Procedures. Regardless, the document does contain a large number of what are essentially SOPs. They specify operation of the system rather than interactions between command nodes as are often specified in SOPs. Even though they are not specifically operational, they provide insight into operational use of ASOCC.

These SOPs are extensive, covering all aspects of ASOCC use, and are segmented in the CONOPS into Incident and Multi-Echelon levels. There are so many SOPs that, for ease of presentation, we have additionally segmented them into four categories:

Information Management,
Situational Awareness,
Sensor Information, and
Information Display.

There is some overlap between SOPs at the Incident and Multi-Echelon levels. When that occurs, they are listed in both.

Incident Level:

Information Management

- Information on events happening off base: These will be entered into ASOCC by the federal, state and local agencies that maintain nodes, or reported via JOC channels.
- At the incident level, both an Unclassified and a Classified (SIPR only) network would be maintained.
- When other first responders have ASOCC, the fire department, disaster response group, or other designated incident-level organizations may be responsible for WMD event calculation and reporting in ASOCC.
- The location and details of events and incidents with installation security implications: Using the Event Log on the eX-Panel, these log entries will be linked to locally developed, interactive (future capability) checklists to expedite the taking and logging of actions.

- Creation of incident reports in the ASOCC Event Log by JHOC/EOC personnel would provide a primary ("quicklook") information summary for use by higher (e.g. multi-echelon level) command elements.
- Local and State agencies such as local police, harbor patrol, fire department, etc., would have input and access to the Unclassified network.

Situational Awareness

- Using this sensor network, along with inputs from security patrols and on-scene observers, JHOC/EOC watchstanders would maintain a tactical picture of the area of interest, whether it be at a specific base installation, harbor, or facility perimeter.
- ASOCC watchstanders may choose to designate chat rooms for collaboration in the Defense Collaboration Tools Suite (DCTS) and specify the purpose for each room. They can establish these chat rooms for constant monitoring and establish schedules for regular collaboration sessions involving key personnel or nodes.

Sensor Information

- Sensor feeds coming from Radar, CCTV, Thermal Imagers, etc., would be fed into the Unclassified terminals located at the JHOC, EOC, and RCC/ROC.

Information Display

- JHOC/EOC personnel would maintain database information on the location, identity and status of critical infrastructure and assets that is compatible with XIS (e.g. MS Access database or Oracle database) so that it can be displayed in XIS and shared with other users.
- ASOCC watchstanders may locally create and use "overlays" for the tactical-picture graphic display showing base defense, FPCON, and contingency plans to aid in situation response.
- If intelligence suggests the possibility of a WMD threat, or in response to an actual WMD event and/or industrial (HAZMAT) accident, ASOCC watchstanders would calculate and display graphic overlays of the estimated areas affected (using the CATS tool) and be responsible for reporting the incident in ASOCC.

Multi-Echelon Level

Information Management

- DoD ASOCC workstations supporting this operational level will (generally) operate at classified security levels on the SIPRNET.
- Incident information will be provided on incidents occurring on or near U.S. installations, and in the entire AOR, including information on the location and identification of critical infrastructure and assets, and off-base operations.
- U.S forces at DoD installations will be the source of information for incidents occurring on or very near U.S. installations.
- JOCs and various Federal, State, and local agencies will be the sources of information for incidents occurring in the non-DoD portions of the AOR. Regional Operations Centers (ROCs) (via their bilateral cells) are where information derived from regional level organizations will be entered into ASOCC for dissemination to all echelons.

- Information on the locations and identities of critical infrastructure and assets are maintained by the installation Command Post or EOC.
- Tactical type information originated on unclassified ASOCCs and in unclassified databases will migrate to the classified side at the JHOC/EOC or RCC/ROC. Both need access to ASOCCs operating on unclassified and classified networks.
- Using the CATS tool in ASOCC, installation security forces will initiate calculation of areas affected by HAZMAT/WMD and what predicted impact it will have on military and civilian centers.
- Echelon one will maintain a list of recommended web sites in a file in the AOR room on DCTS and may specify sites that all nodes should monitor. Any node may recommend additional sites containing useful information to the AOR.
- Incident folder management: The initial incident reporting node should include the name and location of this folder in the incident event log entry as well as information on which collaboration room in DCTS will be the focal point for collaboration on the incident being reported.

Situational Awareness

- Echelons above the installation level will not normally need tactical information about on-base security forces. Needed is general knowledge of security force location and composition in the AOR, particularly those earmarked to support U.S. installations and those protecting off-base infrastructure critical to U.S. operations. ROCs, and JOCs will obtain this type of information from their counterparts, and enter it into local databases.
- If a WMD event or industrial accident occurs in other regions, it is important to immediately promulgate all I&W information as a preventative measure against possible multiple attacks.
- Status boards will be used for situational awareness.
  - The Incident-Level will create and maintain status boards for information created at their level.
  - Summary status boards to be maintained at the regional level.
  - When U.S. forces are using civilian airfields and ports for HLS operations, the Service Component conducting the operations at that site will maintain status board and assessment information on those sites unless ASOCC connectivity with those locations can be attained, in which case the site will maintain them.
  - Initial implementation for sharing status board type information is for each installation to maintain status boards on its SIPRNET web site.

Sensor Information

- All raw sensor inputs are to be directed to the regional and/or functional workgroup servers within the "incident-level" and selectively "pushed" or "pulled" to any other functional group or ASOCC station within the network.

Information Display

- ASOCC does not come with maps pre-installed. Each node must find and store maps that fit its needs from other sources.

- The echelon one will maintain information on recommended mapping sources and files of geo-registered images in folders in its DCTS AOR room for all to use. Other nodes may add images to this list at any time.

7.3 SYSTEM/PROCESS REQUIREMENTS

Immediately below are information system requirements from the JHOC CONOPS review, showing requirements from the operations support point of view. They are presented very abbreviated as a lead-in to the following ASOCC capabilities.

- Timely
- Interoperability within the Incident Command System
- Information architecture
  - server-based intranet link to integrate
    - sensors,
    - agency databases,
    - intelligence information
- Databases
  - National Criminal Information Center (NCIC)
  - Automated Regional Justice Information System (ARJIS)
  - Marine Information Safety and Law Enforcement (MISLE)
  - Joint Maritime Information Element (JMIE), SEALINK, ELINT query
  - Global Command and Control System Marine/Joint(GCCS-M/J)

There are additional requirements to support MTAC processes.

- TS/SCI
- Dissemination to all navy units, including ships
- Support parallel message traffic

The JHOC CONOPS contains a large number of tasks that are not included in the elements listed above. A number of them overlap with MTAC responsibilities. A list follows immediately with code numbers (A1, B1b, etc) that refer to the subsection and number in Section III "Concept of Operations"

A1 – Maintain situational awareness of current activities.

A4 – Receive and coordinate initial investigations of suspicious and/or anomalous activities.

A5 – Monitor radios for voice traffic.

A3 – Monitor and track other vessel activity for suspicious and/or anomalous activity.

A12 – Maintain continuous MDA of Blue Force activities, special events, HVAs, and boardings.

A16 – Respond to requests for information from federal, state, and local authorities.

B1b – Divert/launch the most appropriate law enforcement asset(s) to investigate or intercept threats/targets of interest.

B1c – Alert all participating agencies threats/targets of interest.

B1f – Requests for Navy Security assets will go directly to the Regional Dispatch Center.

B1g – All participating agencies will agree to comply with JHOC requests whenever feasible.
B1j – Provide tactical coordination between available law enforcement and protective (USN Force Protection) assets.
B5 – Coordinate information dissemination to appropriate commands and stakeholders.
D1 – Utilize an informational technology architecture that will integrate sensors, agency databases, and intelligence information to provide common situational awareness for decision-makers and security assets…

This is an interesting list. It ranges from information dissemination that is clearly within the MTAC area of responsibility (B1c), to how NCIS Field Agents might be assigned (B1g), to new coordination tasks (D1). There is, as yet, no indication of how these tasks would be shared between MTAC and a JHOC. This needs to be clarified as SOP are developed for all phases of terrorist events.

7.4 SYSTEM CAPABILITIES

There is no ASOCC capability to link to TS/SCI information. Thus, intelligence information references are limited to SECRET.

The ASOCC CONOPS segments system and process capabilities into nine categories:

- Sensor Integration
- Assessment Information
- Threat Condition Reporting
- Warning Direction and Coordination
- Incident Reporting
- Collaboration
- Maps
- Web Site Monitoring
- WMD Events and Industrial Action Situations.

This segmentation is preserved below.

Sensor Integration

- Provide a C4ISR backbone for AT/FP plug-and-play sensor packages that can be changed, modified, or removed in a short period of time.
- Provide space, common open architecture, and a common control system for these sensors.
- Capability needed to selectively push or pull all raw sensor inputs to any other functional group within the "incident-level" or ASOCC station within the network.
- Nodes on the network (e.g. regional Border Patrol, Customs, or other Non-DoD law-enforcement organizations) be able to provide cueing information on contacts or areas of interest to U.S. Navy and Coast Guard watchstanders at the JHOC, or Navy Regional Security personnel operating at an EOC.
- Intelligence and sensor information be selectively forwarded to multiple HLS/HLD echelons via NIPRNET, SIPRNET or DCTS collaboration.

Assessment Information Requirements

- Detailed information on the status of security forces, and critical infrastructure and assets, and assessment-type information on them.
- Provide information via status boards with a drilldown to detailed information on numbers, types, capabilities, and assessments of assets.
- Provide incident-level status boards.
- Provide installation status boards.
- Provide regional-level summary status boards.

Threat Condition Reporting

- Provide AOR-level means to direct changes to FPCONs, INFOCONs, and MOPP levels.
- Provide a means to monitor what/when conditions are attained at the installation level.
- Provide a means to determine problems associated with individual station non-compliance and sustainability of threat condition capabilities.

Warning, Direction, and Coordination

- Provide a means to alert installations when specific information or assessments exist.
- Provide a means to receive acknowledgement of receipt from the affected installation.
- Provide a means to disseminate guidance, direction, and coordination instructions.

Incident Reporting

- Provide a means to share incident photographs.
- Provide a means for collaboration to ensure pertinent information is disseminated.
- Provide a means for creating and maintaining incident folders so that other reporting and materials concerning the incident can be filed in a central location for all to access.

Collaboration

- Provide multiple Chat rooms, with each to have:
  - Areas for sharing files
  - Discussion forums
  - Audio conferences
  - White board collaboration.
- Provide a room structure that supports special purpose themes, e.g. Regional-level, security forces, peer-to-peer level, geographic area, etc.
- Provide collaboration information archiving.

Maps

- Provide the capability to use the following map types:
  - NIMA's SIPRNET web site
  - Geo-registered base maps used by installation Public Works/Civil Engineering departments
  - Commercial mapping programs
  - Manually geo-registered map images
- Provide a means to insert maps into incident folders.

Web Site Monitoring

- Provide a location for a list of recommended web sites for the incident or associated information.

WMD Events and Industrial Accident Situations

- Provide a means for reachback to obtain assessment of WMD event and industrial accidents impact.
- Provide a means for system calculation of WMD event and industrial accidents impact.
- Provide a means for immediately promulgating all WMD/I&W information as a preventative measure against possible multiple attacks.

This page intentionally left blank.

8.0 MTAC/ASOCC FITNESS CONCLUSIONS

In this section we first examine the correlation between MTAC processes and requirements and ASOCC capabilities, then comment on MTAC used of the system, including some recommendations. This is followed by some comments on NCIS's interaction with other centers.

8.1 NCIS PROCESSES AND ASOCC CONOPS CORRELATIONS

The ASOCC CONOPS was written to describe how the hardware system would be used to support Crisis and Consequence management during a terrorist attack event. Operations center processes are noted, primarily to describe how ASOCC will support them, but the processes themselves are not discussed. Above we have provided descriptions of pertinent MTAC and Field Agent processes. We merge these processes and examine Fitness between them and ASOCC capabilities in this section. This section focuses on:

- Can ASOCC support the full range of MTAC information processes?
- Can ASOCC support the full range of Field Agent information processes?
- Is ASOCC adequate for those processes it could support?

In order to answer these questions, correlations between MTAC processes and ASOCC CONOPS are identified for the following elements:

Purpose/Objectives
High-Level Functions
Operational/Tactical Actions
System and Process Requirements and Capabilities

We first discuss each of these areas then present the Fitness Table.

Associated questions arise because the existence of ASOCC in MTAC opens the possibility of participation more directly in real-time, terrorist-event activities, and becoming more directly involved in HLS.

- Should MTAC expand its activities to provide support to HLS?
- Should MTAC expand its activities into real-time situational awareness and I&W?

8.1.1 Broad Purpose, Objectives

ASOCC is designed to support information input, access, display, and exchange, and collaboration for decision-making. MTAC's principal activities are such information processes and the correlation between ASOCC CONOPS and MTAC processes at this level is natural and expected. This does not mean that the specific design of the system matches the cohort with which NTAC works. The following general comments are appropriate:

- ASOCC's collaboration capabilities could improve the workflow of both MTAC watchstanders and analysts.
- ASOCC's capability to display large amounts of diverse information for easy comprehension could aid MTAC near-term and real-time analyses.

8.1.2 High-Level Functions

ASOCC supports four high-level functions. Two correlate with MTAC functions:

- Collaborative course-of-action planning (MTAC match)
- Crisis and Consequence Management execution (Not an MTAC function)
- Situation monitoring (MTAC match)
- Response asset readiness monitoring (Not an MTAC function)

Collaborative Course-of-Action Planning and situation monitoring, and analyses that are required for both, are MTAC responsibilities. Currently these responsibilities are pre-event and longer-range than the support ASOCC is designed to provide. ASOCC is designed for real-time information and collaboration capabilities, for crisis planning/deterrence, and for C2 during the Consequence Management phase of an event. Even so,

- a system designed for short-term, real-time support can also provide support for longer-term processes.

In order to determine if use of the system for MTAC's current activities, the following need to be examined:

- Manning required for using ASOCC for daily operations.
- Whether the distribution of ASOCC systems is sufficient to support MTAC activities.

Later in this Section we discuss the possibility of MTAC expanding its mission go fully support HLS. If that is done, it would expand its operations to become more involved in real-time information and assessments in response to the emerging CONUS threat environment. Then

- ASOCC would provide the capabilities needed for this mission with the exception of deficiencies that are noted below.
- SOPs would have to be written for this mission, both for use of ASOCC and for other HLS processes using current information exchange means.

8.1.3 Operational/Tactical Actions

MTAC and NCIS Field Agents have responsibilities for:

- Providing assessments to naval units
- Collaboration with other agencies to develop assessments
- Collaboration with Operations Centers
- Interaction with local authorities

ASOCC can support all of these activities, with the caveats noted below. In addition to these, the system is designed to support

- ID through engagement of specific threat objects
- Real-time situation monitoring

<u>Providing Assessments to Naval Units</u>

MTAC has the responsibility to provide a variety of assessments and warnings to naval units, including ships. The types range from Threat Assessments, which are long-range and general, to Blue Darts, which are specific and initiate immediate action.

- ASOCC can provide a distribution means to those units that have the system.
- Current means, primarily message traffic, will continue to be required.
- Having parallel means for distribution is an advantage. Redundant paths will be needed when one path is unavailable.

Collaboration With Other Agencies To Develop Assessments

A significant portion of MTAC's information input comes from other agencies. Most of this information is at the TS/SCI level.

- ASOCC cannot support information at the TS/SCI level.
- ASOCC Chat collaboration tools at the Secret level would benefit assessment operations.

Collaboration With Operations Centers

MTAC currently coordinates with a number of centers, e.g. ROCs, JITTF. This is currently done to both obtain and provide threat information.

- AOCC will be at many centers and can implement instant, multi-person collaboration for operational and tactical purposes.
- Assessments could be speeded with use of the system.
- Availability of side-by-side Secret and Unclassified collaboration could aid fusing both types of information.

Interaction With Local Authorities

I&W and real-time Force Protection information can come from a variety of sources, including unclassified such as local police or even civilians. Current NCIS interaction with local authorities is primarily through Field Agents and Field Offices.

- ASOCC being located in EOCs could speed access to local threat information.
- Field agents will most often not have direct access to these systems.
- Local information is filtered through a Field Office (first-level assessment by subject-matter experts), which will not have an ASOCC system.
- There is no process for direct MTAC access to locally produced information.
- It is unclear how local information, vetted for assessment, would be placed in ASOCC and how, when, and by whom.

ID Through Engagement Of Specific Threat Objects

ASOCC has considerable capabilities to identify and track threat objects and to distribute that information to local and regional response elements. Tracking such objects in real-time is not an MTAC responsibility. However, it is an MTAC responsibility to monitor and assess the threat environment and knowledge of anything that contributes to that environment is of high interest, e.g. a ship that is suspected of carrying WMD.

- ASOCC's presentation of threat tracks could aid assessing the threat environment.
- ASOCC may not be in operation and presenting tracks during the pre-event phase.

Real-time Situation Monitoring

This is only a marginal MTAC responsibility, while a major focus of ASOCC. MTAC does not participate in terrorist-event, tactical C2.

- Involvement in tactical C2 would be a major addition to MTAC responsibilities.
- MTAC does have the responsibility to monitor all information to assess current threats and provide warnings.
- The information used for tactical C2 can be important for assessing immediate threats, even beyond the current incident.

8.1.4 System Capabilities

The ASOCC CONOPS specifically address requirements for, and the system has solutions for:

speed of information access,
information fusion (presentation for fusion, not the process),
situation assessment,
widespread information dissemination, and
speed of collaboration.

- The system fully meets these requirements for real-time Consequence Management.

ASOCC does not meet MTAC operations requirements for:

- Automatic generation of Navy messages and/or e-mail.
- Field Agent connectivity to SIPRNET when ASOCC is not available to them.
- Availability at all naval units.
- TS/SCI information sources and collaboration.

The first two MTAC requirements could be accomplished within ASOCC with some additional system development. The second two are unrealistic. This implies

- ASOCC cannot replace existing MTAC process means. It would have to work in parallel with them.
- This is not a serious restriction. Regardless of the support provided by the system, the requirement to use existing means will remain.

It is unclear whether NCIS Field Agents will have access to ASOCC, probably not. These Agents are an important source of information, both I&W and real-time. They also provide information directly to ships and installations and play a key role in ship Force Protection overseas. Because of these responsibilities, and their possible need for rapid communications, consideration must be given to how they carry out their duties when ASOCC is in use.

- There are no means determined for Agents inputting information to ASOCC.
- There are no processes for ASOCC distribution of SIRs and Spot Reports.
- There is no process for Field Office or MTAC verification of information in ASOCC.

There is a classification spectrum for MTAC information, both input and output: TS/SCI. Secret, and a small amount of Unclassified. The amount of Unclassified would increase if MTAC became actively involved in HLS. Much of MTAC information exchange and collaboration for I&W is at TS/SCI. Messages that are sent to naval units are at the Secret level.

- MTAC cannot share TS/SCI information using ASOCC because it does not operate at that classification level. This is a significant restriction that reduces the value of ASOCC for MTAC.

8.2 COMMENTS AND RECOMMENDATIONS ON ASOCC USE

Review of the ASOCC Draft CONOPS has raised issues both with regard to ASOCC use and concerning possible additional MTAC responsibilities, especially with regard to possible involvement with HLS. We explore both here, including actions that need to be taken in order to make any transition viable.

Parallel Paths

As noted above, the requirement to disseminate information from MTAC to naval forces via message traffic will remain regardless of other means that are put into place. E-mail is also extensively used for alerting. Thus, if ASOCC and existing means are to operate in parallel:

- Single-point-entry is needed.
- If there is no automatic means creating messages and e-mail from single-point-entry, the amount of work to be done in MTAC will be increased by inclusion of ASOCC paths.

Benefits to MTAC from having the ASOCC path also available are:

- Current messages and e-mail paths can be slow.
- Use of ASOCC and associated alerting could speed the information processes.
- Availability of ASOCC could provide an alternate path when current means are down.

Future Context

Most crucial at this point is deciding how extensively MTAC will support HLS. How ASOCC will be used and what resources will be devoted to its use depend on this decision. The following needs to be done.

- Determine what role MTAC will play in HLS.
- Determine what new processes this involvement will introduce, if any.
- Determine which of these functions will be supported by ASOCC.

The current ASOCC CONOPS and contained SOPs are fairly complete for Crisis and Consequence Management. They do not address many MTAC requirements, which is not a shortcoming of the document but a natural consequence of the fact that it was not written for this purpose. A precursor to use of ASOCC by MTAC is to:

- Develop new MTAC SOPs
  - For use of ASOCC in parallel with current means for current processes.
  - HLS responsibilities.
- Develop ASOCC SOPs specific to how it provides NCIS support.
  - For placing SIRs, Spot Reports, SARs, etc. in ASOCC.
  - Field Agent access and use.

Personnel Requirements

ASOCC manning requirements are unclear. Manning depends on how it will be used, which depends on some of the above factors. It is expected that decisions on how ASOCC will be used will depend on whether needed manning can be supported. The following needs to be done.

- Determine ASOCC manning requirements for various use configurations.
  - Full 24/7 support for MTAC daily operations.
  - Support for only new HLD operations.
  - Use of the collaboration capabilities for daily analyst operations.
  - Use of the collaboration capabilities by watchstanders.

System Improvements: Fusion of Real-Time and I&W Information

Pre-terrorist-event I&W information can be valuable for evaluating the current situation. This could be information acquired and processed for as long as several months before an event.

Such information needs to be fused with that obtained during the event. There is currently no archive location or process for doing this.

- Develop a means for inputting, archiving, and retrieving long-term I&W information in ASOCC.
  - A permanent archive.
  - A classification scheme so that pertinent information can be identified.
  - A means for extracting that information which applies to the current situation.
  - A means for displaying that information which applies to the current situation.
- Develop SOP for fusing I&W and current event information for real-time analysis.

System Improvements: Alerting Naval Units to Threats

The current alerting system in ASOCC needs modification and additional capabilities. The following should be provided:

- A means to go directly from an alert to pertinent information.
- Visible alert status for the sender, e.g. has it been opened and acted on.
- Visual time of entry and status for all ASOCC users
- Prioritization scheme.
- Direct alert to the recipient for directed information.
- Provide special section for official information, such as SAR, SIR, Blue Dart.

As procedures currently stand, Field Agents will have to phone in information to an EOC or an NCIS coordinator in order to get it into ASOCC. In the near future they will have available RASP systems so they can send classified information from the field directly to NCIS or MTAC.

- A means is needed for this information to go directly to ASOCC when Agents use RASP.

8.3 ASOCC IN COMBINATION WITH OTHER NAVY SYSTEMS

The combination of MTACs I&W information, real-time local threat information, and local sensor information for SA, produces a broad spectrum that no single current system is designed to accommodate. This opens the possibility of using more than one system to meet requirements. Ideally, one would like a fusion of existing systems.

Requirements for a system-of-systems are:

- Support TS/SCI I&W information.
- Have a means for transferring information across classification levels.
- Be accessible to all naval units.
- Ingest and display sensor information.
- Provide a Common Operational Picture (COP) for shared Situational Awareness.
- Support multiple levels of C2.
- Contain human friendly GUIs for rapid situation assessment.
- Have archive and retrieval capabilities for analysis.

The Navy currently has systems that collectively meet all of the above requirements, with ASOCC adding the needed COP and SA at the local level. For example:

- Joint Fires Network (JFN)
- Tactical Exploitation System- Navy (TES-N)
- Collaboration at Sea (CaS)
- Global Command and Control System (GCCS)

These are chosen these (there are others) for illustration because the first two support Navy Fires and the last two provide access throughout the Fleets. Navy Fires processes have some correspondence to what needs to be done for the HLS and Navy Force Protection operations noted in this report.

JFN methods and systems may provide some solutions for MTAC. Compatibility with ASOCC would be needed, which is not technically difficult.

Much of MTAC's information and collaboration is at the TS/SCI level. If network solutions are to be used for information dissemination at the Secret level, a means is needed to move information between these levels. JFN includes TES-N (TS/SCI) for image exploitation and ADOCS (SECRET/NOFORN) for target execution. The following capabilities exist:

- TES-N processes TS/SCI information and passes Secret target information to ADOCS for target exploitation.
- TES-N can also pass information to GCCS for SA.

Thus, technical solutions for the exchange of information across classification levels exist. It is germane that

- ASOCC has capabilities for import of information from GCCS.

Solutions are available that, in combination, could meet all of MTAC information requirements. This does not mean that it will be simple to hook the various components into a complete system that meets these requirements. The next subsection deals with a possible road ahead.

The need to provide information to all naval units is a significant consideration for any system supporting MTAC operations. ASOCC will not be available at all locations with which MTAC has to exchange information. We assume that network-based information systems are the wave of the future and moving toward that type of solution is needed. Most challenging are small ships at sea, which have intermittent internet connectivity and limited bandwidth. The Collaboration at Sea system exists on essentially all Navy ships. It is a replication system that updates information files whenever a ship has connectivity and logs on.

- CaS is not directly compatible with ASOCC, JFN, or its variants and it would be somewhat cumbersome to use for this application without modifications.
- However, it illustrates that network solutions to widespread distribution are available without starting from scratch.

8.4 RECOMMENDED PROCESS MODELING

This work has expanded beyond examining support that ASOCC, a system designed for other purposes, can provide for current MTAC processes. The discussion has ranged from the requirement to reach all naval units to possible new missions to support HLS. Included has been the possibility of combinations of ASOCC with existing systems, none of which are currently

used by MTAC. Sorting all this out so that a sensible way-ahead can be determined is complicated.

We have suggested a possible solution to meet all requirements that makes use of several systems. Those systems have been designed for other purposes, are different programs, and none have considered MTAC processes. A process to look at available solutions together, with a primary focus on MTAC Force Protection responsibilities, is needed.

The means by which such studies are carried out is process modeling. It is recommended that such a study be undertaken to determine appropriate solutions for the full spectrum of MTAC and Navy Force Protection. The study would include how to utilize a combination of systems and processes. Without such a study, sorting out how best MTAC can support full-spectrum FP, including HLS, will be difficult.

Such work is simplified by modern methods that allow one to modularize processes. One would build modules that represent operational processes, FP and Fires primarily. The modules would have layers so that information flow and decisions would be transparent. MTAC would probably be a module of its own. The focus would be on information flow and how proposed systems support that flow. The techniques to perform such a study are well known and software is readily available to streamline the study.

Note that even the ASOCC CONOPS alludes to such a study in their recommendation that information flow diagrams are needed as a basis for CONOPS and SOP development. The DRAFT CONOPS contains the statement, added by the authors as an edit: *"[Information clutter management needs to be figured out. Much larger issue is strategy of information flow up the chain. Diagram "ASOCC INFORMATION FLOW PATHS" is a start. Supporting logic needs to be drafted.]"* This reprot concurs with the statement's implications and recommends that information flow diagrams be developed to:

- Map non-ASOCC MTAC information paths.
- Map MTAC information paths assuming ASOCC and current means used in parallel.
- Map MTAC/ASOCC information paths for any new processes to support HLD.

Process modeling would follow and use these information flow diagrams

8.5 INTERACTION WITH OPERATIONS CENTERS

The JHOC CONOPS contains elements describing how that Center will support Crisis and Consequence Management operations, and describes information tasks which will be supported by ASOCC. The CONOPS was written for that Center's operation, and does not include processes that involve MTAC.

An underlying assumption of the CONOPS, and the processes described by the MIDLANT ROC personnel, is that Operations Center (OC) interaction with NCIS will remain as is. It is currently through the Field Office or a Field Agent assigned to the OC and sitting in the Center during a crisis operation. There is no direct interaction with MTAC. The presence of ASOCC potentially changes this. If MTAC expands its operations in response to HLS, overlap of responsibilities

will increase. Thus, it is appropriate for this study to consider OC operations and how MTAC may interact with them. JHOC is used as the example for this discussion.

MTAC Shared Responsibilities with JHOC

MTAC has the responsibility to provide I&W information to Navy units, including ships. JHOC will necessarily communicate with Navy ships that are in or approaching the harbor and a Navy Watchstander may be in the JHOC during a crisis situation. It is not currently specified how the responsibility for alerting naval units will be shared. The CONOPS refers to the services having TACON over their assets, but this doesn't clarify who supplies, or how, the following types of information:

a. Standard I&W.
b. Force Protection, real-time terrorist threat.
c. Local, multi-component Situational Awareness.

For a: Providing standard I&W is a current MTAC responsibility and they have means for doing so for several levels of warning. This includes Force Protection information.

For b: The situation with real-time information is unclear. Agents in the field communicate directly with ships and shore installations during a crisis so real-time information may not go through MTAC.

For c: Local, multi-component Situational Awareness information is not currently an MTAC responsibility.

Overlaps exist but there are functional differences. MTAC functions are inherently longer range. The JHOC deals with events immediately before and as they are occurring, whereas MTAC focuses on longer-range analysis and planning. Again, a central question is whether MTAC will become more involved in real-time information and assessments. If it does, the overlap will be significant.

The operational and tactical actions planned for a JHOC include ID through engagement of specific threat objects. These are not MTAC responsibilities unless the ID function extends back in time to threat I&W. If it does, MTAC has a role to play. That role would be the assessment one it now plays and promulgating threat information. Presumably, it would pass such information to the JHOC, which would then fuse it with their real time information.

- SOPs for how information exchange and collaboration between MTAC and OCs are needed.

The JHOC CONOPS discusses operations during the time the Center is in operation, which is immediately preceding or during an event. There will be a pre-event phase where I&W is the primary activity. Information from this phase will be a key component of what JHOC has initially available. MTAC will play a major role in providing such information.

- Procedures for making this information available and installing it within JHOC are needed.

The JHOC CONOPS lists several needed databases, but there is no reference to NCIS information. Information in SARs, SIRs, Spot Reports, etc, will be needed by a JHOC.

- SOPs need to be developed to make this information available to the JHOC.

The requirement to disseminate information from MTAC to naval forces via message traffic will remain regardless of other means that are put into place. Whether or not JHOC CONOPS, SOP, or TTP should address this is not clear.

- MTAC SOPs are needed for situations where a JHOC is in place and information exchange with them is required.
- There is, as yet, no indication of how these tasks would be shared between MTAC and a JHOC. This needs to be clarified as SOP are developed for all phases of terrorist events.

APPENDIX A ASOCC 12 MAY 03 DRAFT CONOPS

Area Security Operations Command and Control (ASOCC) System
Concept of Operations
For Homeland Security/Homeland Defense

Navy AT/FP Testbed
12 May 2003
Ver. 1A

Table of Contents

BACKGROUND

Overview

A continuing concern for the United States is the threat of additional terrorist attacks against its critical infrastructure, historical landmarks, civilian populations, and military facilities both at home and abroad. The Navy is taking aggressive action to reduce and counter the threat of additional small boat attacks such as the one that seriously damaged the Aegis guided missile destroyer USS COLE in Aden harbor on 12 October 2000. Since that time there have been indications that Al Qaeda might be planning to replicate that attack, which remains a classic case of asymmetric warfare, and to exploit other critical vulnerabilities against other naval assets and maritime centers of gravity. The proliferation and increasing lethality of weapons of mass destruction (WMD), for example, has added new and frightening dimensions to the problem. As communication, logistics, and other related systems become more sophisticated and interconnected, they also become more vulnerable to disruption, not only from terrorists/SOF but also from industrial accidents and natural disasters. Consequently, the need has never been greater to combine the strengths and resources of U.S. military forces and civilian intelligence and law enforcement agencies to deter attacks and mitigate the impact of attacks, accidents, and natural disasters.

The missions of the Navy and naval components of the Unified Commands requiring command and control of facilities ashore include foreign and domestic Antiterrorism/Force Protection (AT/FP), Homeland Security (HLS) and Homeland Defense (HLD). The goal of a Navy C4ISR technical architecture is to support these missions with guidelines for a robust and flexible infrastructure that is compliant with applicable technical standards to ensure both the wide-ranging interoperability and the security required for these missions. A unique feature of these missions is the requirement to collaborate with DOD, Federal, State and local authorities within the borders of the United States, as well as with coalition forces beyond our borders to deter, prevent, prepare for, respond to and recover from terrorist attacks, major disasters and other emergencies. Governing policies, doctrine and plans include Homeland Security Presidential Directive 5 (HSPD-5), Joint Pub 3-10 Doctrine for Rear Area Security Operations, The Interagency Counterterrorism CONPLAN and the Federal Response Plan.

The **Area Security Operations Command and Control (ASOCC)** system addresses the need for an effective C4ISR architecture to support command and control of joint antiterrorism / force protection (AT/FP) efforts and to coordinate such efforts with other DoD components, other federal, state and local agencies and s. The fully integrated GOTS and COTS software that makes up the ASOCC tool kit is the product of a multi-component integration and configuration effort by DISA in support of Joint Staff validated requirements for execution of AT/FP operations under Joint Pub 3-10 [series]. It integrates and streamlines the flow and processing of information to enable commanders, coordinators, security forces, and first responders to make quicker and better-informed decisions related to planning base defenses and security operations; and responding to attacks, accidents and natural disasters. It provides multi-echelons of command with security responsibilities and a means to:

- Deter terrorist surveillance activity by integrating event trigger and remote sensor feeds to provide real-time logging, alerting and event visualization capabilities.

- Conduct secure, multimedia collaboration between echelons, agencies and organizations to enhance understanding of potential threats, provide warning, direct force protection-related conditions and measures, and report status of achieving those directions.

- Assemble and share a common and complete tactical picture of the threat environment; and the location and status of friendly security forces, operations, critical assets and infrastructure.

- Directly support the security forces at the installation level by providing a means to potentially incorporate the inputs of and collaboration with other first responders (e.g. local law enforcement, fire department, medical, etc.), enhancing the comprehensive response to incidents of concern.

Joint and DOD Drivers

The mission need for improved AT/FP and related C2 capabilities was codified in the wake of the USS Cole incident when increased attention was placed on improving DOD's ability to prevent, prepare for, respond to and recover from terrorist attacks, major disasters and other emergencies threatening DOD installations overseas. Joint Pub 3-10 Doctrine for Rear Area Security Operations and the Global C2 Management Structure, outlined in CJCSI/M 6721, provided the CONOPS and requirements underpinnings that enabled rapid deployment of initial C4ISR capabilities conformant with joint architecture and policy. JP 3-10 continues to provide good insights for structuring command and organizational relationships to coordinate AT/FP and complements direction to define "a core set of concepts, principles, terminology, and technologies covering [an] incident command system…" as outlined in Homeland Security Presidential Directive Nbr. 5 (HSPD-5). HSPD-5 further directs all federal agencies to ensure that their systems are interoperable with National Incident Management System (NIMS) standards to be specified by DHS in compliance with HSPD-5. With ASOCC, the Navy's continuing efforts to deploy Ashore C4ISR capabilities are able to build on Joint requirements and architecture as documented in the Joint Staff's Global Requirements Identification Database (GRiD), with allocated requirements documented in the AT/FP Joint Allocated Requirements Repository (JARR).

Scope

The purpose of this CONOPS is to describe the features of the ASOCC system (to include those envisioned as future capabilities within the scope of the current development cycle), the architecture in which it will operate, and the concept of how users will employ it to support their operational requirements. This CONOPS focuses on force protection within CONUS-based AOR (e.g. Homeland Security/Homeland Defense assets). A separate CONOPS is envisioned to be developed (as required) to address issues associated with utilization of a C4ISR system in support of the Joint Rear Area Command (JRAC) environment for expeditionary forces.

SYSTEM ARCHITECTURE

ASOCC does not work from a central database, but rather is primarily a client-server system topology with the capability for workstations to operate autonomously using data stored locally if communications paths are lost or degraded. Clients can retrieve data directly from other workstations (commonly referred to as a peer-to-peer relationship), and all clients are able to access specific, remote databases (security classifications allowing) via servers that are not part of the ASOCC system itself (See Figure 1). Clients needing classified information will use the SIPRNET over existing connections. Remote clients can access an installation's NIPRNET via Dial-up and the establishment of a Virtual Private Network (VPN.)

ASOCC supports different types of users. The first is at the installation level, horizontally among security forces' nodes, command nodes, and eventually various other first responder nodes; the second is vertically from the installation level up through multiple echelons of command.

At the installation level, ASOCC supports nodes dealing with the tactical security problem on and immediately around the installation. It will operate over the NIPRNET in an Unclassified/FOUO security environment, protected by the installation's network firewall and other security measures. Workstations can potentially be located at a command's Emergency Operations Center (EOC), Security Forces' Operations Center (SFOC); a Joint Operations Center (JOC); ships in port; and other first responder nodes on or near the installation (e.g. fire department, civil engineering, medical, etc.)

To support multiple echelons of U.S. command and coordination ASOCC workstations will be located in Operations Centers at the Regional and Echelon One levels. These workstations will operate over the SIPRNET in a classified (SECRET) security environment.

Security Classification Considerations

ASOCC workstations will have to operate in one of two security environments: Classified, (SECRET level) operating on the SIPRNET; or Unclassified, operating on the NIPRNET.

An automated Multi-Level Security (MLS) system is the preferred method for transferring appropriately classified information between the two security domains, however, there is currently no appropriate and accredited MLS available for use on ASOCC. Transfer of information between these two air-gapped domains will be handled by disk transfer until an approved MLS system is in place, (see Figure 1).

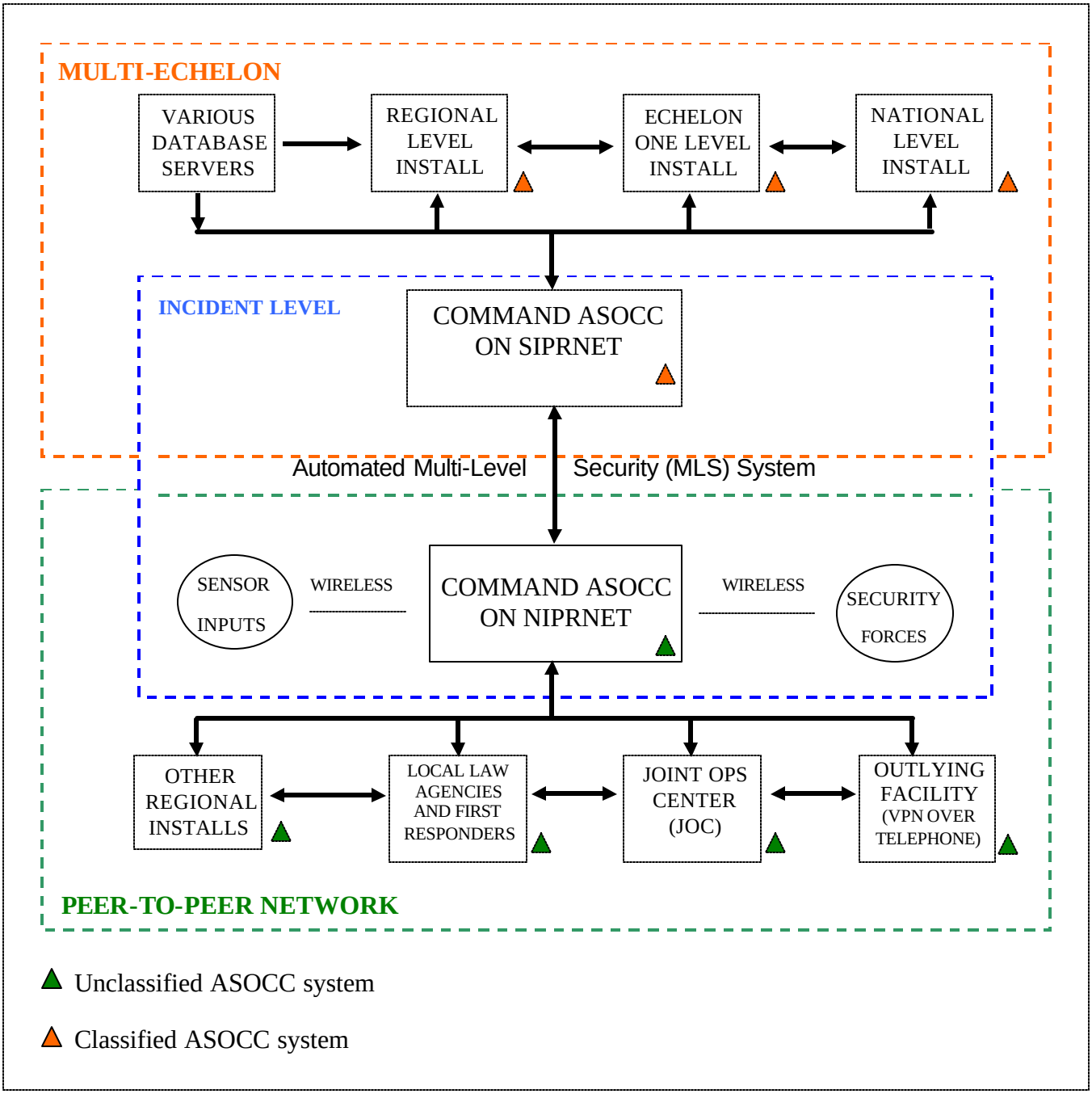


FIGURE 1 – ASOCC ARCHITECTURE

SYSTEM FEATURES

The ASOCC software applications operate on a normal personal computer with sufficient capacity and with a single VGA monitor or an integrated 3-monitor (preferred) configuration, (see Figure 2). The ASOCC software applications are added to the PC, which functions on the command's LAN as any other workstation.

The **3-screen configuration** of a standard ASOCC workstation allows all of the ASOCC tools to be working and displayed simultaneously.

Figure 2. ASOCC's 3-screen configuration.

ASOCC consists of a series of tools that allow users to:

- Conduct real-time audio, chat room, white board, and file sharing collaboration with other users (Defense Collaboration Tool Suite-DCTS),
- Monitor multiple web sites of interest (KnowledgeBoard),
- Update and monitor status boards on force protection and other security-related conditions (eX-Panel),
- Update and monitor status boards on critical infrastructure and assets (eX-Panel),
- Update and monitor status boards on security forces (both U.S. and) (eX-Panel),

- Pull geo-registered data, overlays, and maps from multiple local and remote databases, and integrate them to produce a locally tailored, but common tactical picture of the AOR. Integrate this with user-generated information on incidents with force protection implications (eXtensible Information Systems- XIS),

- Share information on incidents with force protection implications (multiple applications),

- Import non-geo-registered imagery and mapping products, and feeds from remote sensors to enhance situational awareness (Java Imagery and Video Exploitation-JIVE),

- Provide warning, direction, and coordination (eX-panel),

- Calculate and share information on areas potentially and actually affected by WMD events, natural disasters and industrial accidents (Consequence Assessment Tool Set - CATS/XIS),

The eX-Panel is the central menu from which to access other applications, maintain electronic log entries on events and incidents of force protection interest, send warning information, direct FPCON and other condition changes, and update status boards.

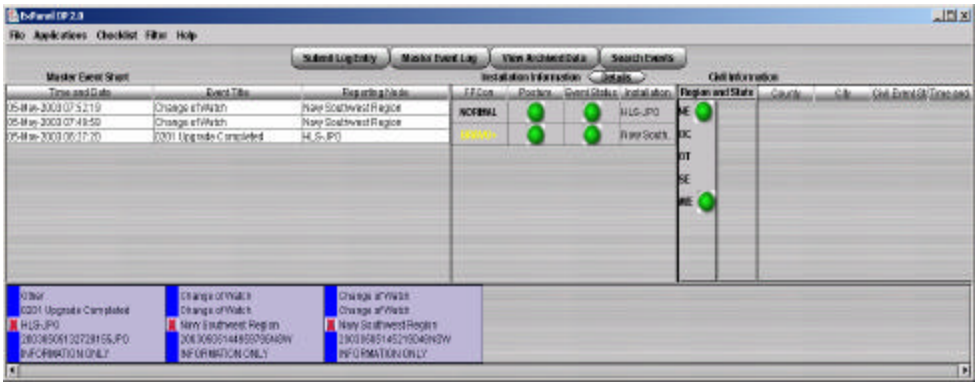


Figure 3. ASOCC's eX-Panel display.

These log entries are then automatically distributed to other ASOCC users via peer-to-peer relationships over the SIPRNET or NIPRNET. This is the primary means of disseminating information on incidents that will make up the common tactical picture among ASOCC users. Event Log entries that have positional data associated with them can have that data displayed on a geographic display. The eX-Panel also features system-generated alerts and user-defined checklists linked to specific types of reported events.

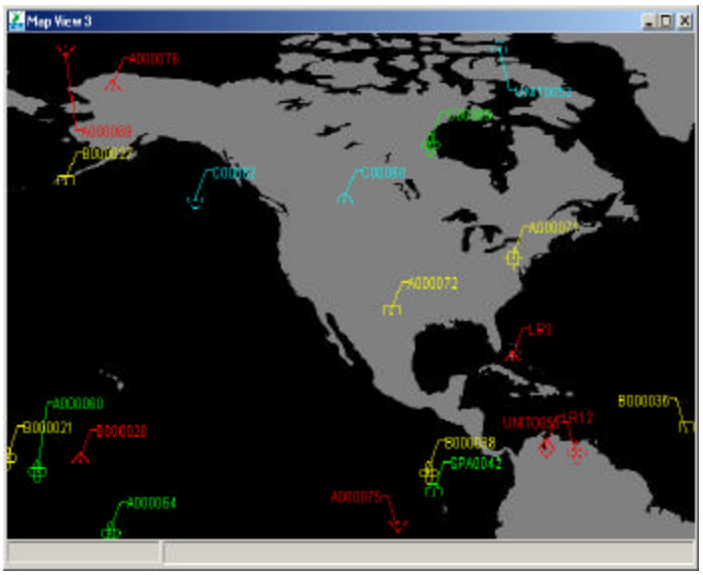


Figure 4. Extensible Information System (XIS) Tool.

The Extensible Information System (XIS) is the primary situational awareness visualization tool in ASOCC, and provides a means to import geo-registered data from a variety of databases and integrate it to form a consolidated graphical tactical picture. This provides an operator with the ability to keep track of activity in the AOR through the use of geo-registered maps and images, incident locations from the Event Log, critical infrastructure status information from local and shared databases, etc, (see Figure 4).

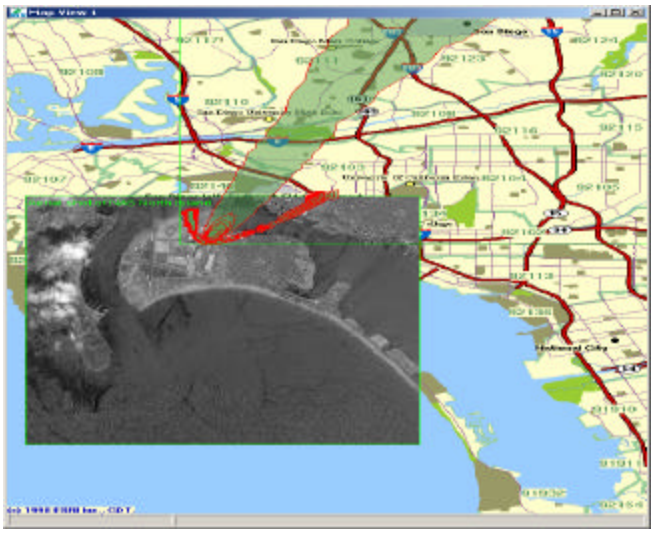


Figure 5. Consequence Assessment Tool Set (CATS)

Within XIS is the **Consequence Assessment Tool Set** (CATS). The CATS tool set enables the display of plume models, providing the ASOCC operator the ability to assess the potential effects of WMD and industrial accidents, (see Figure 5).

Defense Collaboration Tool Suite (DCTS) is a means for multiple ASOCC users to conduct real-time video, audio, chat room, and white board collaboration, and file sharing. This can be done over secure or non-secure paths. (See Figure 6.)

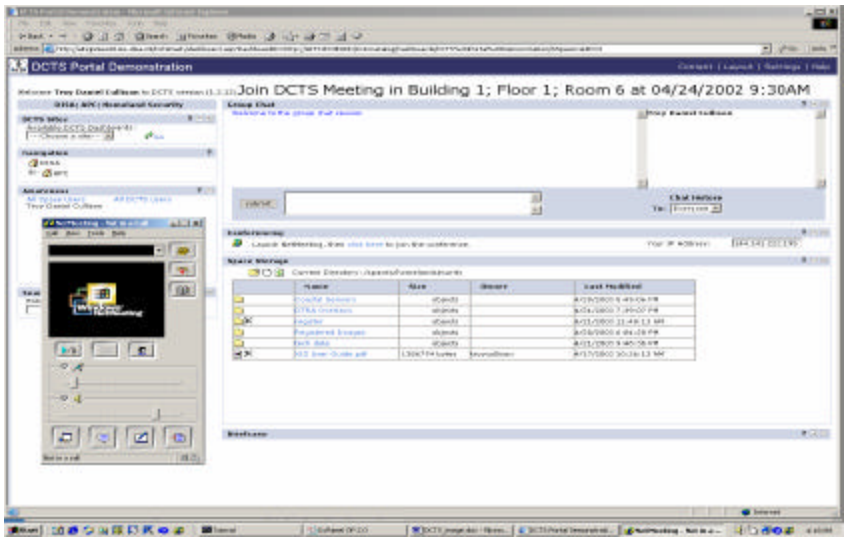


Figure 6. Defense Collaboration Tool Suite (DCTS)

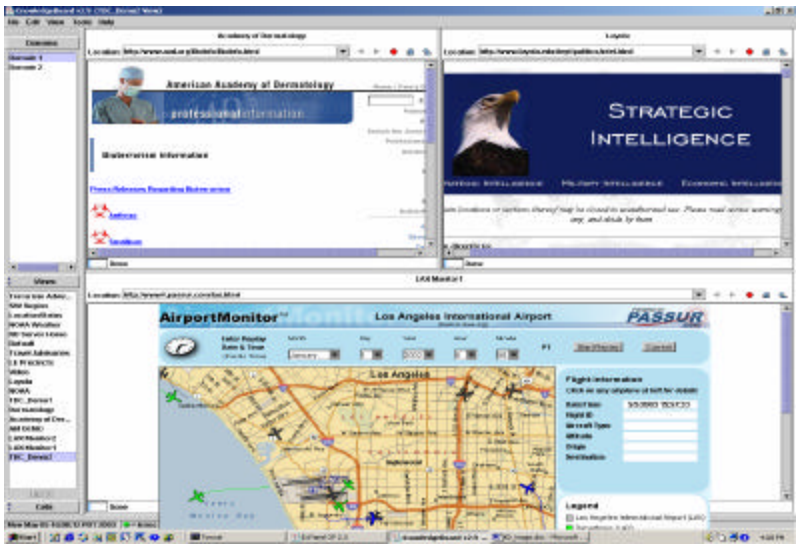


Figure 7. KnowledgeBoard

KnowledgeBoard enables users to simultaneously monitor up to nine user-defined web sites, and automatically refreshes the view of the web pages being monitored at user-defined intervals. This feature is ideal for monitoring intelligence and weather web sites to which new and updated information is often posted, as well as monitoring web-based status boards. (See Figure 7.)

The JAVA Imagery and Video Exploitation (JIVE) tool enables users to import images in a variety of formats and to manipulate and annotate them for better situational awareness/collaboration purposes. JIVE also enables users to import video, for example real-time feeds from a UAV; thus enabling multiple and geographically separated users to view the same picture. (See Figure 8.)

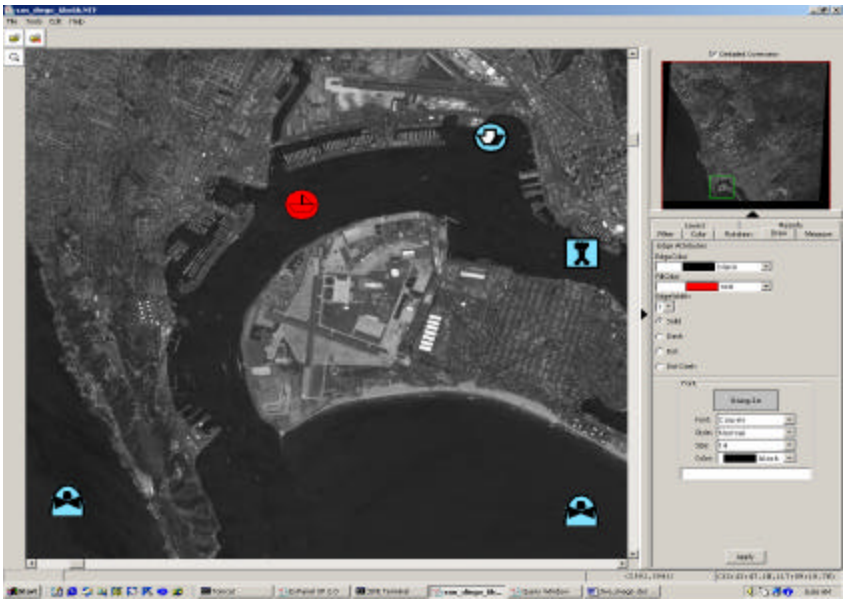


Figure 8. Java Imagery and Video Exploitation (JIVE)

Summary

The ASOCC system provides the C4ISR backbone that permits the integration of sensor data, intelligence information, and decision/analysis aids into a shared, fused, real-time, common operating picture. This system permits the rapid exchange of pertinent information with both vertical and horizontal connectivity among each responsible activity or command, resulting in the:

- Enhanced prevention opportunities to potential threats
- Timely reaction to emergent crisis situations
- Efficient coordination of resources to execute decision plans
- Effective incident response through collaborative planning/decision-making

The complexity, scope and potential consequences associated with a terrorist attack, particularly in response to the use of Weapons of Mass Destruction (WMD), require that there be a rapid and decisive capability to assess and resolve the situation. The prevention / deterrence and defeat of a potential act of terrorism demands an extraordinary level of coordination, collaboration and sharing of technical expertise across all levels of government. Development and installation of a C4ISR system, coupled with sensors and alerted security forces, are key elements in providing for a meaningful AT/FP capability.

CONCEPT OF OPERATIONS

Introduction

This CONOPS is intended to provide a strategy for the integration and employment of ASOCC in support of a tailored, time-phased, coordinated response by Homeland Security/Homeland defense assets in response to a terrorist threat or incident. While it is recognized that several non-DoD agencies and local municipalities (for example: New York Port Authority, San Diego Port Authority, New Orleans Police Department and Louisiana National Guard, etc.) have already purchased and deployed ASOCC, this CONOPS exclusively focuses on Navy employment, and in particular, the current Phase I employment strategy (e.g. San Diego and Norfolk fleet concentration areas). This CONOPS does not supersede existing plans or organizational relationships that were developed for response to incidents under department and agency statutory authorities. This CONOPS does, however, attempt to identify how ASOCC would be used to meet the critical demands associated with the HLS/HLD mission. Other CONOPS assumptions include:

- Terrorist incidents may occur at any time of day, with little or no warning, and may involve a single or multiple geographic areas, and possibly result in mass casualties
- No single government agency at the local, State, or Federal level will possess the expertise to act unilaterally on the many difficult issues that may arise
- Agencies at all levels would need to respond on short notice in order to provide effective and timely prevention and/or response to a threat or incident
- Response operations might be require over a multi-jurisdictional, multi-State region, requiring Local, State, and Federal responders to coordinate responsibilities and actions

Mission

The Department of Defense is a support agency to the Department of Justice (with the Federal Bureau of Investigation acting as the lead delegate) for crisis management functions, and is a support agency to the Federal Emergency Management Agency (FEMA) for consequence management. In accordance with DoD directives 3025.15 and 2000.12, and the Chairman of the Joint Chiefs of Staff CONPLAN 0300-97, and upon approval by the Secretary of Defense, DoD will provide assistance to the Lead Federal Agency (LFA) and/or other primary agencies as appropriate, during all aspects of a terrorist incident, including both crisis and consequence management. DoD assistance includes threat assessment, operational and tactical support, and response to the presence of a WMD device.

Within the DoD/DHLS the U.S. Navy and U.S. Coast Guard have complimentary and overlapping Homeland Security/Port Security missions that require rapid and effective integration of protection mechanisms in cooperation with other local, State, and Federal agencies. The spectrum of agencies involved, and the acute need for a development of common situational awareness, collaborative course-of-action planning, and cooperative decision-making provides the impetus for ASOCC's C4ISR system.

Employment Scheme

The number of ASOCC systems available, the specific scenarios in different theaters, the requirements of the Global Naval Concept of Operations and other issues will affect how ASOCC is employed worldwide. Within CONUS however, it is envisioned that the Navy would install ASOCC terminals at key decision/collaboration points both within the "incident level" and the "multi-echelon level" hierarchies, (Figure 9).

"Incident level". Incident-level ASOCC sites/participants would be first critical C4I link between "first responders" charged with dealing with the immediate and short-term effects at the onset of an emergency or disaster, and the supporting local/State/Federal (civilian and DoD) organizations charged with executing larger scale responsibilities envisioned in the Federal Response Plan (FRP). ASOCC sites involved in the "incident level" would principally include:

- Joint Harbor Operations Center (JHOC) – manned by USN, USCG, and specified local law enforcement personnel. Both a Classified ASOCC terminal (e.g. ASOCC-High) and an Unclassified terminal (e.g. ASOCC-Low) would be onsite.

- Emergency Operations Center (EOC) – Often serves as the response team's "dispatch" center. Normally each local agency or regional State/Federal agency, such as Customs, Border Patrol, Local Police, County Sheriffs Department, Navy Regional Commander, have an EOC which is routinely manned 7/24 during peacetime operations. It is envisioned that some ASOCC-Low systems would be onsite or available to local municipalities and regional State/Federal agency EOCs.

- Joint Operations Center (JOC) – The term JOC is used by both the military and Federal agencies to identify a key decision-making command center used to manage and direct specified response activities. For C2F/C3F, which have specified coordination and supporting responsibilities within their AORs, both ASOCC-High and ASOCC-Low terminals would be available within their JOCs. When a Lead Federal Agency (LFA) designates a regional Federal On-Scene-Commander (F-OSC), they too are authorized to stand-up a JOC. In fleet concentration areas, (assuming appropriate MOAs are in place), the LFA-JOC could be co-located with the Navy Regional Commander's RCC/ROC, enabling a quicker C4I start-up, along with enhanced ongoing information-sharing and mutually-supported decision-making.

- Navy Regional Command Center (RCC) or Navy Regional Operations Center (ROC) – Depending upon the level, complexity, and immediacy of the crisis, a RCC/ROC would be stood up as ordered by the USN Regional Commander. This center serves as the key transition point between "incident-level" and "multi-echelon level" hierarchies. Both ASOCC-Low and ASOCC-High terminals would be available onsite.

"Multi-echelon level". Multi-echelon level participants would be provided a prioritized, pre-screened level of information to reduce clutter from routine traffic and to focus

decisions on higher level requirements (e.g. "information push"). Given that ASOCC is a peer-to-peer network, all information is available to be shared among all ASOCC workstations. Therefore if a Commander desired additional information on an event, it can still be accessed from the subordinate levels, (e.g. "information pull"). ASOCC sites involved in the "Multi-echelon level" would include:

- USNORTHCOM/ECH 1 Commands/LFA – The Federal Response Plan (FRP) identifies unique and specific responsibilities to each Federal Agency in response to an act of terrorism or other national emergency. For the purpose of this CONOPS it is assumed that the respective Operations Centers of these activities (e.g. National Command Center, Navy Operations Center, etc.) would have an ASOCC terminal, or the ability to easily integrate ASOCC software.

- NAVNORTH/JFMCC – The Unified Command Plan (UCP) designates NAVNORTH as the Joint Forces Maritime Component Commander (JFMCC) responsible for Operational Control of Maritime defense forces. The JFMCC would have an ASOCC-High terminal, with all ASOCC-Low data and video features mirrored to the High-side system.

- CPF/CLF – As Maritime Defense force providers each of these major commands would have both ASOCC-High and ASOCC-Low terminals.

Coordination/Support, Command and Control Strategy

ASOCC would operate throughout the continuum of operations as part of a distributed C4ISR network to include Navy, Coast Guard, Federal, State and Local emergency response agencies. Command and control of a terrorist threat or begins with the first response team, normally assigned by either a local law enforcement dispatch center (in the case of a civil attack) or a military security/police dispatch office (for DoD facility security). Depending upon the nature, complexity, and/or severity of the crisis, one or more local, State, or Federal agencies may become involved. The first response team would be normally lead by a local Incident Commander located either on-scene or at a JHOC or EOC. Depending upon the complexity, scope, and severity of the crisis, the local Navy Regional Commander would stand-up a Regional Command Center (also called a Regional Operations Center). This RCC/ROC serves as the transition point between incident-level crisis and consequence management/reporting and multi-echelon communication/decision-making/support. Since ASOCC is a peer-to-peer network, allowing permissive/approved access to all users for information being assimilated on the net, the concept of a command and control process, with strict hierarchies for reporting and communication, is not entirely applicable. Yet the ASOCC toolkit does provide commanders with mission-critical capabilities to plan, coordinate, integrate and manage AT/FP operations by integrating the efforts of the Joint Maritime Component Commander (JFMCC), CPF/CLF, C2F/C3F, other U.S. Combatant Commanders, Navy Regional Commanders, U.S. Coast Guard activities, and local/State/Federal law enforcement partners, (See Figure 9).

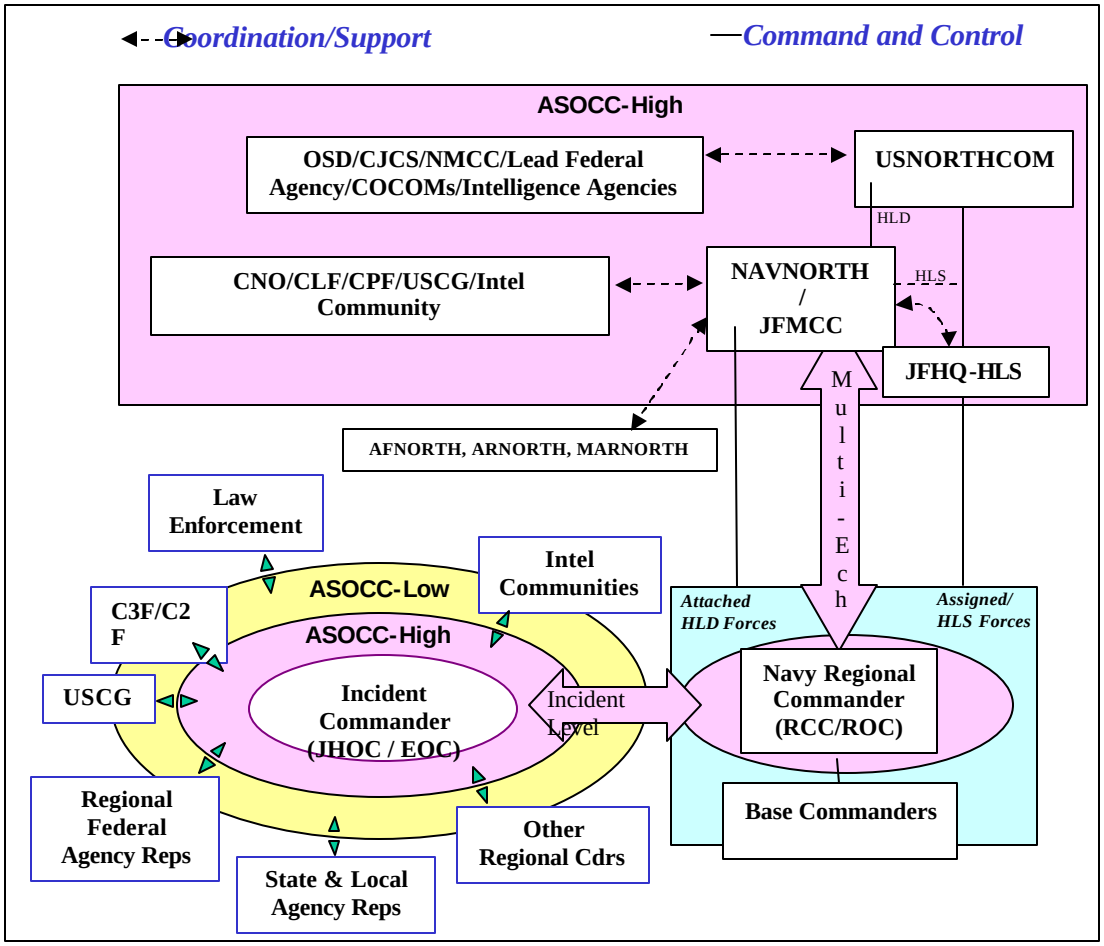


Figure 9. ASOCC Integration into HLS and HLD Missions.

Incident Level. At the incident level, both an Unclassified (e.g ASOCC-Low) and a Classified (e.g. ASOCC-High) network would be maintained. Sensor feeds coming from Radar, CCTV, Thermal Imagers, etc., would be fed into the ASOCC-Low terminals located at the JHOC, EOC, and RCC/ROC. The purpose of these sensor feeds is to aid incident-level nodes in visualizing the location and status of incidents, friendly forces and defenses, and to ensure proper and timely support by available resources. Local and State agencies such as local police, harbor patrol, fire department, etc., would have input and access to the ASOCC-Low network. Using this sensor network, along with inputs from security patrols and onscene observers, JHOC/EOC watchstanders would maintain a tactical picture of the area of interest, whether it be at a specific base installation, harbor, or facility perimeter. This tactical picture will consist, at a minimum, of:

- The location and identification of U.S. and supporting security forces.

- The location and details of events and incidents with installation security implications. Using the Event Log on the eX-Panel, these log entries will be linked to locally developed, interactive (future capability) checklists to expedite the taking and logging of actions.

- Information on events happening off-base. These will be entered into ASOCC by the federal, state and local agencies that maintain nodes, or reported via JOC channels.

Creation of incident reports in the ASOCC Event Log by JHOC/EOC personnel would provide a primary ("quicklook") information summary for use by higher (e.g. multi-echelon level) command elements.

JHOC/EOC personnel would also maintain database information on the location, identity and status of critical infrastructure and assets that is compatible with XIS (e.g. MS Access database or Oracle database) so that it can be displayed in XIS and shared with other users. These ASOCC watchstanders may locally create and use "overlays" for the tactical picture graphic display showing base defense, FPCON, and other contingency plans to aid in situation response.

If intelligence suggests the possibility of a WMD threat, or in response to an actual WMD event and/or industrial accident, ASOCC watchstanders would calculate and display graphic overlays of the estimated areas affected (using the CATS tool) and be responsible for reporting the incident in ASOCC. (Note: When other first responders have ASOCC, the fire department, disaster response group, or other designated incident-level organizations may be responsible for WMD event calculation and reporting in ASOCC.)

ASOCC watchstanders may also choose to designate chat rooms for collaboration in the Defense Collaboration Tools Suite and specify the purpose for each room. They can establish these chat rooms for constant monitoring and establish schedules for regular collaboration sessions involving key personnel or nodes.

Multi-Echelon Level. This segment of the CONOPS addresses the information requirements and C2 requirements above the incident-level. ASOCC workstations supporting this portion of the CONOPS will (generally) operate at classified security levels on the SIPRNET.

Tactical Information Requirements. Commanders, coordinators and intelligence analysts at all levels require information on incidents with security implications for a variety of purposes. This includes information on incidents occurring on or near U.S. installations, and in the entire AOR; and they all need to have the same information. They also require information on the location and identification of critical infrastructure and assets, and off-base operations.

While forces at U.S. installations will be the source of information on incidents occurring on or very near U.S. installations, JOCs and various Federal, State and local agencies will be the source of information on incidents occurring in the rest of the AOR. Regional Operations Centers (ROCs) (via their bilateral cells) are where information derived from regional level organizations will be entered into ASOCC for dissemination to all echelons (using the Event Log in the ExPanel).

Information on the locations and identities of critical infrastructure and assets are maintained by the installation command post/EOC. These local databases can be shared via file sharing in the DCTS and/or disseminated periodically via email, and displayed graphically using XIS.

Echelons above the installation level will routinely not have need of tactical information on the locations and composition of on-base security forces. There is, however, a need for general knowledge of the location and composition of security forces in the AOR, particularly those earmarked to support U.S. installations and those protecting off-base infrastructure critical to U.S. operations. ROCs, and JOCs will obtain this type of information from their counterparts, and enter it into local databases. As with the local critical infrastructure databases, these can be shared via the DCTS and displayed graphically using XIS. Alternatively, the location of forces can be displayed using the overlay palate of XIS; which can also be shared using DCTS.

Tactical type information originated on unclassified ASOCCs and in unclassified databases will migrate to the classified side at the JHOC/EOC or RCC/ROC. Both of these should have access to ASOCCs operating on unclassified and classified networks.

Sensor Integration

ASOCC is envisioned to serve as the C4ISR "backbone" for AT/FP "plug and play" sensor packages that can be changed, modified, or removed in a short period of time. ASOCC will provide space, common open architecture, and a common control system for these sensors. It is envisioned that while raw sensor inputs would be directed to the regional and/or functional workgroup servers within the "incident-level", all sensor information could be selectively "pushed" or "pulled" to any other functional group or ASOCC station within the network. For example, regional Border Patrol, Customs, or other Non-DoD law-enforcement organizations with an ASOCC station at their disposal, might be able to provide valuable cueing information on contacts or areas of interest to U.S. Navy and Coast Guard watchstanders at the JHOC, or Navy Regional Security personnel operating at an EOC. This intelligence and sensor information could also be selectively forwarded to multiple HLS/HLD echelons via NIPRNET, SIPRNET or DCTS collaboration.

Assessment Information Requirements

Another type of information required by echelons above the incident-level is detailed information on the status of security forces, and critical infrastructure and assets; and assessment-type information on them. This type of information is best conveyed using status boards with a drilldown to detailed information on numbers, types, capabilities, and assessments of assets. This type of information will be classified. The primary source of this information resides at the incident-level, which will maintain the status boards. Summary status boards and assessments presented by Service will be maintained at the regional level.

When U.S. forces are using civilian airfields and ports for HLD operations, the Service Component conducting the operations at that site will maintain status board and assessment information on those sites unless ASOCC connectivity with those locations can be attained, in which case the site will maintain its own status board and assessment information.

The initial CONOPS for sharing status board-type information is for each installation to maintain status boards on its SIPRNET web site. These could then be accessed directly and individually via the SIPRNET, or multiple sites could be monitored using the KnowledgeBoard tool in ASOCC. In the future, this type of status board function will be an integral feature of ASOCC.

Threat Condition Reporting

Commanders in the AOR require a means to direct changes to FPCONs, INFOCONs and MOPP levels based on threat assessments and conditions. They also require a means to monitor what and when conditions are attained at the installation level and problems associated with non-compliance and sustainability.

SIPRNET web sites with FPCON, INFOCON and MOPP level information can be maintained at the incident-level using the Event Log function of ASOCC, which can direct changes and view the FPCON status of individual bases/installations.

Warning, Direction, and Coordination

There are several means to provide warning to installations when specific information or assessments exist. The Event Log function of the ASOCC ExPanel can be one of them; redundancy in such cases is preferable. Nodes having warning type information can disseminate it directly to the security forces and installation decision makers using ASOCC, and (future capability) receive acknowledgement of receipt from the affected installation.

Likewise, watchstanders at the RCC/ROC can use the Event Log to disseminate guidance, direction, and coordination instructions.

Incident Reporting

When a significant incident occurs, there is normally a great deal of reporting on the incident, photographs to be shared, collaboration to be done to ensure pertinent information is disseminated. As a standard practice, the originator of an incident report in the Event Log, besides providing updates to the log report, should create a folder about the incident in a DCTS room so that other reporting and materials concerning the incident can be filed in a central location for all to access. The initial incident reporting node should include the name and location of this folder in the incident event log entry as well as information on which collaboration room in DCTS will be the focal point for collaboration on the incident being reported. [Information clutter management needs to be figured out. Much larger issue is strategy of information flow up the chain. Diagram "ASOCC INFORMATION FLOW PATHS" is a start. Supporting logic needs to be drafted.]

Collaboration

The DCTS is organized into collaboration "buildings", "floors" and "rooms". Each room has areas for sharing files, conducting chat room discussions, audio conferences, and white board collaboration.

An AOR room will be used primarily for sharing administrative information, files of interest to all nodes in the echelon, and Regional level chat sessions.

Additional rooms are primarily for sharing security force status type information by Region; i.e. COMNAVREGSW can coordinate Navy security forces in the CNRSW room of DCTS.

Other rooms can be created/used to discuss and share information on security incidents occurring within peer-to-peer geographic areas. For example, when a significant incident occurs in one harbor, then the affected regional JHOC can utilized ASOCC to immediately alert other JHOCs as to the situation and any preceding indications and warnings (I&W). An incident collaboration room could be established, along with an incident folder, so that anyone with information, messages, photographs, etc. related to the incident can log them or upload them. Chat sessions with information related to the incident may also be saved and added to the incident folder.

Maps

ASOCC does not come with maps pre-installed. Each node must find and store maps that fit its needs from other sources. Sources include:

- NIMA's SIPRNET web site
- Geo-registered base maps used by installation Public Works/Civil Engineering departments
- Commercial mapping programs
- Manually geo-registered map images

The echelon one will maintain information on recommended mapping sources and files of geo-registered images in folders in its DCTS AOR room for all to use. Other nodes may add images to this list at any time.

Web Site Monitoring

Each node may monitor web sites of interest using the KnowledgeBoard tool. However, the echelon one will maintain a list of recommended web sites in a file in the AOR room on DCTS and may specify sites that all nodes should monitor. Any node may recommend additional sites containing useful information to the AOR.

WMD Events and Industrial Accident Situations

WMD events and industrial accidents may affect large areas. Defining those areas as quickly as possible after the event takes place is critical to minimizing potential harm to military and civilian personnel, and provides for more timely resumption of normal operations. Using the CATS tool in ASOCC, installation security forces will initiate calculation of areas affected and what predicted impact it will have on military and civilian centers. If a WMD event or industrial accident occurs in other regions, it is important to immediately promulgate all I&W information as a preventative measure against possible multiple attacks.

Mission Phases

The ASOCC system integrates surveillance and communication capabilities to enable effective and efficient performance of HLS/HLD missions within a given AOR, including maritime security, AT/FP, maritime safety, law enforcement, environmental protection, and national security. ASOCC watchstanders located within the "incident-level" at JHOCs/EOCs will coordinate the activities of first-responders and supporting forces from U.S. Navy, U.S. Coast Guard, local base commanders, along with local/State/Federal agencies. ASOCC watchstanders located at the RCCs/ROCs will serve as the key transition node between the incident-level and the multi-echelon (e.g. National) level nodes. As a crises develops, the primary role of ASOCC watchstanders operating within the "incident level" is to coordinate the engagement of appropriate resources as quickly as possible. These "incident level" ASOCC operators, who are located at the JHOC and/or EOC, are tied into their local sensor suites and local intelligence agencies, and presumably would have been developing situational awareness for hours, days, or even weeks preceeding any potential event. Once an incident occurs, the Navy Regional Commander would stand up their RCC/ROC in order to manage the crisis from a regional support level. ASOCC watchstanders located at the RCC/ROC would serve as the information pivot point between the incident-level responders and multi-echelon level commands.

Watchstander Manning

The following notional manning plan is envisioned to support an ASOCC node.

System Administrator. To ensure the smooth functioning of ASOCC, an ASOCC system administrator at the echelon one level is required. This person will: [Not certain at what level support personnel should occur- keep it divided by AOR or centralize into 1-3 regional areas?]

- Monitor the status of ASOCC nodes and adjust peer-to-peer relationships as required,
- Provide Tier II maintenance support to ASOCC workstations in the AOR,
- Maintain a database on the configuration and ASOCC software version at each node,
- Perform or coordinate installation of new software releases,
- Do ASOCC user and local administrator training,

Operations Support. A second position at the echelon one level is required to support users. The person in this position will:

- Configure the XIS tool to access locally designed and remote databases for all nodes in the AOR,
- Assist all nodes in developing or modifying and sharing of local databases for ASOCC access,

- Provide quality control for local databases used as sources for ASOCC,
- Identify remote databases of interest to ASOCC users and arrange for ASOCC access to them,
- Identify and demonstrate mapping sources that may be of interest to ASOCC users,
- Assist ASOCC nodes in developing and sharing overlays, shape files, etc. that could be used in ASOCC,
- Assist in the training of ASOCC users.

Summary

The recent series of attacks on U.S. civilian and military forces, coupled with the United State's very visible leadership role in the Global War against terrorism, have changed the world environment forever. For perhaps the first time in its history, the U.S. cannot take for granted the relative security of its ports, infrastructure, territory, and territorial waters. The potentially devastating asymmetric threats posed by terrorists, coupled with the challenging complexities associated with defending the vast expanse of potential U.S. targets, demands a previously unrealized level of cooperation and collaboration between military forces and local/State/Federal agencies. Improvements in overlapping sensors, non-lethal/lethal weapons, and intelligence gathering all have an important their role in anti-terrorism/force protection. Yet investments in these areas will not have the desired effect unless they are coupled with the proper tools, processes, and communication strategies to affect cooperation among the various agencies and activities having explicit responsibilities for Homeland Security/Homeland Defense.

The development, fielding, and active utilization of an integrated C4ISR system dedicated to the HLS/HLD mission is critical to effectively synchronizing the cooperative resources and actions of these law enforcement, military, and civilian agencies. The ASOCC toolkit made up of fully-integrated GOTS and COTS software installed on commercial desktop computers, provides its users with the capability to command, control, and coordinate AT/FP efforts across multiple echelons and authorities. While this DISA approved software component is in phase I of its spiral development, it offers an important first step in meeting the Navy's requirements for operational deployment of an AT/FP C4ISR network.

APPENDIX A: NOTIONAL AT/FP SCENARIO

Introduction.

Within the scenario, the national intelligence community will develop information and assessments that Al Quaeda has obtained weapons of mass destruction and is shipping them to the U.S. on merchant ships. The intelligence will then be developed to the point that the Navy [NAVNORTH] is able to intercept and neutralize the ships under the direction of NORTHCOM in a homeland defense [HLD] mission.

In related events, a terrorist cell in San Diego will plan and execute a suicide attack against NAS North Island using a stolen propane tanker. The attack is mitigated by the defensive posture at the gate, where traffic bollards prevent access to the base. The resulting collision explodes the tanker contents, with the subsequent damage and fire confined to the immediate gate area adjacent to the harbor.

Finally, NAS North Island security forces will react to an intrusion alert along the carrier exclusion zone involving a small power boat. This will prove to be a non-threat event.

Scenario considerations:-

1. The contents described are limited to actions conducted horizontally and vertically within the affected area only.
2. Certain actions and intelligence-gathering/assessment activities are taking place outside the ASOCC domain, (i.e. outside networks, telephone, wireless communications, etc.)

Scenario matrix design-

The matrix design separates the ASOCC entries into phases designed to illustrate the conceptual development of the event and to emphasize the versatility of the ASOCC functions.

Scenario phases chosen for this example are:

Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt

Explanation of matrix contents-

The ASOCC entries described within the matrix fall into five categories:

1. Informational- realtime awareness
2. Informational- reporting/responding
3. Informational- database postings (DCTS)
4. Action required- realtime C4ISR operations
5. Action required- C2 and coordination (DCTS)]

Non-ASOCC entries describing situational developments are listed in brackets.

Day-1

	Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt
National	JITF-CT posts notice on ASOCC of terrorist threat assessment with amplifying information in DCTS: terrorists will launch attacks against U.S. port in the near future. Attacks are postulated to include attacks from the sea by ships that could have WMD onboard, and physical and cyber attacks against infrastructure around port.	HLS Nebraska Ave posts alert that national Homeland Security Advisory System status raised from "elevated" to "high". FBI HQ posts advisory that national intelligence community threat alerts have been passed to LE agencies.	PACOM directs FPCON Bravo-plus at Navy bases.		
RCC/ROC			Region SW reports FPCON Bravo-plus set.		
JHOC/EOC	San Diego police report increase in numbers of students in San Diego State University who have expired passports. One individual has numerous pictures of local bridges and tunnels in his automobile. NAS North Island NCIS posts advisory conspicuous inquiries about the base.				

DAY-2

	Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt
National	IC reports indications that WMD materials may be aboard ships headed toward Long Beach, San Diego and/or Port of Tacoma. OHLS posts alert of threat to coastal areas from terrorists aboard merchant ships.	Navy Operations Center (NOC) posts alert to COMPACFLT to report readiness to sortie ships and ensure base FPCONs are updated. NOC directs Naval Reserve to deploy harbor and security units to Puget Sound and San Diego. COMPACFLT HQ directs COMTHIRDFLT to prepare to sortie ships;.reports confirmation of FPCON.		NCIS/Multiple Threat Analysis Ctr. Posts advisory that latest PIVA (Port Integrated Vulnerability Assessment) for Naval ports available in DCTS room. DTRA posts advisory of DCTS location of checklists for requesting support from DTRA. NORTHCOM posts advisory that the Navy and Coast Guard are collaborating in defensive measures to protect against terrorists aboard merchant vessels. COMPACFLT posts alert to Region SW to join in DCTS collaboration with DTRA to discuss CBRNE response plans.	
RCC/ROC		Region SW directs test/report of sensor system readiness at North Island.		Washington and California DEM EOCs post coastal evacuation plans in DCTS.	
JHOC/EOC	San Diego Police Dept. posts a notice of the theft of a propane tanker with a summary of the vehicle description.			Emergency Services for affected areas post maps with locations of Primary HAZMAT/WMD capabilities.	

DAY-3

	Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt
National	DIA JITF posts alert Identifying San Diego port as theSpecific target.	PACOM posts alert directing San Diego Navy waterfront bases to FPCON Charlie.		NIPC posts advisory that port authorities and industry groups in threatened area have been issued threat advisories. JTF-CS posts alert to NIMA of request for facilities maps/imagery of threatened port. NIMA posts advisory pointing to maps/imagery in DCTS room.	NORTHCOM HQ posts alert for NAVNORTH to locate and intercept threat shipping. NAVNORTH reports its assessment that most of the suspect ships can be stopped before the 200-mile nautical limit of territorial waters. Two ships are closer to shore and will be stopped and searched by the U.S. Coast Guard.
JHOC/EOC		Region SW reports FPCON Charlie set.		FBI alerts San Diego JHOC to National Law Enforcement Telecommunications message (NLET) and posts messages in DCTS.	
RCC/ROC	Border Patrol posts Advisory detailing arrest of people smuggling C4 into U.S. Debrief reflects that shipment was intended for men of middle east descent.			San Diego JHOC posts alert to peer-to-peer nodes to meet in collaboration space to coordinate port security measures.	

DAY-4

	Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt
National	JITF posts report concerning a raid against a terrorist planning cell in vicinity of Jakarta. Raid yields knowledge of planned major attack against U.S. homeland port with biological weapons.	NORTHCOM HQ posts advisory of assignment of Army chemical/ radiological forces to JTF-CS. Coast Guard posts alert that it has set Maritime Security Condition 3.		NORTHCOM asks DTRA to perform a "worst-case" analysis to likely fallout pattern of biological weapon. A ship bound for Port of San Diego is identified as a likely culprit; JITF-CT posts advisory pointing to reports posted in DCTS from the IC providing more info on ship's type. NAVNORTH HQ posts alert to NORTHCOM, JTF-CS, DTRA, Coast Guard, and IC to join in collaborative planning in DCTS to plan intercept of merchant ship with biological weapon aboard. Collaborative session initiated via NetMeeting; participants provide info with likely responses to various courses of action. DTRA provides assessments with shared files (maps) via white board.	
RCC/ROC				California state EMD EOC posts alert of DCTS posting: a) Governor's Proclamation b) State WMD checklist c) SITREP	
JHOC/EOC					

DAY-5

	Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt
National	NCIS posts warning to San Diego port about possible ancillary attacks by speedboat or other delivery vehicle.	NORTHCOM posts advisory that all merchant ships suspected to have terrorist connections have been located, intercepted, seized and neutralized at sea; by the Navy and the Coast Guard. COMPACFLT HQ posts advisory that Navy will conduct tactical reconnaissance missions over San Diego area.			
RCC/ROC	[Region SW ROC monitors radio report of California Highway Patrol in pursuit of propane tanker approaching NAS North Island. Vehicle matches description of stolen tanker reported Day -1]	Region SW ROC directs San Diego Navy bases to set FPCON Delta; requests assist of Coronado City Police in containment of vehicle.			
JHOC/EOC	CNRSW SM -10 camera system alerts a violation of virtual barrier around carrier pier.		San Diego JHOC diverts Harbor police And Coast Guard assets to assist Navy Police in securing perimeter around barrier violation. [Patrols report intruder to be druken recreational boater; vessel escorted out of security zone.]		

DAY-6

	Indications & Warnings	Prevention & Deterrence	Reaction/First Response	Crisis Mgt	Consequence Mgt
National			PACOM directs San Diego Navy bases to FPCON Delta.		NORTHCOM coordinates activities with LFA to execute Federal Response Plan.
RCC/ROC			Region SW reports FPCON Delta set.		SW Region shares live sensor input of explosion site activity in DCTS.
JHOC/EOC			[NAS North Island Security reports tanker engagement with gate bollards near harborside entrance, resulting in explosion of vehicle contents; Emergency Services responding.]		San Diego JHOC requests assist from Harbor Fire along waterside adjacent to explosion site.

APPENDIX B: ACQUISITION/LOGISTICS STRATEGY

Acquisition/Logistics Strategy

ASOCC acquisition will be somewhat simplified because the software is a Government off-the-shelf (GOTS) item, while the associated hardware consists of Commercial off-the-shelf (COTS) equipment. The current strategy for Phase I of the acquisition is to have the "end user" (e.g. Fleet Commanders on both coasts) bear the cost of initial procurement, with follow-on ILS costs being handled by a program office currently in development. Initial procurement of ASOCC will be in the form of an ASOCC pilot deployment in the major fleet concentration areas for each fleet commander (San Diego and Norfolk). Depending upon the SOW, this pilot could provide ASOCC terminals at multiple echelons within each command, as well as initial training for watch standers and on-site technical support to help the user configure the ASOCC software to meet evolving AT/FP CONOPS.

As the ashore AT/FP C2 system, ASOCC will be part of a larger ashore C4ISR architecture which includes such things as emergency dispatch centers and base operating and management systems. As of this writing N46 has sponsored a study by PMW 157 to identify an ashore C4ISR architecture to include ashore AT/FP C2. N46 has granted oversight of this study to N34 and CFFC as the AT/FP assessment and requirements sponsors. This oversight will ensure that ASOCC is utilized for ashore AT/FP C2. Results of this study are to be used as input into the POM '06 budget process. This will inject ASOCC into the PPBS system, relieving the fleet commands of any financial burdens beyond the initial procurement of the pilot deployment.

Phase I Implementation

(To be written. Need to discuss first installment of terminals in San Diego, Hawaii and Norfolk. Actual locations: JHOC, Regional Dispatch, Regional Command Center, C3F, CPF, ???? Discuss spiral development goals. Key issue is development of information sharing strategies that work among functional workgroups and regional groups, Joint centers, and don't clutter up terminals at the very highest levels. How is information going to be shared among work groups and then summary data pushed to higher levels.)

Training Support

The National Terrorism Preparedness Institute (NTPI) is currently chartered to conduct ASOCC training and produce training materials.

Online training materials can be found on the following unclassified web site: http://terrorism.spjc.edu/ASOCC.htm .

NTPI also will periodically conduct mobile training. [Is this contracted in initial ASOCC deployment?]

Echelon one ASOCC support personnel (see below) will assist NTPI trainers in a "train-the-trainer" role and coordinate NTPI training in the AOR.

APPENDIX C: OPERATIONAL DEFINITIONS

The following operational definitions will be used throughout this document:

Antiterrorism (AT). Deterrent/defensive measures used to reduce the vulnerability of personnel and resources to terrorist attack.

Counter-terrorism (CT). Offensive measures, including the gathering of information and threat analysis, taken to prevent, deter, and respond to acts of terrorism.

Consequence Management. Predominantly an emergency management function that includes measures to protect public health and safety, restore essential government services, and provide emergency relief to individuals and organizations affected by the consequences of terrorism.

Crisis Management. Predominantly a law enforcement function that includes measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. In a terrorist incident, a crisis management response may include traditional law enforcement missions, such as intelligence, surveillance, tactical operations, negotiations, forensics, and investigations, as well as technical support missions, such as agent identification, search, render safe procedures, transfer and disposal, and limited decontamination.

Deterrence. Overt physical security enhancements and other measures used to discourage/dissuade potential terrorists from selecting/attacking potential targets.

Emergency Operations Center (EOC). The site from which civil government and/or military officials (municipal, county, State and Federal) exercise direction and control in an emergency.

Federal On-Scene Commander (F-OSC). The FBI official designated upon JOC activation to ensure appropriate coordination of the overall U.S. government response with Federal, State and local authorities, until such time as the Attorney General transfers the LFA role to FEMA.

First Responder. Local fire, police, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic needs

Force Protection (FP). The blended integration of antiterrorism measures, physical security, operations security (OPSEC), protective services, law enforcement operations, foreign intelligence, counter-intelligence, and other security actions.

Indications and Warning (I&W). Results from the focused and aggressive merging of (1) intelligence information gathering/dissemination with respect to suspected terrorist groups, methods of operation, potential targets, attack methodology, etc., and (2) real-time situational awareness/analysis of the areas to be protected. Successful I&W enables timely/anticipatory action to counter emergent threats.

Joint Harbor Operations Center (JHOC). The site from which U.S. Navy and U.S. Coast Guard personnel, along with selected representatives from municipal, county, State, and Federal

agencies, exercise direction and control over the activities associated with protection of harbor assets and infrastructure.

Joint Information Center (JIC). Center established to coordinate Federal public information activities on-scene. It is the central point of contact for all news media at the scene of the incident, and should include all public information officials from all participating Federal Agencies. Public information officials from participating State and local agencies may also collocate at the JIC.

Joint Operations Center (JOC). Normally established by the Lead Federal Agency (LFA) under the operational control of the Federal On-Scene-Commander (F-OSC), as the focal point for management and direction of onsite activities, coordination/establishment of State requirements/priorities, and coordination of the overall Federal response.

Lead Federal Agency (LFA). The Federal department or agency assigned lead responsibility to manage and coordinate the Federal response in a specific functional area. Normally the LFA for Crisis Management is the Department of Justice (delegated to the FBI), with FEMA acting as the LFA for Consequence Management.

On-Scene Coordinator (OSC). The Federal official pre-designated by the EPA and USCG to coordinate and direct the response/removals of Oil and Hazardous Substances.

Prevention. Measures designed to thwart the acts of terrorists before an action can be completed or an objective can be achieved. Prevention efforts can be either overt (in the case of deterrence and/or reaction), or covert (e.g. surveillance, detection, identification, alertment, etc.)

Reaction. Actions that control the course of a terrorist incident and limit the resulting damage when both deterrence and prevention have failed.

Recovery. Includes all types of emergency actions dedicated to the continued protection of the public or to promoting the resumption of normal activities in the affected area.

Regional Commander. The U.S. Navy Flag officer assigned to as the Commander of one of the Navy's seven regional headquarters, responsible for the protection and support of all infrastructure (e.g. bases, airfields, facilities, equipment, etc.) within the designated region.

Regional Director. The Director of one of FEMA's ten regional offices and principal representative for working with other Federal regions, State and local governments, and the private sector in that jurisdiction.

This page intentionally left blank.

APPENDIX B JHOC DRAFT CONOPS

March 24, 2003

CONCEPT OF OPERATIONS
FOR
SAN DIEGO JOINT HARBOR OPERATIONS CENTER
- PHASE I -

I. Overview

The confluence of federal, state and local missions in the maritime environment provide the motivation to integrate Navy Force Protection/Anti-Terrorism forces, Coast Guard Maritime Homeland Security forces, and Civil Law Enforcement forces in a coherent and fully functional joint operations cell. Establishment of a Joint Harbor Operations Center (JHOC) of Coast Guard, Navy and other federal, state and local law enforcement agencies allows for unity of force and command in day to day operations, initial responses in emergency situations, and Consequence Management (CM) operations when required.

Individually, the Navy's Homeland Defense (HLD) mission is to conduct operations in defense of United States territories as well as Anti-Terrorism/Force Protection operations for military units under its control. The Coast Guard's Homeland Security (HLS) mission is to protect the U.S. Maritime Domain and the U.S. Maritime Transportation System and deny their use and exploitation by terrorists as a means of attack on U.S. Territory, population, and critical infrastructure. Federal, state and local law enforcement authorities are charged with enforcing civil/criminal statutes and protecting the general population. Together, these missions are complimentary and overlapping. Furthermore, other federal agencies such as FBI, Directorate of Border Transportation Security (BTS), local and state law enforcement organizations, routinely support port security and AT/FP missions in U.S. ports with Navy presence.

The integration of an operational command and control system for these forces is essential and will provide a common situational awareness across the spectrum of organizations involved. This system should provide collaborative course-of-action planning, analysis, execution, and monitoring; interoperable secure communications among decision-makers and response assets; and other tactical decision aides that support key functions, such as operational risk management and response asset readiness monitoring.

The overarching goal of this system is to collect, process, facilitate fusion, and disseminate data from a variety of disparate, geographically separated, sensors and static information sources and provide the decision support necessary for key decision-makers in a timely enough manner to identify, target, interdict, engage and re-engage, if necessary, and destroy/thwart asymmetric threats through coordinated interagency actions.

The JHOC will improve the command and control and coordination of the multi-agency efforts to deter, detect and defend against asymmetrical terrorist threats offshore and within the Port of San Diego by leveraging the collective efforts and limited resources of the stakeholders and

optimizing their use. The JHOC is designed to take full advantage of the synergistic effect of collocating watchstanders from the Coast Guard, Navy, and OGA stakeholders at the U.S Coast Guard Activities San Diego Operations Center. Additionally, the JHOC promotes the enhanced coordination of incident management and consequence management activities between federal, state and local agencies, including interoperability with the Incident Command System (ICS) during chemical, biological, radiological, nuclear and explosives (CBRNE) events, as well as the routine response to standard law enforcement activities.

The organizations involved in staffing the JHOC in Phase I are Commander Navy Region Southwest, Coast Guard Activities San Diego, and San Diego Harbor Police. Three locations have been identified to house the JHOC capabilities, including USCG Activities San Diego Operations Center, CNRSW Emergency Operations Center, and Commander Third Fleet. This built in redundancy allows continuity of operations should there be a need to shift operations.

II. OBJECTIVES

- To improve situational awareness (SA) and responsiveness of participating organizations in day-to-day operations, both in the seaward approaches to San Diego and within the port itself.

To improve command, control and coordination of multi-agency efforts to deter, detect and defend against asymmetrical terrorist threats offshore and within the Port of San Diego by leveraging the collective efforts and limited resources of the stakeholders and optimizing their use.

To enhance coordination of Incident Management (IM) and Consequence Management (CM) activities between federal, state and local agencies, including interoperability with the Incident Command System (ICS) during chemical, biological, radiological, nuclear, and explosives (CBRNE) events.

The JHOC will accomplish these objectives by taking full advantage of the synergistic effects of co-locating watch standers from the Navy, Coast Guard, and OGA stakeholders at the designated JHOC location and leveraging technologies such as Area Security Operations Command and Control (ASOCC) system to develop and maintain a Common Operating Picture.

III. Concept of Operations

A. Daily Operations

1. Maintain situational awareness of current activities and de-conflict off-shore and in port operations through the use of the Common Operational Picture (COP).
2. Monitor, track and record deep draft vessel traffic including moored and anchored vessels.
3. Monitor and track other vessel activity for suspicious and/or anomalous activity.

4. Receive and coordinate initial investigation of suspicious and/or anomalous activities
5. Monitor radios for voice traffic.
6. Maintain a real time and historical vessel traffic database.
7. Maintain a weather watch.
8. Compare actual vessel arrival information with scheduled arrival information.
9. Schedule Sea Marshal escorts, as required.
10. Establish and maintain dialogue with the local pilots associations concerning vessel movements.
11. Produce a daily authorized vessel entry list (AVEL) for the Port of San Diego.
12. Maintain continuous MDA (commercial vessels in port, cargo operations, Blue Force activities, channel clearings, special events, HVA/HIVs, and boardings).
13. Monitor escorts of CLASS "A" USN/USNS and other High Value Assets.
14. Assist with de-confliction of high value asset and deep draft vessel transits.
15. Monitor boarding operations, High Interest Vessel boardings in particular.
16. Respond to requests for information from federal, state and local level authorities.

B. Initial Response to Threat Activities

1. Participating agencies will retain Tactical Control (TACON) of their assets through existing C2 organizations.
    a. Diverting USN assets should be avoided to ensure continuous protection of USN vessels and facilities.
    b. Divert/launch the most appropriate law enforcement asset(s) to investigate or intercept threats/targets of interest.
    c. Alert all participating agencies about threats/targets of interest.
    d. Requests for USCG assets will go directly to the Coast Guard Activities Operations Duty Officer.
    e. Requests for Harbor Police assets will go directly to Harbor Police Dispatch.
    f. Requests for Navy Security assets will go directly to Regional Dispatch Center (NRDC)/Emergency Operations Center (EOC). Navy Security response outside of designated Security Zones is pending MOU between USN and USCG.
    g. All participating agencies will agree to comply with JHOC asset requests whenever feasible.
    h. Maintain MDA

i. Control/restrict vessel movements in- bound/out-bound the Port of San Diego and the Regulated Navigation Area (RNA), when established.

j. Blue Force Coordination: Provide tactical coordination between available law enforcement (federal, state, and local) and protective (USN Force Protection) assets.

2. Coordinate utilization of DOD combatants to mitigate threats.
3. Coordinate EOD/Mine Countermeasures to mitigate threats.
4. Coordinate USN and commercial towing and salvage resources.
5. Coordinate information dissemination to appropriate commands and stakeholders.

C. Consequence Management

1. Coordinate establishment and enforcement of safety perimeters.
2. Initiate the Incident Command System (ICS).
3. Assist and support designated Incident Commander.
4. Coordinate vessel traffic control.

D. Sensors/Systems

1. The JHOC will utilize an informational technology architecture that will integrate sensors, agency databases, and intelligence information to provide common situational awareness for decision-makers and security assets via a shared Common Operational Picture over a server-based intranet link to all designated shareholders utilizing a Virtual Private Network (VPN).
2. Sensors will include video, radar, thermal imaging, sonar systems, and ACTD Direction Finding System (position localization).
3. Related systems include Automatic Identification System (AIS) and Blue Force Locating System.
4. Databases will include National Criminal Information Center (NCIC); Automated Regional Justice Information System (ARJIS); Marine Information Safety and Law Enforcement (MISLE); Joint Maritime Information Element (JMIE), SEALINK, ELINT query, and Global Command and Control System Marine/Joint(GCCS-M/J).

E. Rules of Engagement/Use of Force

1. Policies:

   All participating agencies will continue to operate under their existing Rules of Engagement and Use of Force policies in accordance with their parent organizations' rules and regulations.

2. Oversight:

   It is recognized that the majority of Small Boat and Point Defense Use of Force/Rules of Engagement decisions must be made within seconds or minutes on scene. In rare circumstances where there is the time or need for UOF/ROE

guidance or permission, participating assets will contact their tactical commander for guidance (participating agencies will retain TACON of their assets through existing C2 organizations).

IV. Command Relationships

A. Watch Organization

The JHOC will have three watch standers, one USCG, one USN and one San Diego Harbor Police. The watchstanders will be assigned COP terminals (Two SIPR and One NIPR terminals) based on their Security Clearance within the JHOC space.

B. Watchstander Responsibilities

Option I:

One watchstander is designated as the Watch Commander. This individual is assigned authority to coordinate the movement of all available assets through the other watchstanders within the JHOC. The watchstanders will contact their respective dispatch centers to coordinate Blue Force movement. TACON remains within the parent organization.

Option II:

All watchstanders are equal (e.g.: no Watch Commander) and responsible to their parent organizations for direction of organizational assets. Individual watchstanders in the JHOC have responsibility to coordinate dispatch of their own resources while coordinating with the other JHOC watchstanders.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Dudley Knox Library, Code 013 Naval Postgraduate School Monterey, CA 93943-5100	2
3.	Research Office, Code 09 Naval Postgraduate School Monterey, CA 93943-5138	1
4.	Mike Stumborg Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
5.	Mike Dorsey Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
6.	LCDR Tim Tutt Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
7.	LTJG Eric Westlin Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
8.	Bill VonStorch Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1
9.	Special Agent Cliff Link Naval Criminal Investigative Service 716 Sicard St SE, Bldg 111 Washington Navy Yard, DC 20388-5380	1

10.	Special Agent Warren Brownley Commander Navy Region Mid-Atlantic 1510 GILBERT ST ATTN: N2/SSA Brownley Norfolk VA 23511-2737	1
11.	Kim Kelly, Special Agent NCIS 3405 Welles St., Suite 1 San Diego, CA 92136-5050	1
12.	Gordon Schacher Wayne Meyer Institute of Systems Engineering Naval Postgraduate School 777 Dyer Rd., Rm 100D Monterey, CA 93943	2
13.	Shelley Gallup Wayne Meyer Institute of Systems Engineering Naval Postgraduate School 777 Dyer Rd., Rm 100D Monterey, CA 93943	5