AFRL-IF-RS-TM-2007-8
Final Technical Memorandum
March 2007

INTEGRATED INFORMATION MANAGEMENT (IIM)

NGI Systems, Inc.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the Air Force Research Laboratory Rome Research Site Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-IF-RS-TM-2007-8 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/	/s/
JAMES F. REILLY Work Unit Manager	JAMES W. CUSACK Chief, Information Systems Division Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAR 2007	Final	Sep 05 – Jun 06

4. TITLE AND SUBTITLE

INTEGRATED INFORMATION MANAGEMENT (IIM)

5a. CONTRACT NUMBER
FA8750-05-C-0263

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
63789F/62384B

6. AUTHOR(S)

Jason McIlvain

5d. PROJECT NUMBER
IIMS

5e. TASK NUMBER
NG

5f. WORK UNIT NUMBER
IS

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

NGI Systems, Inc.
7676 Pine Bluff Circle
Manlius NY 13104-9544

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/IFSA
525 Brooks Rd
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TM-2007-8

12. DISTRIBUTION AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 07-137

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Information Technology is the core capability required to align our resources and increase our effectiveness on the battlefield by integrating and coordinating our preventative measures and responses along with the tools used to perform them. To win the War on Terrorism, the US defense strategy requires information superiority to secure our advantage over adversaries. This focus on technology is identical to Joint Vision 2020's goal of information dominance, and the Joint Services' focus on network-centric warfare. As learned through the RestOps and CASPOD ACTDs, systems must be built to shift, grow, and shrink as the context of their use changes. As stated in Joint Vision 2020, this capability will allow commanders to bring together the correct mix of assets at the place and time most favorable to success. Systems providing these characteristics are largely unavailable and a high priority need for battle management. This report discusses the requirements of an integrated management system and progress on the effort.

15. SUBJECT TERMS

COP, geospatial display, Remote Data Relay (RDR), integrated information management systems

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			James F. Reilly
U	U	U	UL	15	19b. TELEPHONE NUMBER (*Include area code*)

TABLE OF CONTENTS

1.0 ABSTRACT

Information Technology is the core capability required to align our resources and increase our effectiveness on the battlefield by integrating and coordinating our preventative measures and responses along with the tools used to perform them. To win the War on Terrorism, the US defense strategy requires information superiority to secure our advantage over adversaries. This focus on technology is identical to Joint Vision 2020's goal of information dominance, and the Joint services' focus on network-centric warfare.

As learned through the RestOps and CASPOD ACTDs, systems must be built to shift, grow, and shrink as the context of their use changes. As stated in Joint Vision 2020, this capability will allow commanders to bring together the correct mix of assets at the place and time most favorable to success. Systems providing these characteristics are largely unavailable and a high priority need for battle management.

This report discusses the requirements of an integrated information managements system and progress on the effort between October 2005 and May 2006.

2.0 SUMMARY

This report discusses the requirements of an integrated information managements system and progress on the effort between October 2005 and May 2006.

3.0 INTRODUCTION

Years before the 911 tragedy, military planners were concerned with improving the protection and recovery of fixed military logistical sites from the consequences of chemical and biological attacks. In 2001, the US Department of Defense and the Defense Threat Reduction Agency formed the RestOps (Restoration of Operations) ACTD (Advanced Concept Technology Demonstration) to address this concern.

Osan Air Base in South Korea served as the host site for RestOps. At the outset, Osan's SRC(Survival Recovery Center) relied heavily on phone systems, paper reports, and grease

pencil maps to acquire, manage and display information. They had very little ability to filter and correlate fragments of information or build a distributed COP(Common Operational Picture). Rome Laboratory served as lead technical integrator of the ITWG (Information Technology Working Group). The ITWG's objective was to develop a COP concerning base chemical and biological attack status and related situational awareness information by integrating and exploiting disparate data sources. The result of our efforts was ROIMS (RestOps Information Management System).

ROIMS included the SRC3 Command, NBC-RPM (Nuclear Biological Chemical – Reporting Plotting Modeling), and ROIM Digital Dashboard applications. SRC3 Command provided a geospatial display, NBC-RPM provided hazard modeling, and the ROIM Digital Dashboard provided event reporting and reconnaissance management tools. The ROIMS applications were integrated via the TBMCS_UL database. ROIMS also integrated the Portal Shield detector network with the C2 network residing on SIPRNET using a one-way fiber-optic guard. ROIMS was evaluated in several Military Utility Assessments (MUA's) and deemed a proven utility to warfighters. ROIMS changed CONOPS at Osan Air Base and was successfully transitioned to TBMCS-UL.

Following RestOps, DTRA formed another sister ACTD named CASPOD (Contamination Avoidance at Seaports of Debarkation). While similar in scope, CASPOD aimed to address contingency response at Sea Ports and expeditionary sites. While the RestOps ACTD focused on the Air Force, CASPOD would bring similar capabilities to the Joint Services. And while the objective remained the same the system needed to be more modular, easier to setup and use, and able to run independently of TBMCS.

Again, Rome Laboratory functioned as lead technical integrator of the ITWG. To address these requirements the ITWG chose to integrate the geospatial display of SRC3 Command and the hazard modeling tools of NBC-RPM into the ROIM Digital Dashboard. The result was not only a more cleanly packaged product, but also a significant savings in network bandwidth since all 3 applications previously had independent data caches on the client. Since the Portal Shield network required significant infrastructure in place it was not a viable choice for an

expeditionary detector network. Additionally, CASPOD aimed to integrate warning devices and the Portal Shield network had limited extensibility. Due to these constraints, Sentel's RDR (Remote Data Relay) network was selected and integrated with the C2 System. The result of this effort was PortWARN (Port Warning and Reporting Network). Components and concepts from PortWARN have transitioned to JWARN (Joint Warning and Reporting Network), the program of record for NBC Defense. Additionally, 143rd Transportation Command of the Army is in the process of acquiring PortWARN for fielding in SWA to protect their port operations.

The DTRA JSTO CBD Next Generation CB Battle Management System effort enhanced the PortWARN code base integrating multiple models, information tagging, active guidance and other information capture and management tools. The system was renamed the Integrated Information Management System (IIMS). The DTRA JSTO CBD Shared Common Operational Picture (COP) effort integrated IIMS with Area Security Operations Command and Control (ASOCC) and Joint Warning and Reporting Network (JWARN).

Terrorism is no longer a question of if it will happen, but when. Unfortunately, the War on Terrorism poses unique challenges in identifying adversaries, as well as there plans, motivations, intentions, resources, and opportunities. Technologies that aid prevention through predictive analysis and early detection, as well as those which enable the successful response to attacks are of vital importance. Failure to develop such technology would yield unacceptable loss of life, and degradation of military readiness.

Information Technology is the core capability required to align our resources and increase our effectiveness on the battlefield by integrating and coordinating our preventative measures and responses along with the tools used to perform them. To win the War on Terrorism, the US defense strategy requires information superiority to secure our advantage over adversaries. This focus on technology is identical to Joint Vision 2020's goal of information dominance, and the Joint services' focus on network-centric warfare.

As learned through the RestOps and CASPOD ACTDs, systems must be built to shift, grow, and shrink as the context of their use changes. As stated in Joint Vision 2020, this capability will allow commanders to bring together the correct mix of assets at the place and time most

favorable to success. Systems providing these characteristics are largely unavailable and a high priority need for battle management.

4.0 METHODS, ASSUMPTIONS, AND PROCEDURES

Through involvement with Advanced Concept Technology Demonstrations (ACTDs) including Restoration of Operation (RestOps) and Contamination Avoidance at Seaports of Debarkation (CASPOD), NGI Systems helped develop the Installation Warning and Reporting Network (IWARN). This effort utilized the IWARN code base and capitalized on ACTD experience to develop these next generation C4I Battle Management capabilities. Active Guidance, Dynamic Tagging, Disconnected Operations, Publish & Subscribe, Data Archiving, Force Templates, and Dynamic Planning represent the core technological thrusts that must be pursued for systems to fulfill the requirements of highly dynamic operational environments.

Development strategy is the key to building dynamic systems. Our strategy represents an open systems approach, that allows for development of loosely coupled, distributed, modular, and extensible systems. Architectures grounded in this approach increase technology transition opportunities, enable developers to focuses on core competencies rather than heterogeneous integration efforts, allow commanders to reconfigure systems according to threats and demands, and enable the research community to focus on science rather than developing test beds.

This investigation will result in a versatile battle management system capable of transforming to match the demands of the mission at hand. This advantage will result in faster OODA(Observe Orient Decide Act) cycles for the commander and her action officers. Additionally, the ability to dynamically adjust with CONOPS increases the system's potential application in other areas. NGI Systems believes this potential will lead to an evolutionary jump in the ubiquitous use of the IWARN System during normal operations as well as during post attack recovery.

GOALS

Active Guidance:

As the capability of IWARN to rapidly gather information grows, so does the problem of information overload. The use of active guidance is the correct method for addressing this issue.

Active Guidance notifies users of relevant information and status they need to be aware of but are not. Active Guidance helps users accomplish their mission by providing assistance in interacting with the system. This capability also aids users in understanding their role and responsibilities. Active Guidance will monitor the system for information that is usually recorded, or transactions that are typically performed and make attempts to collect the information or engage transactions when they have not been performed. If operators decide not to perform a standard transaction the system could then attempt to capture the reason why.

Our Active Guidance System will rely on a data model to determine the user role and qualifications. The model will relate events, processes or transactions to roles and qualifications. Ideally, this mapping would be dynamic and customizable by the user. Using this model the system will identify when a process or event occurs and provide the user with appropriate response. This response would be presented to the user as a checklist. Use of historical data would allow the Active Guidance System to learn not only what responses are appropriate to given events but also enable the automatic storage of personal preferences to further simplify the users interaction with the system.

These features will result in a system that can be used by a broader range of warfighters, require less training and ensure that pertinent time critical information is presented to users in an actionable form NGI Systems believes this capability is critical given the growing number of tools and technologies the warfighter is required to utilize in the battlefield.

Dynamic Tagging:

Defining and collecting information according to predefined schema is constraining. Dynamic Tagging is the ability to define and capture new information types along with the ability to create new association types between information types on the fly. This capability will enable CONOPS concerning data collection and fusion to shift, grow and shrink dynamically. The following examples demonstrate the powerful implications of this technology.

- Explosions are usually reported to the SRC by several people. In the current WARN, this results in several Electronic Action Reports (EARs) being submitted, all representing the same explosion event. Multiple reports must be generated due to the predefined EAR data model having only one field for the reporter. With Dynamic Tagging the operator could simply add another reporter to the same event because the underlying system will define information objects independently and allow the associations to be created whenever they exist.
- Within the current IWARN System, EAR's have a concept of ownership. Ownership allows the EAR to be sent between action officers and attempts to promote resolution by ensuring the token of responsibility is always held. While the concept of ownership improves workflow efficiency it has limitations and undesirable side effects. Exercise data concludes that assigning a single action officer results in "hot potato" behavior between operators. Additionally, EAR's often require the collaboration of several operators yet single ownership limits the ability to notify or coordinate the collaboration of a group. With Dynamic Tagging, EAR's can be associated with multiple action officers or organizations for a dynamic set of purposes without modifying the data model.
- Tagging of information objects in connection with the use of Guard technology will provide fine grain selective information sharing. New classification types can be created on demand and each information object could be tagged with multiple classifications.

CONOPS and technology spiral in tandem. This technology will allow operators to specify business rules on the fly and allow the system engineers to focus on providing more ways for the

operator to do this. In expeditionary or coalition operations this will enable the seamless transformation of loosely or uncoordinated CONOPS into well defined force templates.

Publish & Subscribe:

The current IWARN Architecture is a 2-Tier, Client/Server Database Management System (DBMS). And like most systems of this type, the client contains a polling mechanism that retrieves information from data-sources at a specified refresh rate. Polling systems are inefficient because they don't know when data has changed. Thus, data is often reloaded when it hasn't changed and data that has changed is not received in an optimal way. To increase situation awareness the client polls more frequently, however, this consumes bandwidth which in turn decreases the amount of information available to the user.

To increase the efficiency of polling in IWARN, a Pedigree System was developed. The Pedigree System uses timestamps and triggers to track changes to entities in the database. When a client polls the database to refresh its cache it first checks a pedigree table to see which entities had updates or deletions. The client then proceeds to select only the data from these entities that has a timestamp after the most recent timestamp of the last refresh made against that entity.

While the Pedigree mechanism improves performance by only retrieving information deltas, it's far from an optimal solution. The following examples detail these shortcomings and how the Pub/Sub architecture is a better solution.

- If a large amount of data changes in a single transaction a polling system creates a Denial of Service (DOS) Attack because the database is overloaded with requests for new information. Even if the database was resilient, the flow of information into the system is hampered.

- Polling systems have no mechanism to prevent all clients from refreshing at the same time. The potential burst in traffic can bring down the system. As an example, imagine the burst in load on financial networks when the stock markets open at 9:30AM.

Publish & Subscribe architectures can resolve these problems by publishing information as resources and policies allow. This aids in preventing data loss by allowing data input to be treated with priority over data dissemination. The ability to publish also enables the system to be scaled for handling thousands of clients instead of hundreds and to operate over low-bandwidth connections. Most importantly, prioritization of this dataflow will allow the system to achieve optimal real-time situation awareness. Additionally, our architecture will be designed such that models for prioritization of dataflow can be plugged into the system.

Disconnected Operations:

As information networks replace paper workflow, their availability gains importance. In the context of C2 networks, information availability must be guaranteed. However, great potential exists within this context for events to occur, such as loss of electrons, network overload, and servers crashing, that can result in loss of network resources.

The IWARN architecture was engineered with these issues in mind. An offline mode was developed which enables clients to continue running after the network goes down. Also, the IWARN architecture persists an information cache in files of type BED (Business Entity Data). This allows the system to start in disconnected mode and prevents the user from loading all the current data each time the application starts. However, the current implementation of offline mode limits the user to viewing data. The ability to continue data entry while offline and resynchronize with the network when available is of key importance during a crisis response situation. Without this ability all operations must fall back to a paper workflow when electrons are lost.

The IWARN architecture has addressed the issue of batching work done offline and resynchronization to a limited degree. However, only one specialized data entry tool has been developed and each dataset and accompanying dataflow has different requirements making it a cumbersome implementation prone to human error.

However, the real difficulty is in developing a synchronization mechanism that doesn't require users to merge changes made at different times by them and other users. For example, a client may have 3 copies of the same data entity available when the system attempts to synchronize changes. One copy is the original data, another is the copy containing changes made by the user, and the third copy represents changes made to the data by other users since the synchronizing user received the original.

In a database containing information that's not historical this kind of merging can cause loss of important information because it forces the user merging changes to choose between there change and that made by another user. Using the publication mechanisms of the JBI will allow all changes to be stores in the Information Object Repository (IOR) and thus prevents users from making complicated merge decisions and potentially loosing valuable information.

Since the JBI stores all information objects in the IOR the process of synchronizing simply requires the client to publish all changes.

Data Archiving and Temporal Analysis:

Historical data has great value when trying to learn from and improve methods for dealing with crisis response. This data is often lost because the mechanism for retaining it doesn't exist or must be performed manually by someone in addition to normal duty.

Currently, no mechanism exists in the IWARN System to generically store all data historically. Further, no system exists that enables archived data to be reloaded into the system. Thus, the database grows until it reaches a point when the data is archived and deleted from the system. There is no way to reload system state as of a given date or for a given window in time.

By using a historical data model, IWARN inherits export, import and replay capabilities. The data can then be archived to disk as data looses value and reloaded if needed. Replay becomes possible by querying for status during various time slices.

Force Templates:

Transient organizational structures pose a challenge to defining coordinated CONOPS. Defining an entities responsibilities, capabilities, availability, protocols, and CONOPS is the first step in attempting to combine the efforts of disparate forces. Within the context of the proposed system this type of information would have the following benefits.

Within the current IWARN System users must select a duty position upon sign in. The duty position is provided so other users understand who is on the system from a responsibility and capability perspective. In the context of tightly integrated groups this solution works. However, in the case of loosely integrated groups each one is likely to be unfamiliar with the duty position of others. Using Force Templates, selection of duty positions would be unnecessary since the system knows your credentials. Since credentials or responsibilities could be mapped to the language of each group, operators would be able to find the right people to collaborate with. This would prevent situations such as all hospital personnel signing on as MEDICAL. It would also prevent them from signing on as some cryptic position name only understood by hospital staff. Ex. MED_SR_SGN, MED_SF_NRS.

Beyond improvements in collaboration, Force Templates could provide the ability to map CONOPS between organizations which then could lead to the ability to define joint CONOPS.

Dynamic Planning:

Most planning tools are starved for information. IWARN provides a unique opportunity for these tools to be integrated with live status of unit resources thereby enabling the detection of vulnerabilities in defense plans and the ability to take corrective action mitigating operational impacts.

By utilizing IWARN's historical data, planning tools can begin to predict when resources are unavailable thus lowering the probability of a plans successful execution. Predictive Battlespace Awareness will result in higher levels of situation awareness.

5.0 RESULTS AND DISCUSSION

This report discusses the requirements of an integrated information managements system and progress on the effort between October 2005 and May 2006. Progress under this effort focused on: cleanup of the Oracle database and migration to Oracle 10G; security lockdowns in accordance with the DISA Gold Standard; documentation of the existing system; and bug fixes in the existing system.

Our level of effort on the IIMS has resulted in a more versatile battle management system capable of transforming to match the demands of the mission at hand. This advantage will result in faster OODA(Observe Orient Decide Act) cycles for the commander and her action officers. Additionally, the ability to dynamically adjust with CONOPS increases the system's potential application in other areas. NGI Systems believes this potential will lead to an evolutionary jump in the ubiquitous use of the IWARN System during normal operations as well as during post attack recovery.