NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

Examination of the Open Market Corridor

By: **James T. Chavis**
James Cheatham
Vaughn Gonzalez
Rolando Ibanez
Rich Nalwasky
Martin Rios
Marco Turner

December 2003

Advisors: **Ron Tudor**
Rod Tudor

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY U. S.E ONLY ***(Leave blank)***	**2. REPORT DATE** December 2003	**3. REPORT TYPE AND DATES COVERED** MBA Professional Report	
4. TITLE AND SUBTITLE: Title (Mix case letters) Examination of the Open Market Corridor			**5. FUNDING NUMBERS**
6. AUTHOR(S) James T. Chavis, James Cheatham, Vaughn Gonzalez, Rolando Ibanez, Rich Nalwasky, Martin Rios, Marco Turner			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Present procurement practices for the purchase of commercial, commercial off-the-shelf, and non-developmental products and services can take anywhere from thirty days to sometimes years to procure and deliver to the end user. Federal Government contracting offices spend costly amounts of time advertising the actions and preparing formal solicitation documents for each purchase order generated by the end-user. This translates to high administrative costs, high prices, and, at times, marginal performance. In an effort to ease the administrative burden on the contracting system by capitalizing on current technologies, a new system was recently developed by Professor Ron Tudor and students at the Naval Postgraduate School. This new program is currently under testing by a prime contractor under the auspices of the Department of Interior. The new on-line contracting/procurement program, known as the Open Market Corridor, will allow Federal, State and local Government users to purchase supplies and services on-line through the use of electronic catalogs and embedded contract templates accessible via the Internet. This thesis project will review various aspects of the new program evaluating current efficiencies and recommend modifications in an effort to improve the current procurement and logistics process.

14. SUBJECT TERMS Procurement, E-commerce, E-procurement, Contingency Contracting, Defense Transportation System, Government Wide Purchase Card, Wireless Communication, IT Security			**15. NUMBER OF PAGES** 265
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXAMINATION OF THE OPEN MARKET CORRIDOR

James T. Chavis, Lieutenant Commander, United States Navy
James Cheatham, Lieutenant Commander (sel), United States Navy
Vaughn Gonzalez, 2nd Lieutenant, United States Air Force
Rolando Ibanez, Lieutenant, United States Navy
Richard Nalwasky, Lieutenant Commander, United States Navy
Martin Rios, Lieutenant Commander, United States Navy
Marco A. Turner, Lieutenant Commander (sel), United States Navy

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2003

Authors:

_____ _____
James T. Chavis Vaughn Gonzalez

_____ _____
James Cheatham Rolando Ibanez

_____ _____
Richard Nalwasky Martin Rios

_____
Marco A. Turner

Approved by:

_____
Ron Tudor, Lead Advisor

_____
Rodney E. Tudor, Support Advisor

_____
Douglas A. Brook, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

EXAMINATION OF THE OPEN MARKET CORRIDOR

ABSTRACT

Present procurement practices for the purchase of commercial, commercial off-the-shelf, and non-developmental products and services can take anywhere from thirty days to sometimes years to procure and deliver to the end user. Federal Government contracting offices spend costly amounts of time advertising the actions and preparing formal solicitation documents for each purchase order generated by the end-user. This translates to high administrative costs, high prices, and, at times, marginal performance. In an effort to ease the administrative burden on the contracting system throughout the DoD by capitalizing on current technologies, a new system was recently developed by Professor Ron Tudor and students at the Naval Postgraduate School. This new program is currently under testing by a prime contractor under the auspices of the Department of Interior. The new on-line contracting/procurement program, known as the Open Market Corridor, will allow Federal, State and local Government users to purchase supplies and services on-line through the use of electronic catalogs and embedded contract templates accessible via the Internet. This thesis project will review various aspects of the new program evaluating current efficiencies and recommend modifications in an effort to improve the current procurement and logistics process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE

In response to the needs of the contracting workforce and mandates of the Federal Acquisition Regulation (FAR), Professor Ron Tudor and students of the Naval Postgraduate School (NPS) conceived a revolutionary and superlative acquisition system. This system, the Open Market Corridor (OMC), addresses the needs of the contracting professional and offers the potential to fulfill ALL the goals of the federal procurement system. This research seeks to evaluate the potential effectiveness of the current system and recommend modifications in an effort to improve the current procurement and logistics process.

B. ISSUES FACING THE ACQUISITION COMMUNITY

1. Logistics Transformation

Transformation is an oft-used but rarely defined term. In this context, military transformation refers to the set of activities by which the Department of Defense (DoD) attempts to harness the revolution in military affairs to make fundamental changes in technology, operational concepts, doctrine, and organizational structure. The model for military transformation is not just about acquiring new military systems, but also about modifying doctrine, organizations, training and education, material, leadership, and personnel policies to maximize the capabilities of future military forces (Flournoy, Page 14). Nowhere is this idea of military transformation more pervasive than in the world of military logistics.

As with any large undertaking, DoD Logistics Transformation is a complex and difficult undertaking. With the advent of new and innovative technology, DoD is close to developing a blueprint for the future. To ensure the success of this transformation the importance of logistics (how we support our warfighters on the battlefield) has to be adequately imbedded in leadership priorities. Continuing to regard logistics as the secondary 'tail' to warfighter doctrine, training, and armament will have unacceptable consequences in the 21st Century battle space, resulting in decreased ability to achieve national security objectives and costs. Leadership must clearly provide a focus and a

mechanism for review and recalibration, as required, with the Services and OSD agencies.

The 1998 Logistics Transformation Study emphasized the critical, indeed fundamental, importance of logistics to the success of U.S. military operations. The study noted that an artificial dichotomy exists between operations and logistics and that this dichotomy threatens to undermine DoD's planned revolution in military affairs. The study also noted that a properly reformed logistics system would reduce a Combatant Commander's operational footprint, cost less money, and effectively support U.S. military strategy. To enable a Combatant Commander to "pull" the requisite logistics support, new tools and systems are needed. These tools must be fully integrated into the operational environment (OU. S.D, AT/L, January 2001).

The study highlights the vital need to transform the process of deploying and sustaining the warfighter. Among other things, the Task Force called for DoD to exploit commercial capabilities and accelerate the pace of change. For the U.S. military to maintain its position of global leadership, it must transform its logistics system. Failure to do so imperils the ability to deploy and sustain military forces to meet the new threats the U.S. will face in the future (OU. S.D, AT/L, January 2001).

2. Acquisition Work Force Reductions

Federal contracting began declining in the late 1980s as the Cold War drew to a close and defense spending decreased. This decline in federal contracting continued for most of the 1990s, reaching a low of about $187 billion in fiscal year 1999. Spending subsequently increased to about $204 billion in fiscal year 2000. As Figure 1 illustrates, between fiscal year 1990 and fiscal year 2000, purchases of supplies and equipment fell by about $25 billion, while purchases of services increased by $17 billion, or about 24 percent. Consequently, purchases for services now account for about 43 percent of federal contracting expenses—the largest single spending category (GAO, May 2001). The increase in the use of service contracts coincided with a 21-percent decrease in the federal workforce, which fell from about 2.25 million employees as of September 1990 to 1.78 million employees as of September 2000. The future acquisition professional will have to become a better manager of services than they have in the past.

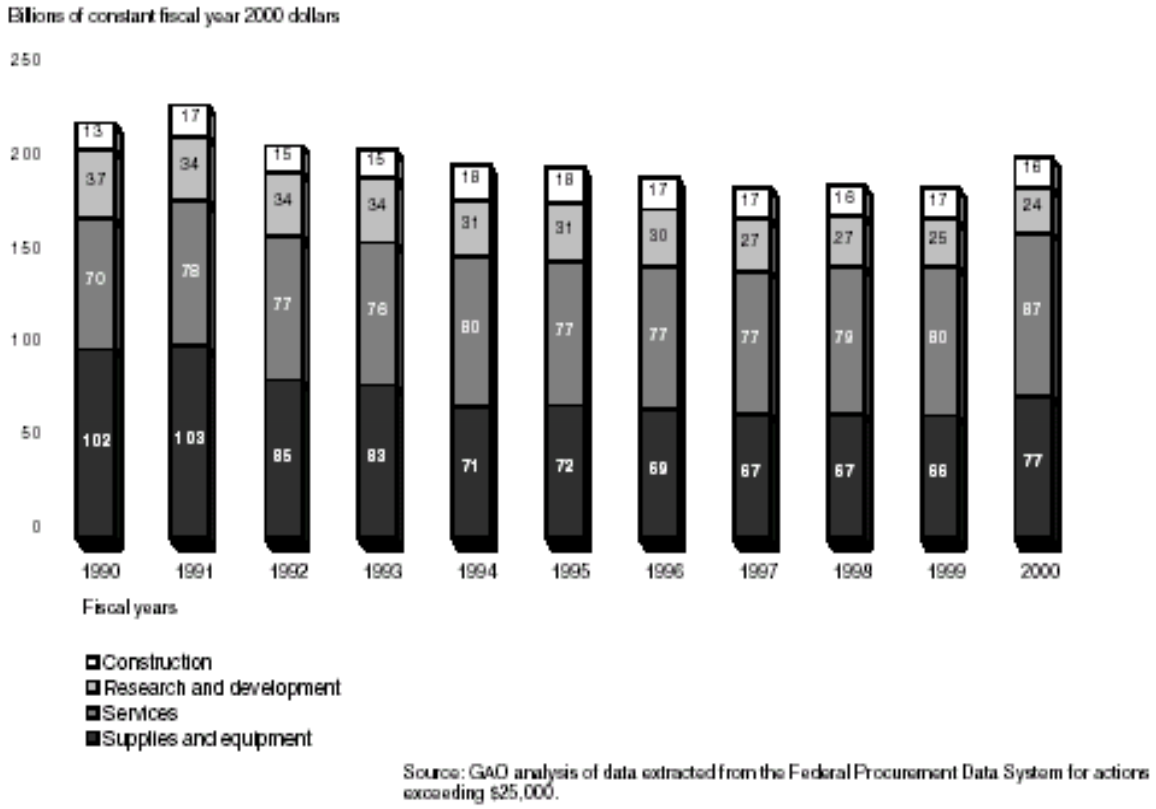


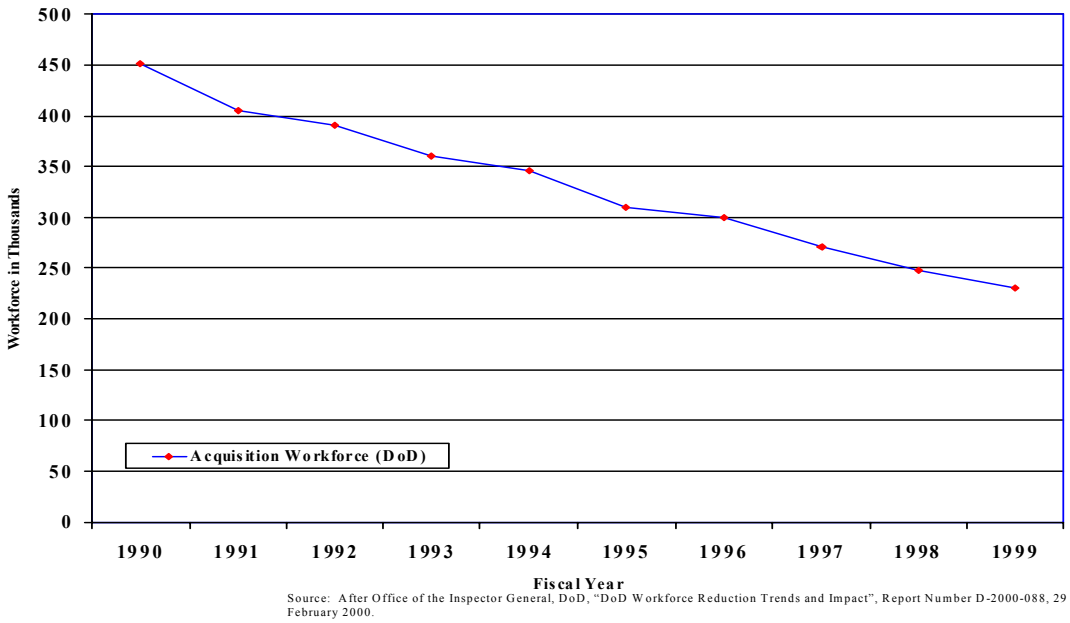
Figure 1. Changes in Federal Contract Spending, Fiscal Year 1990 to Fiscal Year 2000

In a general sense, DoD acquisition workforce reductions are part of the overall downsizing of the Federal and Defense workforce. However, Congress has singled out the DoD acquisition population for separate downsizing emphasis, even while allowing the Secretary of Defense considerable latitude in implementing reductions. Using the congressional definition of the DoD acquisition workforce, DoD reduced its acquisition workforce from 460,516 to 230,556 personnel (Figure 2), about 50 percent, from the end of FY 1990 to the end of FY 1999; however, the workload has not been reduced proportionately. From FY 1990 through FY 1999, the value of DoD procurement actions decreased from about $222 billion to about $188 billion, about 15 percent, while the number of procurement actions increased from about 13.2 million to about 14.8 million, about 12 percent (a result of increased modifications vice new contract actions). The greatest amount of work for acquisition personnel occurs on contracting actions over $100,000, and the annual number of those actions increased from 97,948 to 125,692,

about 28 percent, from FY 1990 to FY 1999. The following impacts from acquisition workforce reductions were identified by the organizations surveyed:

- Increased backlog in closing out completed contracts (3 organizations),
- Increased program costs resulting from contracting for technical support versus using in-house technical support (7 organizations),
- Insufficient personnel to fill-in for employees on deployment (1 organization),
- Insufficient staff to manage requirements (9 organizations),
- Reduced scrutiny and timeliness in reviewing acquisition actions (4 organizations),
- Personnel retention difficulty (6 organizations),
- Increase in procurement action lead time (1 organization),
- Some skill imbalances (9 organizations), and
- Lost opportunities to develop cost savings initiatives (2 organizations).

The fourteen DoD acquisition organizations surveyed anticipated additional adverse effects on performance if further downsizing occurs (IG-DoD, February 2000).



Source: After Office of the Inspector General, DoD, "DoD Workforce Reduction Trends and Impact", Report Number D-2000-088, 29 February 2000.

Figure 2. Acquisition Workforce Reduction

Likewise, there is cause for serious concern due to the possibility that the DoD acquisition workforce could lose about 55,000 experienced personnel through attrition by FY 2005 and due to the overall disconnects which exists between workload forecasts, performance measures, productivity indicators, and plans for workforce sizing and training. The expected loss of experienced procurement professionals from the workforce is exacerbated by pending legislation that seeks to slice an additional 13,000 acquisition workforce members from the Government's payrolls, despite an increased workload of oversight and judgment application. It will become increasing evident in the years to come that agencies do not have the right people with the right skills to manage procurements.

DoD's leadership had anticipated that using streamlined acquisition procedures would improve the efficiency of contracting operations and help offset the effects of workforce downsizing. To improve the acquisition process, DoD implemented over forty reform initiatives over the last five years. The DoD acquisition organizations improved efficiency in contracting through acquisition reform initiatives, such as using credit cards for processing acquisitions of $2,500 or less, using simplified acquisition threshold procedures for acquisitions of $100,000 or less, and using reengineered acquisition procedures for acquisitions in general. These improvements helped offset the impact of acquisition workforce reductions and may have increasing beneficial effect as time passes and they are fine-tuned. Nevertheless, concern is warranted because staffing reductions have clearly outpaced productivity increases and the acquisition workforce's capacity to handle its still formidable workload (IG-DoD, February 2000). Efficiency gains from using streamlined procedures have not kept pace with acquisition workforce reductions. Consequently, the extent to which agencies provide the necessary training, guidance and tools to their workforce will determine if the acquisition community will be able to effectively meet future customer demands as mandated by the FAR.

3. Regulatory Implications

a. Standard Procurement System

The Standard Procurement System (SPS) is an acquisition system mandated for use by field contracting activities. The Director, Defense Procurement (DDP) is responsible for acquiring and deploying SPS, as well as for software installation, training, and all steps necessary to gain user acceptance of SPS, a program initiated in November 1994 to provide an automated system that would perform DoD procurement functions. SPS is designed to improve the speed and effectiveness of contract placement and contract administration functions from receipt of requirement until contract closeout at all DoD procurement organizations. SPS is intended to replace seventy-six procurement systems and manual processes. As of December 30, 2000, the Program Management Office reported that 16,207 users at 745 DoD sites used SPS. By the end of FY 2003, SPS is expected to serve 43,000 users at 1,100 DoD sites. Estimated costs for SPS are $433.5 million to procure commercial software licenses and support services. Estimated life-cycle costs for FY 1995 through FY 2005 are $3.7 billion. Operational benefits from SPS are estimated at $1.4 billion derived primarily from increased productivity and reduced costs associated with paper transactions. (IG-DoD, March 2001)

Unfortunately, due to the weakness of its spiral development implementation, a significant number of system deficiencies and inaccuracies exist, rendering the system neither operationally effective nor operationally suitable for administering large procurement contracts. A DoD IG audit dated 13 March 2001 reported results based on responses to a web-based survey of statistically selected personnel from a population of SPS 4.1 users at 534 DoD procurement sites. About 85.9 percent of SPS users stated that SPS was available always or most of the time. The SPS Program Management Office in the Defense Contract Management Agency had taken steps to better meet user needs, and respondents stated that SPS had the potential of being a very effective and useful tool, but more is required to improve the software and gain greater acceptance and user confidence. Specifically, the projected survey results indicated that:

- 60.8 percent of SPS users preferred a procurement system other than SPS,
- 45.8 percent of SPS users stated that the number of workarounds increased,
- 51.4 percent of SPS users stated that productivity has not increased since SPS version 4.1 was implemented, and
- 63.5 percent of SPS users stated that SPS had not substantially contributed to the DoD goal of paperless contracting. (IG-DoD, March 2001)

Further, projected survey responses indicate that about 26.5 percent of the personnel licensed to use SPS version 4.1 have not used it because SPS either lacked the functionality for those sites or employees received SPS when it was not needed to perform their jobs. As such, many procurement offices still do not use the system today.

b. Federal Acquisition Streamlining Act and the Clinger-Cohen Act

The Federal Acquisition Streamlining Act (FASA) of 1994 significantly changed how the Government does business. The Clinton Administration passed the act to create a "Government That Works Better and Costs Less." In addition, it was designed to overhaul the cumbersome and complex procurement system of the Federal Government, which required costly paperwork for even small purchases and weeks, months, or sometimes years of waiting between order and delivery of goods.

The Act includes changes in the following regulatory requirements:

1. Eliminating most paperwork and record keeping requirements for acquisitions below $100,000 within the Simplified Acquisition Threshold (SAT).
2. Allowing direct “micro purchases” of items below $2,500 without competitive quotes or compliance with Buy American Act and certain small business requirements.
3. Exempting commercial product procurements from certain existing as well as future enacted laws, including exemptions from the submission of cost or pricing data and the cost accounting standards (CAS) requirements; establishing an agency preference for commercial items; and other continuing initiatives promoting the acquisition of commercial items to minimize time delays, research and development, and detailed

design specifications and testing, thereby making Government procurement easier and less costly.

4. Establishing a Government-wide Federal Acquisition Computer Network (FACNET) to convert a current acquisition process overburdened by paperwork to an expedited electronic data interchange system (EDI) readily accessible to the public. Through use of the FACNET, small businesses have easier and more efficient access to Government contract opportunities all over the country. The National Defense Authorization Act of 1998 repealed the FACNET requirement, changing it to the use of Electronic Commerce/Electronic Data Interchange (EC/EDI). The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) have agreed on a final rule amending the Federal Acquisition Regulation (FAR) to further implement section 850 of the National Defense Authorization Act for Fiscal Year 1998 and implement section 810 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001. This rule finalizes the interim rule that designated Federal Business Opportunities (FedBizOpps) as the Government Wide Point of Entry (GPE) for procurement opportunities. In addition, this final rule makes the GPE the exclusive official source for public access to notices of procurement actions over $25,000. (Federal Register, October 2003)

5. Reserving all acquisitions over $2,500 but under $100,000 exclusively for small business concerns, unless the contracting agency is unable to obtain offers from at least two qualified small business firms.

6. Expanding the Small Disadvantaged Business set-aside program to civilian agency procurements. (The set-aside program has since been refined. It now includes closer scrutiny rather than a blanket policy on selection. Criteria for selection also identify **hub zones--historically under-utilized business and economic areas**.)

7. Establishing a new 5 percent contracting goal for women-owned small businesses.

8. Creating a "Small Business Procurement Advisory Council" comprised of representatives from federal agencies, which will give high-level attention and focus to small businesses.

In addition to the FASA changes, the Clinger-Cohen Act was formed in 1996 abolishing the requirement to make GSA the central procurement authority for ADP resources, while the Government works to fully implement Electronic Commerce/ Electronic Data Interchange (EC/EDI).

Commercial customers have always been able to obtain products and services, faster and cheaper than Government customers. For items over $2,500, Government customers, on average, have to wait several weeks to years to receive the requested item. As a result of the Internet, the infrastructure is available to facilitate and mirror commercial EC/EDI practices as mandated by the Clinger-Cohen Act. To maintain currency in technological developments, contractors of the OMC will remain fluid and dynamic, avoiding obsolescence while providing best value to the Government.

c. Multiple Award Task Order Contract (MAC) Instruments

Sections 1004 and 1504 of Public Law 103-355 (FASA) established the authority for awarding multiple award task order contracts for services and delivery order contracts for supplies. The law requires that all contractors awarded Multiple Award Task Order Contracts (MACs) shall be provided a "fair opportunity" to be considered for each task or delivery order over $2,500. While the law says that ordering procedures should be tailored to each contract, the law permitted four specific exceptions to what it described as fair opportunity to be considered (or competitive procedures). Congress has repeatedly emphasized its intent that those are the ONLY exceptions in several authorization acts since FASA was passed. However, users of these GWAC instruments have been accused of bundling contract actions, and improperly generating sole-source purchases, as addressed by the General Accounting Office (GAO), the National Aeronautics and Space Administration (NASA) and DoD Inspectors General. Unfortunately due to these abuses, now the Defense Authorization Act Section 803 requires DoD contracting officers to compete (MAC) instruments over $100,000, and 801 requires DoD to designate a regulatory agent called a Government-wide acquisition contracts (GWAC) czar. These actions threaten to reverse the streamlining initiatives of the Federal Acquisition and Streamlining Act (FASA). If changes are not implemented

soon these Congressional Defense Authorization Acts will lengthen the procurement process and lessen the positive streamlining impacts of FASA.

C. DEFINITIONS

1. Acquisition Workforce

Over the years, DoD has used various definitions to identify the DoD acquisition workforce without achieving a consensus. DoD Instruction 5000.58, "Defense Acquisition Workforce," Change 3, January 13, 1996, defines the acquisition workforce as permanent civilian employees and military members who occupy acquisition positions, who are members of an acquisition corps, or who are in acquisition development programs. In the instruction, DoD identifies twenty-one DoD acquisition organizations whose missions include planning, managing, and executing acquisition programs in accordance with DoD Directive 5000.1, "Defense Acquisition," May 12, 2003, and DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," Change 4, May 11, 1999 (IG-DoD, February 2000).

2. Contingency Contracting Support Kit

The Contingency Contracting Officer (CCO) can be tasked to deploy with little or no notice. As such, the CCO should consolidate materials, which will be required to perform contracting duties in the contingency environment—a contingency contracting support kit. The FAR and DFARS and any branch specific contingency operating manual can be utilized to help develop the kit. The kit must be comparable to the needs of the specific contingency requirements. Yet, at a minimum the kit should consist of reference manuals (FAR, DFAR etc), sixty to ninety days of hard copy forms, a chargeable laptop (with several spare battery packs), communication equipment, office supplies, field safe and so forth. As the kit is developed, consider space and weight requirements in the transportation assets for the deploying contracting force. The CCO should make sure they are a part of the Time Phased Force and Deployment List (TPFDL) to ensure space is allocated for the kit. An example of the types of material to be included in the kit is described in more detail in Appendix F.

3. Focused Logistics

With the end of the Cold War, logistics has taken a more prominent role in military planning and can be best illustrated in the "Focused Logistics Campaign Plan". Here, focused logistics is defined as "the ability to provide the joint force the right personnel, equipment, supplies and support in the right place, at the right time, and in the right quantities, across the full range of military operation" (Paulus, 2). The logistician is required to provide "more accurate and timelier logistics information using a more responsive and agile logistics support structure that can be supported from distant bases" (Paulus, 3). "This ability will be achieved 'through a real-time, web-based information system providing accurate, actionable visibility as part of a common relevant operational picture...." (Paulus, 2). DoD has introduced a number of software products over the course of the past few years to simplify the acquisition process. From programs that track and maintain inventories to software that focuses on ordering high priority items, these programs have had varying degrees of success. The DoD EMALL, a fairly recent creation of the Defense Logistics Agency, and the Open Market Corridor (OMC) allow customers (in this case the logistician) web enabled ordering, thus fulfilling the spirit of the concept of focused logistics.

D. RESEARCH AREAS

In spite of departmental cuts, contract specialists are still responsible for preserving the public trust and maintaining the integrity of the procurement process while fulfilling public policy objectives through the use of sound business practices. For acquisition managers to have efficient and effective tools to satisfy the high standards outlined in the guiding acquisition principles is necessary to fulfill these goals. The Open Market Corridor (OMC), born out of this environment, is potentially the focused logistics tool required to make this a reality.

This research project evaluates the effectiveness of OMC, by reviewing the following areas:

1. Contingency Contracting

The OMC presents the potential to significantly reduce the workload of the contracting professional during normal procurement actions and reduce the footprint of the warfighter in a contingency environment. This research explores its potential to aid the contingency contracting officer responding to contingencies domestically as well as internationally. Furthermore, movement of material into contingency areas presents considerable challenges. This research also explores the effectiveness of using commercial carriers and the Defense Transportation System (DTS) to move material into the contingency areas as well as how effectively OMC can interface with the DTS and commercial logistics systems to increase the visibility of material for the contingency contracting officer.

2. Government-wide Purchase Card

This research reviews the use of the Governmentwide Purchase Card in the Open Market Corridor and analyzes the strengths and weaknesses of this application. Specifically, the following concerns are addressed: reporting in terms of required data and the possibility of duplicate reports, Contracting Officer review of purchases, use of the Government Wide Purchase Card for micro-purchases vs. as a method of payment, and use of the Government Wide Purchase Card for overseas purchases through the OMC.

3. IT Security

This research area explores anti-fraud and encryption devices for combating possible security breaches associated with online purchases from the DoD EMALL System and Open Market Corridor. Database hackers, viruses, worms, and intercepted signals from wireless systems all pose threats to the electronic procurement systems.

4. Wireless Technology

This section explores wireless technology application to the OMC. Use of computers has been limited in the contingency environment because of the need for established infrastructure. A brief history of wireless technology is explained followed

by the most recent technological breakthroughs of wireless technology to include direct satellite connectivity. This section will explain a concept for theater setup of computers, power supply, and satellite connectivity that will ensure immediate use of the Open Market Corridor even before initial infrastructure has been established.

E. RESEARCH QUESTIONS

1. Contingency Contracting

a. Primary Research Questions

What are the basic requirements, functions/functionalities required by a contingency contracting officer for successful execution of duties in a contingency environment?

Typically areas contingency contracting officers deploy to lack sufficient infrastructure to sustain forces. Is it possible for a commercial shipping company to support a contingency contracting officer in this type of environment? What capabilities will be required to be able to successfully move material into these areas?

Evaluation of several of the top shipping organizations is required (FedEx, DHL, Emery, or UPS). Who would be the best shipper to meet our needs? Can any meet the requirements of the contingency contracting officer? What would be the criteria for evaluation?

Traditionally in an unsecured environment (war or other hostilities), Defense Transportation System (DTS) is the shipping avenue of choice. When is the use of DTS required (mandated)? Is DTS the best choice in a contingency environment? How does material flow into DTS? When is the use of WWX appropriate?

b. Secondary Research Questions

Can OMC accommodate some or all of the needs of the contingency contracting officer? Does the system have sufficient functionality as is or will modifications be required?

Can OMC interface with the commercial shipping world to provide visibility in the field to aid the contracting officer?

What hardware/software additions or modifications have to be made to the system for it to be able to perform the functions identified by this research?

2. Government-wide Purchase Card

a. Primary Research Questions

Several issues consistently arise when managing a credit card program. How can the use of OMC reduce/eliminate/prevent these issues?

b. Secondary Research Questions

What are some of the concerns when using the credit card overseas?

3. IT Security

a. Primary Research Questions

What are the Internet security vulnerabilities within the OMC infrastructure?

b. Secondary Research Questions

What measures are in place to ensure continuous security updates?

What technology is available to combat these security vulnerabilities?

4. Wireless Technology

a. Primary Research Questions

What type of equipment/software support would be required to provide wireless support for the contracting officer operating in an immature, semi-mature, or mature environment?

b. Secondary Research Questions

How would wireless technology integrate with OMC/DoD E-mall?

II. CONTINGENCY CONTRACTING

U.S. Forces have deployed to perform tasks in support of national objectives throughout the world. The military has consistently been called upon to take the lead in a variety of missions quite different than the missions of the past. In an effort to maintain an advantage over the amorphous threat poised by today's elusive enemies, the military has to evolve (transform) into a more agile force capable of meeting the enemy in a variety of environments. As such, the technology and training must also transform to keep step with the changing force structure and employment strategies. The need for a viable contingency contracting capability arises from the complex nature of the acquisition process and the necessity to support joint or multinational forces. A trained and properly equipped contracting cadre to support contingency operations ensures that proper methods are employed in the procurement of supplies and services and that responding forces receive the required logistics resources to perform their mission. Localized contracting reduces the dependence on Continental United States (CONUS) based logistics systems, reduces response time and frees up critical storage space within military airlift and sealift channels (NAVSUPINST 4230.37B, 1).

This chapter provides a general overview of the joint theater logistics concept and how contracting fits into the logistics planning. The chapter further reviews the various types of contingencies which today's military will face in the coming years, the advertised recommended organization of these forces and how our forces are actually organized and deployed in a variety of contingencies in various locations around the world. We will further review the requirements of the logistics arm to support these forces, specifically the contingency contracting aspects, movement of material in a contingency environment via commercial as well as defense assets, and the issues our contingency contracting officers face. Finally suggestions as to how OMC can supplement or improve on the current process as well as recommendations as to how OMC should be modified to meet the challenges of the contingency contracting officer are presented.

A. GENERAL LOGISTICS OVERVIEW

Logistics is the science of planning and carrying out the movement and maintenance of forces. In its most comprehensive sense, it includes those aspects of military operations which deal with design and development, acquisition, storage, movement, distribution, maintenance, evacuation, and disposition of materiel; movement, evacuation, and hospitalization of personnel; acquisition or construction, maintenance, operation, and disposition of facilities; and acquisition or furnishing of services. Major logistic areas of responsibility are shown in figure 3.

Source: Joint Publication 4-0; Doctrine For Logistics Support of Joint Operations

Figure 3. Major Logistics Areas

The science of logistics concerns the integration of strategic, operational, and tactical sustainment efforts within the theater, while scheduling the mobilization and deployment of units, personnel, equipment, and supplies in support of the employment concept of a geographic combatant commander. The relative combat power that military forces can bring to bear against an enemy is constrained by a nation's capability to plan for, gain access to, and deliver forces and materiel to the required points of application across the range of military operations.

Considerations in developing a logistic system include logistics sourcing, distribution, geography, weather, transportation, logistic capability, asset visibility, logistic enhancements, logistic resources within the theater, availability of existing logistic facilities; and options for purchase, lease, or construction of other facilities, logistic infrastructure protection, echelon of support, contracted support, assignment of responsibility, and availability of host-nation support. As such the combatant commander has to develop a logistics plan tailored to meet the challenges of the mission at hand as well as develop a system to coordinate the resources necessary to meet mission objectives.

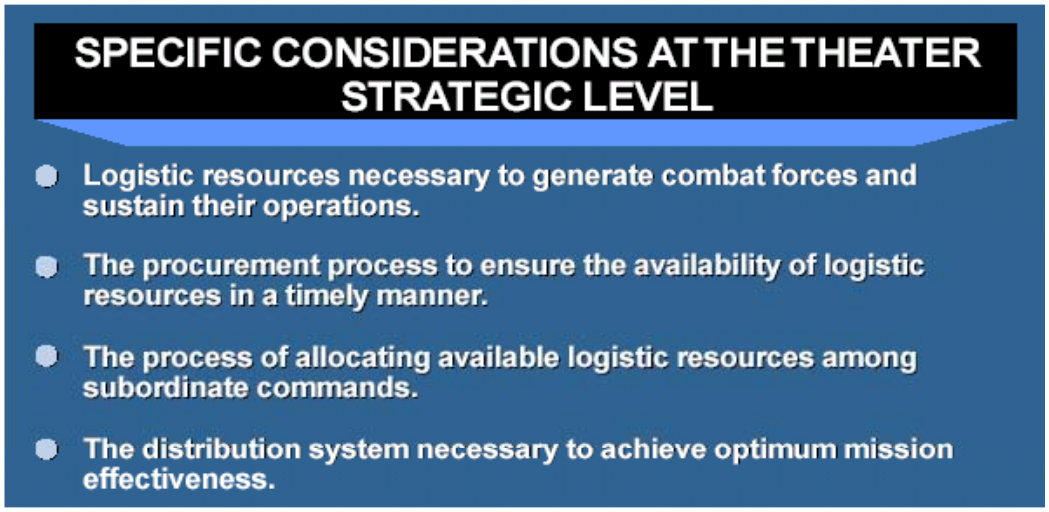
Logistics functions include supply, maintenance, transportation, civil engineering, health services and other services. Supply is the function of acquiring, managing, receiving, storing, and issuing the materiel required by forces. Maintenance includes actions taken to keep materiel in a serviceable condition or to upgrade its capability. Transportation is the movement of units, personnel, equipment, and supplies from the point of origin to the final destination. Civil engineering provides the construction, operation, maintenance, damage repair, and reconstitution of facilities, roads, and utilities and logistic infrastructure. Health services include medical evacuation, hospitalization, medical logistics, medical laboratory services, blood management, vector control, preventive medicine services, veterinary services, and dental services. Other services are nonmaterial support activities provided by Service personnel and the logistic community that are essential to force support. For each of the above functional areas, the combatant commander should consider these four elements of the joint theater logistic process: procurement and contracting, distribution, sustainment, and disposition and disposal.

These elements apply to planning and implementation across the full range of military operations, including multinational operations. (JP 4-0, page v)

Source: Joint Publication 4-0; Doctrine For Logistics Support of Joint Operations

Figure 4. Logistics Support Requirements Functional Areas

B. RESPONSIBILITIES FOR JOINT THEATER LOGISTICS



Source: Joint Publication 4-0; Doctrine For Logistics Support of Joint

Figure 5. Specific Considerations at the Theater Strategic Level

The exercise of directive authority for logistics by a combatant commander includes the authority to issue directives to subordinate commanders. Combatant commanders exercise combatant command (command authority) (COCOM) over assigned forces. COCOM includes directive authority for logistics, giving the combatant commander the unique ability to shift logistic resources within the theater. This directive authority ensures the effective execution of approved operation plans, the effectiveness and economy of the operation, and the prevention or elimination of unnecessary facility duplication and overlapping functions. It also promotes synchronization of effort and builds cohesion among the Service component commands in supporting the combatant commander.

Implementation and execution of logistic functions remain the responsibility of the Services and the Service component commanders. Each Service is responsible for the logistic support of its own forces, except when logistic support is otherwise provided for by agreements with national agencies or allies, or by assignments to common, joint, or cross servicing organizational structures. The combatant commander reviews the requirements of the Service component commands and establishes priorities through the approved deliberate and crisis action planning processes to use supplies, facilities, mobility assets, and personnel effectively.

Logistic responsibilities for subordinate forces to the combatant command follow single-Service command channels, except when specifically directed otherwise either by the authority assigning those subordinate forces to the combatant command or by the Secretary of Defense, when common, joint, cross-servicing, or inter-servicing agreements and procedures provide other responsibilities, or when the geographic combatant commander gives the commander of a subordinate joint force directive authority for a common support capability within that subordinate commander's joint operations area. Combatant commanders are responsible for allocating critical resources, coordinating supply support among the Service components, establishing supply buildup rates, and authorizing theater stockage levels.

Although nations are ultimately responsible for providing logistic support for their own forces, the capability of participating nations' forces to support themselves

organically varies widely in multinational (allied and coalition) operations. Contractors, host nations, or other participating nations may supply substantial non-organic support, but such logistic needs must be identified during the planning phase. The capability of allies and coalition partners to logistically support a multinational operation must be carefully considered, since they may serve as both a source and a competing demand for logistic support. Combatant commanders must be attuned to this, and should strive to negotiate, conclude and integrate the use of acquisition and cross-servicing agreements and associated implementing arrangements for use in time of crisis. Due to the unique issues that arise from these arrangements, contracting in multinational operations is discussed in more detail later in the chapter.

The geographic combatant commander is responsible for provision of supplies for Department of Defense civilians in occupied areas in accordance with current directives, obligations, and treaties the United States recognizes. The geographic combatant commanders are responsible for maintaining an effective distribution network and exercising visibility and positive control of personnel, materiel, and services. The combatant commanders are responsible for coordinating maintenance and salvage; establishing bases; coordinating real estate requirements; and planning, constructing, and maintaining roads, bridges, utilities, and facilities. Geographic combatant commanders are also responsible for coordinating and integrating health service support and the search, recovery, identification, care, and evacuation or disposition of deceased personnel within their theaters. The Services are normally responsible for facility acquisition funding and support. In contingency operations, one Service or agent is normally assigned base operations support responsibility for all Services in a particular area or base; thus they are responsible for facility acquisition funding for all Services. (JP 4-0, page vi)

The Commander in Chief, U. S. Transportation Command (USCINCTRANS) has the mission to provide common-user air, land, and sea transportation and terminal services to deploy, employ, sustain, and redeploy military forces in order to meet national security objectives throughout the range of military operations. Combatant commanders coordinate their movement requirements and required delivery dates with

USCINCTRANS. Geographic combatant commanders retain command of Service component transportation assigned or attached to the theater.

Supported combatant commanders, in coordination with USCINCTRANS, balance the transportation flow of the joint force through effective employment planning. Balance is primarily a function of force composition and transportation flow, but planned theater distribution and joint reception, staging, onward movement, and integration capabilities must also be considered. Logistic planners must focus on seamless deployment, distribution, and sustainment in order to properly enable the employment concept of the mission or task at all levels.

The combatant commander's strategic logistic concept focuses on the ability to generate and move forces and materiel into the theater base and on to desired operational locations where operational logistic concepts are employed. Tactical planning is done primarily by the Service components. Planners must identify and assess critical or key issues unique to a specific operation plan they must support. These issues include the increased demand associated with an expanding force, critical supply items, flow or process constraints, control of all means of transportation (including those provided by allies and host nations), critical infrastructure protection, and the resourcing of supplies and services from civilian, coalition, and allied sources.

Combatant commanders must ensure that their campaign plans fully integrate operational and logistic capabilities. The influence of the combatant commander is essential in bridging any operations-logistic gap. The theater logistic concept should derive from the estimate of logistic supportability of one or more courses of action. It is the coordinated assessment by logistic planners in which the capabilities and resources of the combatant commander's components employed to provide supply, maintenance, transportation, health, and engineering services.

Logistics is the foundation of combat power. Combatant commanders exercise directive authority for logistics. This includes the authority to issue subordinate commanders directives (including peacetime measures) necessary to ensure the effective execution of approved operation plans. Directives also address the effectiveness and

economy of operation, the prevention or elimination of unnecessary facility duplication, overlapping of functions among the Service component commands, and the acceptance of operational risk of foregoing logistic implications. The logistic implications of a combatant commander's operation plan must be continuously updated and coordinated at all levels, through all phases of operation, and take into account prospective allies, coalition partners, and international organizations. (JP 4-0, page vii)

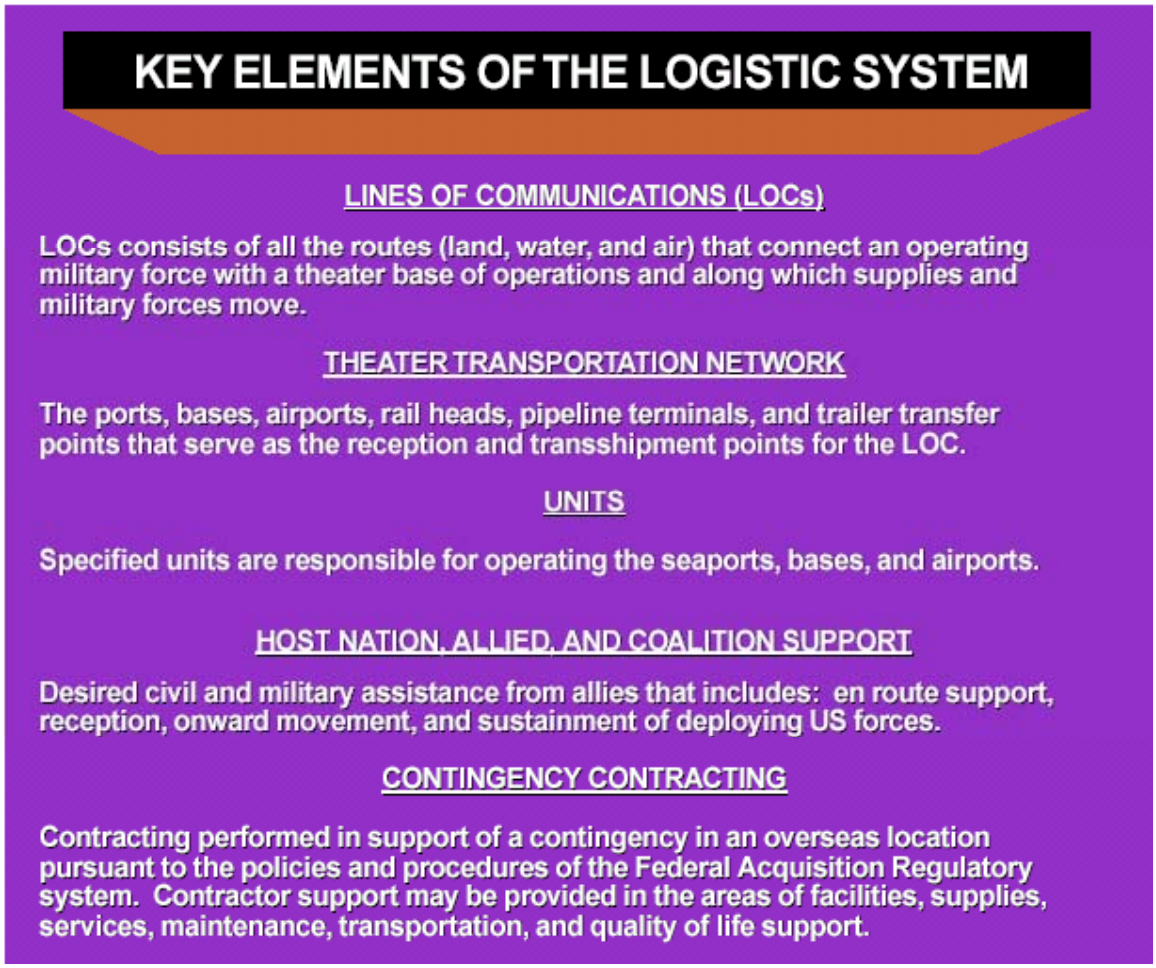
C. PROCUREMENT IMPLICATIONS ON THE LOGISTICS PLAN

Procurement and contracting can have a significant impact on the combatant commander's logistics plan and serve to minimize the logistics footprint in theater. The trend of world events suggests that U. S. forces will deploy, in joint operations, supporting contingencies in various types of theaters from fully matured to immature, without an established logistic support structure. For deployments to contested joint operations areas (JOAs), or where combat action is deemed likely, the combatant commander normally calls for maximum combat power in the initial phase. When possible, satisfying requirements for supplies and services by contracting may improve response time during the critical early stage of a deployment, and make airlift and sealift available for other priority needs. Contracting support can augment existing capabilities, provide expanded sources of supplies and services, bridge gaps in the deployed force structure, leverage assets, and reduce dependence on U. S. -based logistics.

Contracting may bridge gaps that may occur when sufficient organic support is not available in the operational area. Contracting is also valuable where no host-nation support (HNS) agreements exist, or where HNS agreements do not provide for the supplies and/or services required. The emerging trend is to use contractors to augment active military combat service support and assist them in meeting major theater war or other mission requirements that may arise simultaneously with the contingency operation.

Although Contingency contracting is often performed in support of an operation in an overseas location, the contracting process follows the policies and procedures outlined in the Federal Acquisition Regulatory System. Contingency contracting may be an effective force multiplier for deployed forces in providing supplies, services, and construction support to augment organic capabilities. Each Service component has the

capability to initiate contracts for needed support. However, the combatant commander may elect to employ the Joint Theater Logistics Management (JTLM) element or establish a contract-clearing house to ensure that Service components are not bidding against each other for the same commodity or service. (JP 4-0, page I-14)



Source: Joint Publication 4-0; Doctrine For Logistics Support of Joint Operations

Figure 6. Key Elements of the Logistics System

D. CONTINGENCY OPERATIONS

A contingency is the employment of military forces in response to a crisis caused by natural disaster, terrorists, subversives, or required military operations. Due to the uncertainty of the situation, contingencies require rapid planning, response, and development of special procedures to ensure the safety and readiness of personnel, installations, and equipment. Like crises, contingency operations can occur in the environments of peacetime, conflict, and war.

A contingency may be a unique, stand-alone event in response to a natural disaster or a man-made event or change in the direction (branch) of an evolving campaign or major operation. Within a campaign or major operation, a branch is a contingency plan for the deviation of operations from the planned line. It is a result of chance or uncertain events that are identified as crisis triggers. (FM 100-7, page 6-2)

In accordance with 10 U.S.C 101(a) (13) a "contingency" operation of the DoD may be:

a. Designated by the Secretary of Defense when members of the Armed Forces may become involved in military actions against an enemy of the United States, or

b. Declared by the President or the Congress when members of the uniformed forces are called on active duty [a reserve component mobilization] under Title 10, United States Code, or any provision of law during a declared war or national emergency.

The formal declaration of a contingency operation is very significant for the Contingency Contracting Officer (CCO). The declaration of a contingency triggers invocation of 10 U. S.C 2302(7), which raises the Simplified Acquisition Threshold (SAT) to $200,000 for "...any contract to be awarded and performed or purchase made, outside the United States in support of a contingency operation..." (CCSH Chapter 2, page 3)

Although there is no universal definition, contingency contracting can be defined as direct contracting support to tactical and operational forces engaged in the full spectrum of armed conflict and Military Operations Other Than War, both domestic and overseas. This definition is purposely broad enough to include four *types* of contingencies: Major Theater Wars, Smaller-Scale Contingencies, Military Operations Other Than War, and Domestic Disaster/Emergency Relief (these terms are defined later). The definition is also purposely exclusive of military training exercises, routine installation and base operations, and systems/inventory control point contracting, both CONUS and OCONUS. Each of these excluded types of contracting can, under certain conditions, be quite similar to "contingency contracting" as defined here. However, what each of the exclusions lack is the element of *immediate risk* to human life or significant national interests.

1. Types of Contingency Operations

In recent years, crisis situations worldwide have required the rapid deployment of personnel to support United States national interests. These contingencies, ranging from Major Theater War to Military Operations Other Than War (MOOTW), have involved military and other public, joint or allied elements. Contingencies require planning, rapid response, flexible procedures, and integration of efforts. The following is a list of contingencies contracting officers have had to support in recent years and will be supporting in years to come:

- **Major Theater War (MTW) (Formerly Major Regional Conflicts)**: These are conflicts where hostilities are ongoing, imminent or likely and where there is a substantial commitment of U. S. military forces. Operation Desert Shield and Operation Desert Storm are examples of Major Theater War. During these operations, contracting usually supplements robust Combat Support (CS) and Combat Service Support (CSS) infrastructures.

- **Small-Scale Contingencies (SSC, formerly Lesser Regional Conflicts)**: These are also conflicts involving ongoing, imminent or likely hostilities involving the U.S. military, but involve fewer forces, and usually a more restricted time schedule, as with Operation Just Cause (Panama). Contracting often supplements CS and CSS capabilities limited by location, strategic lift or manpower ceilings.

- **Military Operations Other Than War (MOOTW)**: Per Joint Publication 3-0, MOOTW encompass a wide range of activities where the military instrument of national power is used for purposes other than the large-scale combat operations usually associated with war. Although MOOTW are usually conducted outside the U.S., they also include military support to U.S. civil authorities. Joint Publication 3-0 lists the following categories of MOOTW: Arms Control, Combating Terrorism, Counter-drug Operations, Nation Assistance, Noncombatant Evacuation Operations, Civil Support Operations, Peace Operations, and Support to Insurgents. Operations Provide Comfort (Northern Iraq), Uphold Democracy (Haiti) and Joint Endeavor (Bosnia) are examples of the dozens of MOOTW conducted in recent years.

- **Domestic Disaster/Emergency Relief**: Technically a subset of MOOTW, a distinction is drawn for the purposes of this document. Domestic disaster/emergency relief operations can range from domestic natural and man-made disasters to civic disturbances to terrorist activity within the U. S.. DoD missions in the area of disaster relief include efforts to mitigate the results of natural or man-made disasters such as hurricanes, earthquakes, floods, oil spills, riots, and air, rail or highway accidents. Examples of Domestic Disaster/Emergency Relief are DoD support to Hurricanes Hugo, Andrew, and Marilyn.

- **Exercises**: Routine military exercises may feel anything but "routine" to the CCO supporting them. Anyone who has participated in a COBRA GOLD, BRIGHT STAR, TEAM SPIRIT, National Training Center rotation or similar types of exercises will attest there is a very definite sense of urgency and intense mission pressure connected with them. However, there is not the urgency, pressure or risk to life or national interests associated with the four major types of contingency contracting operations discussed in the paragraphs above. Moreover, they do not qualify as "declared contingencies" or as a major contingency type and generally receive no special consideration for other forms of relief discussed in this text. Within the military community we preach, "train as you fight"; but with respect to contracting, senior Executive Branch policy makers and the Congress have been reluctant to allow this application to exercises. CCOs must be fully cognizant of the distinction between what is contractually permitted in an actual contingency and what is permitted in an exercise, which prepares the forces to deal with such a contingencies.

2. Mature vs. Immature Contracting Environments

CCOs must consider the "maturity factor" in planning for contingency operations. They need to bring different contracting tools based on maturity and contingency phase. For example, a CCO would set up a contingency contracting support kit for an operation in Western Europe differently than for an operation in Somalia. Regardless of the nature or location of the contingency operation, CCOs are expected to comply with the spirit

and letter of existing laws and regulations to the fullest extent possible consistent with mission accomplishment.

The following definitions provide a useful, conceptual classification as to the area of operations a CCO will be supporting. (CCSH, page 5)

- Mature. A mature contracting environment is one characterized by: a sophisticated distribution system that can rapidly respond to changing requirements and priorities; sufficient vendors who can comply with FAR requirements in order to meet contingency contracting demands and have previous experience contracting with the U.S. government; and, in the best case, where there is an existing DoD contracting office or structure in place. Examples of mature contracting environments include Kuwait, Saudi Arabia, Korea, and Western Europe.
- Immature. An immature contracting environment is an area with little or no built-up infrastructure, few vendors and of the available vendors few, if any, have previous experience contracting with the U.S. Examples of immature contracting environments include Somalia, Haiti, and Rwanda.
- Semi-mature: A semi-mature environment possesses characteristics of the previously mentioned areas of operations. A distribution system exists but tends not to be extremely sophisticated. The area also has vendors, but they have little experience contracting with the U.S. government. In addition, the infrastructure may not be as robust as in a mature environment, but not as lacking as in an immature environment.

3. Contingency Contracting Support

The mission of contingency contracting is to responsively, effectively, and legally contract for the providing of the supplies, services, and construction necessary to support the mission of the supported organizations. (NCCH, page 1) Because it is an integral part of the overall process of providing logistics resources to deployed forces, the contingency contracting function shifts its focus to match the changing phases of the deployment. While no operation will follow a set temporal format as described below, a contingency as well as the associated procurement actions can generally be divided into four phases.

1) **Phase I: Mobilization/Initial Deployment**: This phase is normally the first 30-45 days of a deployment and is characterized by an extremely high tempo, confusion and controlled chaos. The CCO's number one priority is responsiveness to basic life support requirements, as they are providing contracting support for the arrival of the initial forces. These forces will require the following supplies and services for the initial bed-down: billeting, food service (including potable water), transportation and equipment rental, ground fuel, laundry and bath services, refuse and sanitation services, utilities, and interpreters and/or guides. Since the CCO must be prepared to award contracts immediately upon arrival at the deployment site, a CCO may be placed in the undesirable position of being the requester, approving official, certifying officer, and transportation office for deliveries. Detailed planning can preclude some of these "additional duties". However, physical limitations on the number of support personnel deployed in the early stages of a contingency requires a high degree of flexibility on the part of the CCO. In spite of the personnel limitations, the administrative functions must still be performed. CCOs should have access to sample "boiler-plate" statements of work, PIIN logs, forms, and several other administrative items, either pre-loaded on the CCO's laptop or via an Internet accessible database and in hard copy in the Contingency Contracting Support Kit. SF44s/cash payments and Blanket Purchase Agreements (BPAs) are the predominant contracting actions. CCOs use the Purchase Card Program, Imprest Funds/Third Party Drafts, and Purchase Orders at a level consistent with the maturity of the environment in which they will operate.

2) **Phase II: Build-Up**: This phase is characterized by a reception and bed-down of the main body of deploying forces. In this phase, additional contracting personnel generally arrive with their units, though not necessarily at a rate commensurate with the number of troops to be supported. The CCO's priorities during this phase continue to be responsiveness to life support requirements. Types of requirements during this stage would include the following:

*Construction material *Heavy equipment

*Horizontal construction *Office equipment/furniture

*Quality of life/MWR items

Attention must be given to gaining effective command and control over contracting and contracting personnel by establishing requisitioning, funding and contracting controls and procedures, to include Non-Appropriated Funds (NAF) contracting procedures to support quality of life programs (where applicable). Additionally establishing BPAs, consolidating requirements into purchase orders and contracts rather than using a high volume, and physically time consuming SF 44 cash transactions, establishing an Ordering Officer (OO) network with effective control measures and a vendor base will also aid in placing effective controls on the process. Effective tools to make this an efficient process are desperately needed by the CCO.

3) **Phase III: Sustainment**: This phase provides contracting support from the completion of the build-up phase until redeployment begins. The contracting activity expands into contracts for additional quality of life, more permanent facilities and equipment, additional office supplies, and discretionary services. The CCO's priorities during this phase are:

   a. Establishing long term contracts (IDIQ, additional BPAs) and consolidating requirements wherever possible to achieve economies of scale, reduce cost, and mitigate risk.

   b. Improving documentation of contracting actions and internal controls.

   c. Increasing competition and depth within the vendor base, to include offshore sourcing for items/services not available within the immediate area.

   d. Planning for transition to follow-on forces or termination and redeployment.

4) **Phase IV: Termination/Redeployment**: This phase will be characterized by significant pressure and urgency to either "send the troops home" or prepare forces for "forward deploying" into a new area due to completion of the mission in the current AOR. Life support contracts will continue until the last person has redeployed, though the quantities are supplied at a decreasing rate. Typical new requirements include: packing, crating, and freight services; construction and

operation of wash racks for vehicles; commercial air passenger services (if TRANSCOM is not providing this). The CCO is required to terminate and closeout existing contracts and orders. Ratifications and claims must be processed to completion. When a follow-on force is required, the CCO must prepare contracts and files for delegation/assignment to the incoming contracting agency (DCMA, UN, etc.). Contract reporting and file documentation must be current and accurate so the audit trail is easy to follow, leaving no loose ends on site for someone else to resolve or finalize. Consequently, after action reports are essential. Each CCO should keep a daily record, beginning with deployment, of any unique happenings that may help future CCOs.

With the exception of a natural disaster, hostilities could erupt during any phase of a contingency operation. The more rapidly the CCO "matures" the contracting operation, the better support they will be capable of providing when hostilities do occur. However, some problems are unavoidable. For instance, contractor employees may not report for work, abandon the job site or refuse to drive vehicles in certain areas. Vendors and shops may close during hours of darkness or completely. The threat of snipers, terrorists, and enemy action against the CCO while traveling in the local community may increase significantly. In light of these known risks, CCOs must deploy with the tools that offer the capabilities to quickly mature the contracting environment with a local vendor base or the ability to tap into a robust commercial or military logistics pipeline, which can connect the CCO to a vendor base outside the contingency area.

E. ORGANIZATIONAL STRUCTURE

This overview provides an example of guidance for a large OCONUS deployment; however, this structure will not apply to all situations. Smaller deployments should be tailored to fit mission requirements and may result in completely autonomous operations with "cradle-to-grave" contracting. (NAVSUP, page 3)

The deployed contracting organization includes the Head of Contracting Activity (HCA) or his/her appointed designee. All contracting offices within the contingency area of operation function under the under the contracting theater for procurement purposes. All deploying contracting officers and purchasing agents have their warrants and

appointment letters, respectively, issued by the HCA of the lead service component in the theater. Non-theater HCAs shall not appoint contracting officers for in-theater contracting and shall not award contracts for the in-theater services without theater HCA approval. (NAVSUP, page 3)

The Expeditionary Logistics Support Force (ELSF) immediately deploy contracting Forward Area Support Teams (FAST) consisting of contracting officers to the contingency site to perform initial purchasing. The size and number of teams are dependent on the contingency and operational requirements of the mission as determined by the theater HCA and ELSF. The support staff, contracting officers, contract administrators, contract specialists, procurement clerks, cost and price analysts, property administrators, and administrative personnel deploy with the main element to establish the main contracting organization in the theater. (NAVSUP, page 3)

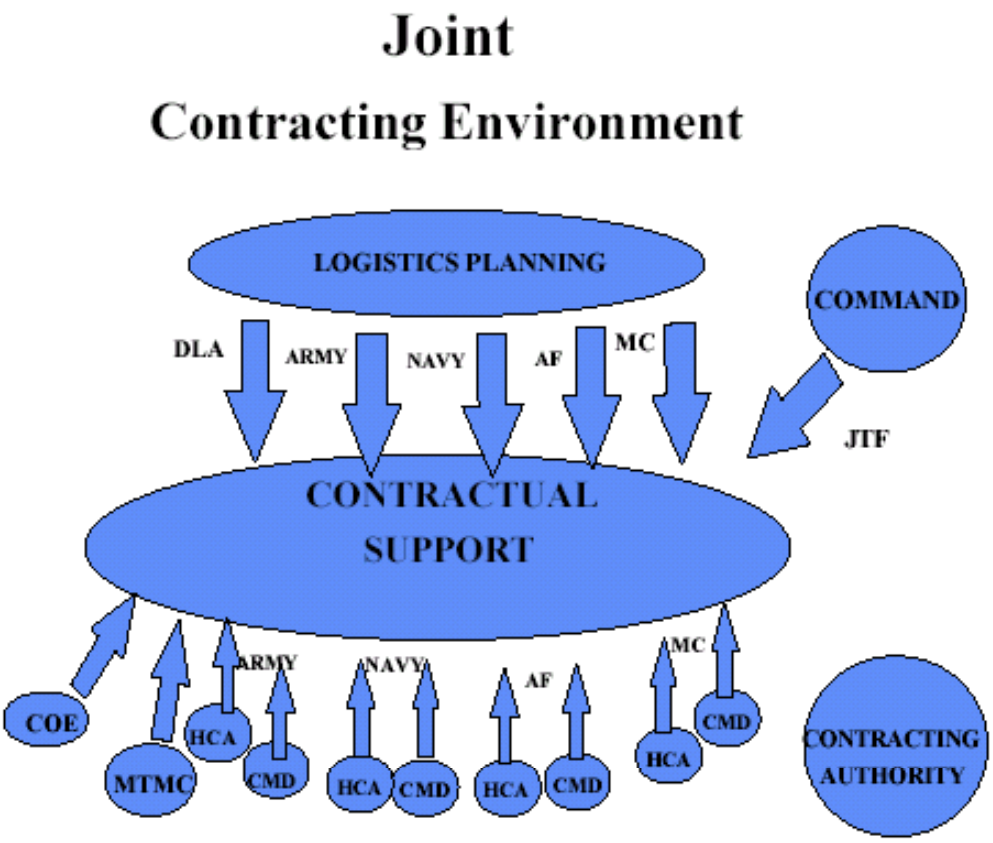
As the support staff arrives and becomes functional, the FAST is integrated under the theater concept and assist in establishing regional contracting offices as identified by the theater HCA. The regional contracting officer is in relative proximity to supported units and is responsible for order officers working in remote areas. As the contingency closes, the contracting function reverses the build-up process, whereby the regional contracting offices close out contracts and procurement actions turning functions over to the main contracting organization at the contracting headquarters. As needed, contracting officers and FASTs will be maintained to continue contracting requirements. As the main element redeploys, a team of contracting personnel remains in the area of operations until contracting requirements cease and ongoing procurement activity is closed out. (NAVSUP, page 3)

1. Joint Contracting Environment

A major problem arising out of non-integrated command and contractual chains is the proliferation of contracting activities and offices in a joint operation. Contracting Officers are hard to identify ahead of time, as most are deployable assets of higher-level support commands (e.g., U.S. Army Contracting Command, Europe; Army Materiel Command; and Defense Contract Management Command, International). A lead agency designation allows a major contracting command to task for Contracting Officer

augmentation from within the Army, Navy, Air Force and Marines. At present there is no doctrine on the use of lead agency during a contingency.

Given the operational tempo of all Services, any contracting assets become critical, closely managed and hard to get. Some activities could virtually ignore the efforts to consolidate contracting assets. This could cause some contracting elements, which had excess contracting capability, to stand by while other contracting elements that are critically short of contracting officers go without support. At times, these units could be collocated on the same camp or base. When deploying forces, all contracting assets should be coordinated and focused in order to prevent duplication of effort, achieve economies of scale, and avoid competition between services for scarce assets.



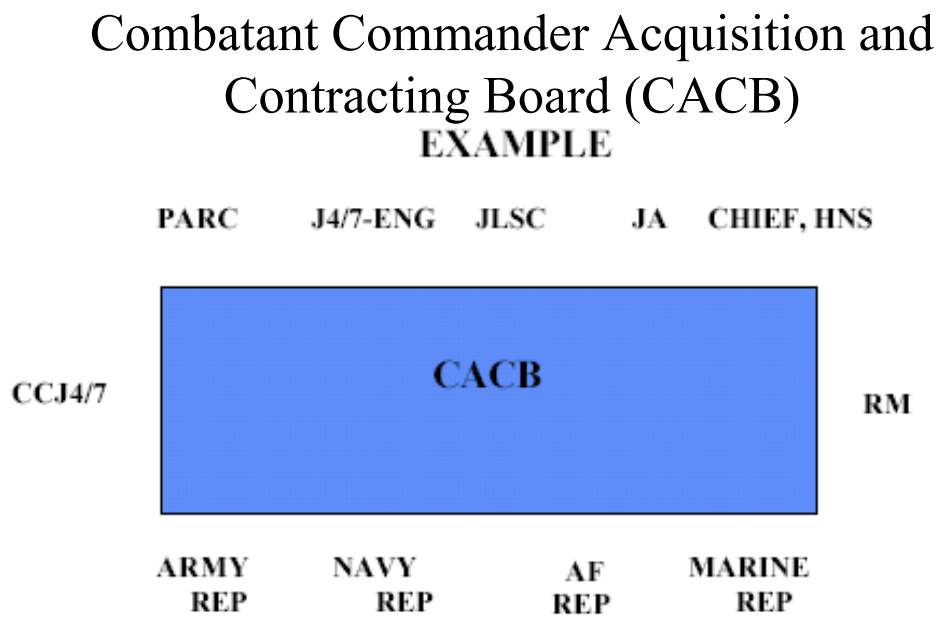
Source: Contingency Contracting Student Guide

Figure 7. Joint Contracting Environment

2. Combatant Commander Acquisition and Contracting Board (CACB)

Joint Publication 4-0 states that the combatant commander may form a CACB in support of a joint operation. (Note: He is not required to do so.) When utilized, the mission of the CACB is to coordinate and resolve contingency contracting and other acquisition matters within the theater. An effective CACB minimizes interservice competition for scarce local resources, reduces overlapping and redundancy of procurement functions within the force, and serves as the body to formulate, coordinate, and communicate the combatant commander's priorities for acquisition matters. The issue of the contracting statutory and reporting chain for an operation is certainly a major policy issue for the CACB. While each combatant commander does it a little differently, this board is typically chaired by the combatant commander's J-4 with membership from the J-4, Host Nation Support, Civil Affairs, Engineer, and contracting functions; each service participating in the operation is represented. Currently, U. S.PACOM has implemented the CACB as a permanent board that meets with regularity under all circumstances. This has greatly increased the cooperation and interoperability among the services in that theater.

In a contingency operation the primary purpose of the joint board is to coordinate local procurement and host nation efforts in support of the operation. The CACB is usually held outside the AOR of the contingency, at the combatant commander headquarters. Only if the combatant commander (and his staff) deploys will this board be held in-theater. The CACB concept can also be employed by the JTF to coordinate contracting efforts in the theater of operations. At the JTF level this board may be called the Joint Acquisition and Contracts Board (JACB), the Joint Acquisition Board (JAB) or, as in Operation Joint Endeavor, the board may be called the Joint Acquisition Review Board (JARB).



Source: Contingency Contracting Student Guide

Figure 8. CACB Example

3. Examples of Organizational Structures in Various Operating Environments

Due to the situation in differing environments, various logistics structures can be employed. The following provides a few examples of recent contingency operations.

a. Contingency Contracting in Kosovo—Operation Task Force Hawk

In April 1999, while an Early Entry Contracting Team (EECT) (similar to a FAST) from the U. S. Army Contracting Command Europe (USACCE) deployed to Albania with Task Force Hawk, USACCE was already finalizing plans to send another EECT to Kosovo to support Task Force Falcon. The second team's mission was to provide critical local contracting support to U.S. troops in the early stages of a permissive to non-permissive Kosovo entry. The EECT traveled with the civil affairs team to perform the initial recon of the area, which took three days. Traveling with the civil affairs team proved useful from both the contracting and informational exchange perspectives.

Based on the information from the recon, the contracting team deployed forward six days later to establish a Joint Contracting Center (JCC), which coincides with a theater logistics concept of operation. Despite numerous challenges, the JCC was able to provide immediate support.

One major challenge was lack of communication. For several weeks, the JCC was unable to link into the tactical communications network because of a continuing wire shortage. Once a link was established within days the lines were cut. These line-cutting occurrences continued over a two-month period. Communications significantly improved in early August when four Iridium satellite phones arrived from the United States. For the first time, the JCC was able to communicate with vendors throughout the U. S. and Europe.

In addition to the lack of communication, at the start of the deployment, the region lacked a local vendor base. The JCC quickly educated local businessmen on U.S. business practices. Most purchases in the first weeks were made at vendor locations using SF-44, Purchase Order Invoice Voucher. These early purchases gave an immediate boost to the local economy.

Under austere conditions and with poor communications, initial Kosovo contracting operations proved extremely challenging. The JCCs provided critical support early in the deployment. This improved working conditions and communications, allowing the JCCs to greatly expand the local vendor base and provide improved support to Task Force Falcon. Soldiers deployed to Kosovo could appreciate a higher level of mission and life support due to the continuing JCC efforts. (Phillips, 2001)

b. Contingency Contracting in Haiti—Operation Uphold Democracy

Jean-Bertrand Aristide was elected President of Haiti in December 1990 in the country's first open and fair election. A populist priest whose followers came mostly from the poor communities of Haiti, Aristide experienced difficulties in governing from the beginning—in part because he did not control the legislative branch of his government and in part because he was resisted by elements of the status quo. Street violence broke out shortly after Aristide was elected.

On September 30, 1991, after only seven months in office, Aristide's government was over-thrown by officers of the Haitian army and Aristide was flown into exile. The repression perpetrated by Haitian soldiers against their own people increased dramatically following the military coup. Murders, abductions, tortures, and politically motivated arrests were common. This systematic violence and abuse of human rights caused a massive exodus of Haitian refugees. Henceforth, U.S. and international policy was focused on restoring the elected civilian government in Haiti.

On July 31, 1994 the United Nations adopted Resolution 940 authorizing member states to use all necessary means to facilitate the departure of Haiti's military leadership and restore constitutional rule and Aristide's presidency. In the weeks that followed, the United States took the lead in forming a multinational force (MNF) to carry out the UN's mandate by means of a military intervention. In Operation Uphold Democracy the U.S. objectives were to encourage democratic institutions and reduce the flow of illegal immigrants into the United States. In preparation for this contingency, DoD simultaneously planned for an invasion and for the peaceful entry of forces into Haiti, and eventually attempted to execute portions of both scenarios. Due to successful last minute negotiations led by former President Jimmy Carter, the MNF was able to deploy peacefully. The last minute change caused confusion in the deployment of forces.

The United States began conducting Operation Uphold Democracy in September 1994, assisting President Aristide in re-establishing a legitimate government in Haiti and helping create a secure environment for the people of Haiti. The Operation consisted of a peaceful entry into Haiti of more than 20,000 U.S. service men and women and over 5,000 non-U.S. forces from twenty-four countries. On March 31, 1995 the United States turned the peacekeeping operation over to UNMIH.

The Corps Acquisition structure arrived in Port-au-Prince Haiti on 21 September. Due to the austere immature environment of Haiti due to the lack of political stability and embargos, the contracting organization had to mature its structure quickly to support the servicemen and women arriving in country. Within forty-eight hours of deployment, a CJTF contracting section was established consisting of procurement personnel from the 10th Mountain division, the 7th Transportation Group, MTMC, and the

Navy as well as CJTF Finance personnel. Within seventy-two hours, a combatant commander acquisition and contracting board (CACB) was formed to coordinate procurement support for the CJTF. The CACB consisted of the board chief, the senior deployed contracting officer from each Service, an estate/real property team chief, a Finance Officer, a contract law attorney and the CJTF J-4.

In spite of the appearance of joint operations, a lack of coordination existed. Various services did not recognize the warrants of other services. Additionally CCOs deployed with PIINs from their parent contracting commands. When they returned home, they took those contract files with them to document the use of the PIINs. If they left before completion of the contract or before the contract could be closed out, the remaining personnel had no documentation by which to measure performance, make payment, or close out the action. Despite the difficulties faced by the CACB, within days 170 contracts were awarded valued at $2.2 Million, providing supplies and non-personal services to nearly twenty-five thousand deployed personnel.

F. U.S. CONTRACTING CONSIDERATIONS IN MULTINATIONAL OPERATIONS

Throughout history, military operations have been conducted with armed forces of several nations in pursuit of common objectives. The changing world environment dictates that future operations will most likely require multinational involvement.

An operation conducted by forces of two or more nations is termed a multinational operation. An operation conducted by forces of two or more nations in a formal arrangement is called an alliance operation. An operation where the military action is temporary or informal is called a coalition operation. Campaigns and major operations may be conducted within the context of an alliance, coalition, or other international arrangement. Such operations, whether or not they involve combat, are planned through both international and U.S. channels. In practice, each coalition operation is unique. Planning and conduct of the operations vary with the international situation and the composition of the forces. Alliance or coalition members may not have identical strategic perspectives, but there should be sufficient harmony of interests to

ensure a common purpose for the campaign. The need to maintain consensus within the alliance or coalition is paramount to preserve a unified effort.

Multinational operations require close cooperation among all forces. Capabilities will often differ substantially among national forces, but higher considerations of national prestige will often be as important to the final success as the contributions to the overall effort. Seemingly small decisions, such as national composition of the main effort, may have significant consequences for the outcome of the operation. Members should be consulted on their recommendations for COA development, ROE, and assignment of missions.

To assure unity of effort, all plans require detailed coordination with essential supporting plans for liaison and the provision of mutual support. Host nation support and the capabilities of coalition partners in particular may dictate the tempo of the attack and its form. The commander must focus on lateral coordination across national and interagency boundaries, and in particular the effective sharing of information. Though unity of command promotes unified effort, American commanders should be prepared to operate within the alliance or coalition under command of other than a senior U. S. commander. (FM 100-7, page 1-12)

1. General

During the planning phase of a multinational operation, U. S. planners must address several issues relating to contracting operations, contractors, and contractor personnel. These issues should be addressed in such documents as the Status of Forces Agreements (SOFAs), Technical Arrangements (TAs), and in both multinational and national Operational Plans (OPLANs). The issues include:

a. Assignment of an in-theater Head of Contracting Activity for all U. S. forces participating in the operation.

b. The status of U.S. citizens, civilian contractors in the country, and protection of contractor personnel.

c. Use of third-country subcontractors or personnel.

d. Limitations on the physical presence of contractors; that is, boundaries within which contractors are to operate.

e. Payment of customs duties by contractors when entering the country.

f. Payment of corporate or individual taxes.

g. Payment by contractors of taxes on goods bought in the operational area.

h. Environmental matters to be addressed, including transportation and disposal criteria and locations for hazardous waste and scrap. (JP 4-08, page D-1)

2. Principles of Contingency Contracting

The Multi National Force Commander (MNFC) establishes rules, policies and procedures applicable to contracting activities in the operational area. However, contracting by U. S. forces participating in a Multi National Force (MNF) is subject to the same laws and regulations that apply to contracting generally, including the requirement for fair and open competition. Therefore, it is important that the rules, policies and procedures developed by the MNFC be consistent with U. S. contracting laws and regulations. Appropriate personnel, including contracting officers and staff legal counsel, should assist the MNFC in developing the MNF contracting rules, policies and procedures. Such rules may, for example, take into consideration that simplified acquisitions (contracts up to $200,000 for non-personal services, supplies or constructions during contingency operations) are not subject to the laws requiring full and open competition (10 U. S.C 2304). Other exceptions to the "full and open" competition rules applicable to contingency operations include limited source purchases, compelling urgency, based on international agreements, national security, and public interest (can only be invoked by head of the agency).

The contracting rules established by the MNFC are designed to ensure that the MNFC's logistic priorities are fully supported. A Multinational Acquisition and Contracting Board (MACB) may be established to develop and promulgate procurement policies and priorities on behalf of the MNFC, in conjunction with the Theater Allied Contracting Office (TACO), if a Multi-National Joint Logistics Center (MJLC) is established. The senior U. S. procurement official will coordinate with the civil-military

operations staff officers of both the U. S. Joint Task Force (JTF) and the MNF to assure that the staff officers understand the total requirements being levied on the host nation through contracting and through requests for HNS. To the extent allowed by law, U.S. policy in some operations may be to award contracts to local suppliers in order to support the local economy and contribute to "nation building." Obtaining contract administration services either from the host nation or another allied and/or coalition nation may aid U.S. political and military objectives in some operations. (JP 4-08, page D-2)

3. Execution of Multinational Contracting Operations

Contracting operations in multinational operations require a detailed understanding of customer requirements. Because of the diverse and unique needs of the various nations, these requirements are much more complex than for U. S. joint operations. Knowledge of these requirements helps assure customer satisfaction and assures that the basis for reimbursement is accurate and complete.

There must be a clear understanding of the standards of performance required of the contractor. Achieving such understanding can be a complex undertaking given the varied cultures and languages that U.S. commanders may encounter. Because of political ramifications, defining clear performance standards is especially relevant when arranging contractor support from an MNF partner or a host nation.

The senior U.S. procurement official in-theater coordinates with the MNF MACB and TACO (if established) to assure that the U. S. benefits from any leveraging available from consolidating requirements for multiple nations. Leveraging possibilities may be developed by the TACO and the Joint Logistics Coordination Center (JLCC), or by the contracting officer on the staff of the MNFC. Leveraging probably will be particularly effective in common user logistics (CUL) areas, such as fuel procurement and distribution, construction materials, transportation, staging areas, and lodging. A U.S. warranted contracting officer should be attached to the TACO or staff element at the MNF HQ to take full advantage of available leveraging possibilities.

Contracting officers during multinational operations use U. S. contracting law and procedures. The techniques will include purchasing locally and using basic ordering

agreements (BOAs) to leverage consolidated requirements and to simplify the procurement process. BOAs are particularly useful when procuring theater-wide supplies and services, such as office supplies, food, vehicle maintenance, and construction materiel. (JP 4-08, page D-3)

G. CONTRACTING OFFICER AUTHORITY

1. Waivers and Deviations

In a contingency environment, there are several waivers, deviations and delegations that may be available to the CCO. This allows the CCO more latitude to conduct successful contracting operations. For example, the statutory requirement for full and open competition is relaxed when it can be defined that the contingency need is unusual and compelling or is for an international agreement. Additionally, it is not necessary to post oral solicitations or synopsize when the contingency is outside the United States. Furthermore, the Simplified Acquisition Threshold (SAT) has been raised to $200,000 for contingencies overseas. This increased spending authority provides the CCO more flexibility to meet customer requirements. Further increasing flexibility, CCOs are also allowed to award letter contracts and other undefinitized contractual actions when involved in contingency operations. For example, if a delay in the contracting process has the potential to be detrimental to the Government, then the CCO is authorized to make oral solicitations. This enables the CCO to obtain requirements expeditiously, while still maintaining positive control over the contracting operation. Finally, contractual actions overseas are not required to follow U.S. socio-economic laws and regulations. However, CCOs should verify that there are no international agreements or treaties that require the U.S. to abide by similar host nation laws.

The waived requirements, delegations and deviations are to help the CCO, so that they can meet urgent requirements in a contingency environment. But as any other contracting officer, the CCO must practice and enforce contractual actions and possess sound judgment. The purpose of these waivers, delegations and deviations is to help the CCO when he faces unusual circumstances that are unique to a contingency operation. Despite the flexibility provided to the CCO, the FAR still applies. Additional FAR exceptions are listed in Table 1.

REFERENCE	SUBJECT	EXCEPTIONS ALLOWED
5.202(a)(2)	Synopsis	Not applicable for purchases conducted using simplified acquisition procedures, if unusual and compelling urgency exists.
5.202(a)(3)	Synopsis	International agreement, treaty or organization specifies the source of supply. For contracts by written direction of foreign governments reimbursing cost of acquisition.
5.202(a)(12)	Synopsis	Does not apply overseas if subject to the Trade Agreements Act or North American Free Trade Agreement (see Subpart 25.4).
6.001(a)	Competition Requirements	Do not apply to contracts using Simplified Acquisition Procedures in FAR Part 13.
13.111(b)	Covenant against contingent fees	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
13.111(c)	Restrictions on subcontractor sales to the government	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
13.111(d)	Anti-Kickback Procedures	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
13.111(e)	Audits and Records-Negotiations	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
13.111(f)	Contract and Work Hours Safety Standards Act	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
13.111(g)	Drug Free Workplace Certification	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
13.111(h)	Estimate of Recovered Materials	Not applicable to contracts or subcontracts at or below the simplified acquisition threshold.
25.102(a)(1)	Buy American Act	Not applicable for items purchased outside the U. S. and its territories
25.302(b)	International Balance of Payment Programs	Acceptable to buy foreign at or below the simplified acquisition threshold.
25.501	Payment in Local Currency	Contracts entered into and performed outside the U. S. with local foreign firms will be priced and paid in local currency unless international agreement provides for payment in U.S. dollars or contracting officer determines local currency to be inappropriate.

25.703 (a) and FAR Supplement	Restrictions on Certain Foreign Purchases	Authorized to buy items restricted under 25.702 (a) in unusual situations for use outside U. S., its possession or Puerto Rico.
28.102-1(a)	Bonds	Miller Act 40 U.S.C. 270a-f, can be waived by the contracting officer for overseas construction

Table 1. FAR Exceptions (Source: AFARS, pages 6-7)

Table 2 provides additional AFARS/DFARS/NAPS exceptions.

REFERENCE	SUBJECT	EXCEPTIONS ALLOWED
5137.104-90 and DFAR 237-104 (b)(i)(B)(2)	Personal Services	Pursuant to 5 U.S.C. 3109, if considered advantageous to National Defense. Requires D&F.
5101.602-3(b)(3) and 5201.602-3	Ratifications	Can be delegated to others by the HCA
5101.603-1-90 and 5201.603	Contracting Authority of Other Personnel	Imprest Fund Purchases IAW FAR/DFAR 13.4. Fuel, oil, and emergency repairs IAW AR 703-1. SF 44 and purchase card purchases IAW FAR 13.505 and AFARS 13.90 provided that the individual has been trained and has a written authorization.

Table 2. AFARS/DFARS/NAPS Exceptions (Source: After AFARS, pages 8 and NAVSUP 23)

Note: Contracting officers should review these exceptions to fully understand their application and use. Although deviations and exceptions to regulatory and statutory procedures cannot be practiced during field exercises, contingency contracting concepts can be applied to field conditions. There are urgency exceptions that apply during deployment. Remember that commanders and their logistics officers, not procurement personnel, drive requirements.

2. Extraordinary Relief (FAR Part 50).

FAR Part 50 prescribes policies and procedures for entering into, amending, or modifying contracts in order to facilitate the national defense under the extraordinary emergency authority granted by Public Law 85-804 (50 U.S.C. 1431-1434) and Executive Order 10789, dated November 14, 1958. The Act empowers the President to authorize agencies exercising functions in connection with the national defense to enter

into, amend, and modify contracts, without regard to other provisions of law related to making, performing, amending, or modifying contracts, whenever the President considers that such action would facilitate the national defense. Extraordinary Relief is a law designed to provide the authority necessary to meet various contingencies. As such, CCOs should be notified before deployments exactly what, if anything, has been authorized before using this authority.

A question often raised is, "Which statutory requirements can we count on being waived during actual contingencies?" A complete reading of the Defense Resources Act sheds little light as to the specific laws that may be waived. However, two excerpts from the act reveal how far-reaching and all-encompassing potential waivers could be:

> *Sec. 401. The President may authorize any agency of the Government exercising functions in connection with the national defense to enter into contracts and into amendments or modifications of contracts heretofore or hereafter made and to make advance, progress or other payments thereon, without regard to the provisions of law relating to the making, performance, amendment, or modification of contracts whenever he deems such action would facilitate the performance of the national defense functions of such agency; except that this title does not authorize the use of the cost-plus-a-percentage-of-cost system of contracting or any contract provision in violation of law relating to limitation of profits.*
>
> *Sec. 1214. Except as provided in this Act, all laws and parts of laws in conflict with the provisions of this Act are hereby suspended to the extent of such conflict for the period during which this Act shall be in force.*

These sections make it appear CCOs will have unlimited authority to write contracts any way they see fit. However, a word of caution should be noted on three points. First, implementing legislation of the Act could change or modify this language. Second, the Act may not be invoked for certain contingencies. Finally, CCOs are still required to adhere to sound contracting principles to the extent possible and contracting records are subject to audit. Moreover, the Act spells out specific penalties for negligent abuse of broad authorities granted during emergencies. The bottom line is CCOs will be given the authority to get the job accomplished, but they must thoroughly document reasons for not following normal procedures.

FAR Part 50 and DFARS Part 250 implement 29 U. S.C 1431 and Executive Order (EO) 10789 concerning granting of extraordinary contractual relief to facilitate the national defense. The statute and EO require that such actions at or above $50,000 must be approved at or above the level of an Assistant Secretary or his deputy. DoD has implemented this through the use of Contract Adjustment Boards headed by such an official. The high level of approval for actions at or above $50,000 removes any practical utility of this authority for the CCO. However, authority to approve extraordinary relief actions below $50,000 is not limited by statute or EO. The DFARS limits exercise of this authority to the HCA - depending on the nature of the contingency and the contracting command and control structure this official may be within "reach" for a CCO. Further, DoD has authority to waive DFARS 250.201 limitations (which delegate this authority no lower than the HCA) on either a one-time or class basis. Such a waiver could provide Extraordinary Relief authority of less than $50,000 to the CCO level.

A review of these emergency authorities may lead one to conclude adequate authority exists within current regulations and laws to be able to provide expedited contracting support with few problems. Indeed, many legal and regulatory requirements, which slow down the acquisition process in peacetime, are not applicable to emergency contracting in a foreign country. Supply, service, and construction requirements under the SAT, which will likely constitute over 95% of the requirements, can be consummated quickly.

There are several pitfalls and legal shortcomings, which CCOs should be aware of so they can be dealt with properly. First of all, care must be taken on how to apply this potential "relief" to peacetime exercises. Ideally, services should practice in peacetime the way they plan on operating in war. However, using some of these exceptions in peacetime could subject the CCO to criticism for overstepping legal boundaries. Secondly, these exceptions deal mainly with administrative aspects of contracting—not the actual written contract itself, nor the enforcement of it. For instance, what does the CCO do if a contractor refuses to sign or otherwise accept a written purchase order or contract and demands cash instead? Lastly, there are several statutory and regulatory problems that are unaffected by any existing relief. For example, all contracts over the

SAT require many clauses which most vendors find objectionable—Examination of Records, Disputes, and the Changes clause just to name a few. Again the question, what is to be done if the only source for a requirement refuses to accept a contract with mandatory clauses, which are objectionable or insulting? While actions may have been initiated to obtain necessary class deviations and legislative relief, CCOs must be prepared to support our deployed forces within the confines of existing laws and regulations. (CON 234, page 2-12)

H. WORLD WIDE EXPRESS (WWX)

1. Background

For more than half a century, the United States Air Mobility Command (AMC), and its predecessor organizations, Military Airlift Command, Military Air Transport Service, and Troop Carrier Command, has had primary responsibility for high-priority air transportation shipments in support of the DoD and forward deployed organizations. AMC's mission is to "Provide airlift, air refueling, special air mission, and aero medical evacuation for U.S. forces." (USTRANSCOM Handbook 24-2, 2000). However, AMC's airlift support capability is decreasing due to conflicting demands and changes in the aircraft fleet. The first Gulf War revealed that the modern strategic airlift capability to support the military wartime airlift requirements was a finite source and have led to the necessity to augment air transportation service support to OCONUS activities because of decreased military budget and personnel, rapidly shrinking overall airlift fleet, the limited number of replacement aircraft, and increasing level of small package cargo requirements not requiring oversize or heavy lift capabilities. To answer this new requirement, USTRANSCOM and its air component command, AMC developed the World Wide Express (WWX) designed to provide an alternative commercial airlift service for small package shipments.

As the contracting component for airlift services, AMC entered a partnership with commercial carriers such as United Parcel Service (UPS), Federal Express (FedEx), and Dalsey, Hillblom and Lynn (DHL) Worldwide Express to contract for the Federal Government an international small package delivery service known as the WWX program in October 1, 1998, (WWX Contract, June 1998). In essence, the contract

provides air transportation services by Civil Reserve Air Fleet (CRAF) carriers to provide customer time-definite delivery, door-to-door delivery, and a myriad of other services for high-priority DoD documents and packages not including unclassified and non-hazardous material. Despite being a commercial service acquisition, WWX is designed to meet the critical needs of the DoD war fighter. Preliminary analysis estimates an annual savings of $50 million with equal or better service.

Under the terms of the contract, the Government user may select whichever WWX carrier provides international service to a geographical region or various regions of service as shown in Table 3. UPS delivers to the Central region, FedEx to the Pacific, European, Central, and Southern regions, and DHL to the delivered Pacific and European regions. In essence, the WWX program provides an express delivery service for global movement of high priority documents/packages, excluding hazardous material or sensitive materials.

The WWX program is a mandatory-use contract for all Federal government agencies and DoD. The contract was established to handle letters and packages up to and including 150 pounds, as well as shipments consisting of multiple packages that may surpass a total weight of 150 pounds (Headquarters AMC, WWX Contract F11626-98-D-0030-32, 1998). All three commercial carriers provide premium service with door-to-door pick-up and delivery and real time visibility that is accessible through the Global Transportation Network (GTN) and the World Wide Web, which is maintained by USTRANSCOM. The GTN is an automated command and control information system designed to integrate passenger, cargo, supply, and unit requirements and movements with airlift, in-flight refueling, and military sealift schedules (AMC 1999, p. 4-20). The government user can access the GTN for In-Transit Visibility of package movement and arrival time.

WORLDWIDE EXPRESS REGIONS

Southern Theater		European Theater			Central Theater			Pacific Theater	
Region A	Region B	Region C	Region D	Region E	Region F	Region G		Region H	Region I
Antigua & Barbuda	Argentina	Austria	Albania	Azerbaijan	Cyprus	Angola	Madagascar	Cambodia	American Samoa
Aruba	Belize	Belgium	Armenia	Belarus	Egypt	Bangladesh	Malawi	China	Australia
Bahamas	Bolivia	Denmark	Bosnia-Herzegovina	Georgia	India	Benin	Mali Republic	Laos	Brunei
Barbados	Brazil	Finland	Bulgaria	Kazakstan	Israel	Botswana	Mauritania	Myanmar	Fiji
Bermuda	Chile	France	Croatia	Kyrgyzstan	Jordan	Burkina Faso	Mauritius	Nepal	Indonesia
Dominican Republic	Columbia	Gibraltar	Czech Republics	Russia	Lebanon	Burundi	Morocco	Singapore	Malaysia
Grenada	Costa Rica	Greece	Estonia	Tajikistan	Oman	Cameroon	Mozambique	Taiwan	Marshall Islands
Haiti	Ecuador	Ireland	Hungary	Turkmenistan	Pakistan	Cape Verde	Namibia	Thailand	Micronesia
Jamaica	El Salvador	Liechtenstein	Iceland	Ukraine	Qatar	Chad	Niger	Vietnam	New Zealand
Martinique	Guatemala	Luxembourg	Latvia	Uzbekistan	Sri Lanka	Congo, Dem Rep of	Nigeria		Palau, Rep of
Mexico	Guyana	Monaco	Lithuania		Syria	Djibouti	Rwanda		Papa New Guinea
Netherland Antilles	Honduras	Netherlands	Macedonia		Turkey	Equatorial Guinea	Senegal		Philippines
St. Lucia	Nicaragua	Norway	Malta		U.A.E.	Eritrea	Seychelles		Saipan
Trinidad/Tobago	Panama	Portugal	Moldova		Yemen	Ethiopia	Sierra Leone		
U. S. Virgin Islands	Paraguay	Sweden	Poland			Gabon	South Africa		
	Peru	Switzerland	Romania			The Gambia	Swaziland		
	Suriname		Serbia-Montenegro			Ghana	Tanzania		
	Uruguay		Slovakia			Guinea	Togo		
	Venezuela		Slovenia			Guinea-Bissau	Tunisia		
						Ivory Coast	Uganda		
						Kenya	Zambia		
						Lesotho	Zimbabwe		

High Volume Routes	
Bahrain	
Kuwait	
Saudi Arabia	
	United Kingdom
Germany	
Italy	Republic of Korea
Guam	
Spain	
Japan	Canada

High Volume Retrograde Routes
Germany
Japan
Republic of Korea

Table 3. World Wide Express Regions (From the WWX Webpage, October 2003)

In case of a national emergency, the WWX program also has a special war clause stipulation ensuring final delivery of package shipments to their destination without being returned to the government shipper. The war clause stipulation and the guaranteed shipping insurance for aircraft loss or damage offer an added value security and service to the government user.

Presently, AMC continues to offer airlift service that includes small packages. However, a decision has been made to not replace the decreasing organic fleet of C-141 and vintage C-5 fleet with expensive C-17s on a one-for-one basis. Instead the C-17s would be purchased in adequate numbers sufficient enough to support contingency requirements for its unique mission parameters to handle oversized and overweight airlift cargo requirements but lacking in capability to support routine general cargo missions. In an era of decreasing operating budgets and limited asset capability, the current trend suggests that AMC will significantly minimize small package delivery altogether and focus mainly on movement of heavy cargo shipments instead.

2. WWX – Next Generation Contract (WWX-2)

The WWX program that provides international premium express delivery for small packages is now well established and fully implemented. On August 28, 2001, the FY02 WWX-2 Next Generation Contract awarded DHL, FedEx, and UPS a one-year award with two option renewal years to provide "Worldwide International Commercial Express Service" for the Department of Defense and certain civilian agencies. The service includes time-definite, door-to-door pick and delivery, transportation, in-transit visibility (ITV), Power Track capability, and customs processing and clearances of non-hazardous materials and small packages weighting not more than 150 pounds. Moreover, the express service is limited to movement of only high transportation priority cargo requiring time definite delivery. These commercial contractors include, but are not limited to, Third Party Logistics (3PL) Contractors, Integrated Logistics Management Contractors (Prime Vendor, etc.), and Cost Reimbursable Contractors (CRCs) (WWX Webpage, 2003).

Under the new WWX-2 program, all awarded carrier routes are now available to all DoD shippers without any lane or theater restrictions to any location worldwide. The current two-percent (2%) administrative service charge (ASC) is included in all fees for service to the government transporter in which WWX carriers can forward the ASC charge to the government. The ASC was established to cover the administrative costs for the management of the WWX program.

Although hazardous material packages remain excluded as a regular feature of WWX contract, the new service allows the government shippers to transport hazardous material if the WWX carrier allows it to become part of its normal commercial service. Carriers will impose the normal WWX rates with an additional "accessorial fee" payable to the carrier.

The WWX-2 program also provides country-specific customs clearance for duty free shipments and expedites shipment deliveries through different countries as stipulated in The Defense Transportation Regulation (DTR) Part V Foreign Customs guidance and information under the Department of Defense Customs and Boarder Clearance Policies and Procedures. Cooperation of both the government shipper and the contractor is required. The government shipper remains responsible for compliance with customs clearance requirements as stipulated in the DTR Part V, and proper completion of all applicable customs documentation. WWX carriers determine customs clearance provisions, handle customs clearance for all government shipments transported, all countries serviced, and serve as the agent for performance of customs clearance.

The WWX-2 carrier reported metrics is another program feature that measures contractual compliance versus actual calendar day deliveries. All DoD Services and Federal Agencies can use the metrics displayed on the web page to reference the shipments on time and shipments with authorized delays. It is imperative to note that many shipments reported in the "authorized delay" section were actually delivered on time. WWX commercial carrier systems automatically default any processing delay, re-routing, paperwork correction, and so forth into the authorized delay section. However, the majority of these problem delays are rectified immediately on the spot with the shipment delivered within the time line detailed in the contract.

The WWX-2 program takes advantage of the best commercial shipping service available today. WWX-2 remains a viable distribution option for the military's small parcel shipments and will become visibly important as support from AMC continues to decrease.

3. Areas of Concern

The design for employment of WWX is to deliver shipments originating from CONUS to OCONUS, limited to fixed location shore infrastructure destinations. Commercial carriers are unable to provide direct door-to-door delivery to forward deployed organizations afloat (e.g., ships and squadrons) causing a complex and unique set of challenges for the Navy such as increased workload for in-theater workforce.

These issues prompted some afloat customers to question the cost effectiveness of WWX compared with AMC rates as the increased workload shouldered by ashore Navy personnel may offset any slight cost advantage and response timesavings. According to Pierre Kirk, NAVTRANS' Air Transportation Policy Officer for the U.S. Navy, comprehensive testing is currently ongoing with additional afloat and mobile units in both the Pacific and Mediterranean regions in conjunction with respective fleet and TYCOM staffs to provide solutions to these critical challenges. In the future, the plan is to extend the WWX program to afloat and mobile units deployed in various contingency locations upon resolving issues involving current customs entry and in-theater manpower impacts.

During a recent joint evolution, NAVTRANS and Command Logistics Group Western Pacific (Singapore) tested a WWX small parcel shipment routing directly into designated Australian ports where U.S. Navy vessels made established port call visits. In the past, only high priority requisitions were allowed shipment directly to the husbanding agent stationed in Sydney who in turn rerouted the package to the final destination where American vessels conducted their routine port call visits. This is an unprecedented attempt by the Navy of small parcel shipment utilization of a husbanding agent as a WWX destination. The process also required the institution of DoD Activity Address Code listing of all husbanding agents' addresses for continued direct use. As a result, DoD users can now send WWX small parcel shipments directly to the husbanding agent

stationed at the nearby port where the American vessels are docked resulting in lower cost and decreased shipping time. More important, the successful increased volume of parcels transported results in added value support to deployed forces by allowing faster and efficient receipt of cargo while still deployed in the Western Pacific Theater of operations. (Kirk, 2002)

NAVTRANS' Pierre Kirk also stated that commercial carriers have continuously met contract delivery requirements for shipments to OCONUS Navy shore activities in terms of reliability and timeliness and have not reported one single loss of package to date with an average of 10 to 12 reportable delays out of 600,000 shipments delivered annually. The WWX program continues to be cost competitive with AMC rates concerning small package deliveries and, at times, can provide a slight cost advantage.

The WWX program provides government shippers another viable transportation alternative to AMC channels for small parcel delivery in selected regions and under certain scenarios. WWX was not implemented to replace AMC services, some of which are specifically unique to AMC capabilities, but instead, designed to assist the shipper deliver materials to the final destination with a time-definite delivery guarantee. WWX remains to be a valuable tool in the government shipper's toolbox.

4. WWX Commercial Carriers

a. FedEx Express

The origin of Federal Express began in 1965 in Yale University when an undergraduate student named Frederick W. Smith wrote a critical essay concerning the economic inadequacies of the passenger route systems used by most airfreight shippers. In essence, Smith believed that combining passenger air traffic with freight air traffic was not the most efficient way of conducting business. The essay also criticized the airfreight industry's lack of growth, inefficient distribution systems, and unrealistic system design to accommodate increasing demand for time-sensitive shipment. One of the most significant selling points was Smith's idea for a revolutionary air cargo service delivery within one to two days, a service that he guaranteed. Smith's vision involved a centrally located cargo distribution system focusing mainly on serving both large and small cities.

Founded in August 1971, Smith bought a controlling interest in Arkansas Aviation Sales and officially began operations on April 17, 1973, with 14 small jets delivering less than 7500 pounds of cargo per flight to twenty-five cities from Rochester, New York, to Miami, Florida. Smith built a single hub in Memphis, Tennessee, to serve as a transfer point for all packages delivered throughout the country. Memphis International Airport was also selected for its geographical center to nearby market cities for small package deliveries, excellent weather flying conditions, and the airport's willingness to make adequate improvements in additional hangar space availability and operational requirements.

Smith named the company Federal Express during an unsuccessful attempt to obtain a contract with the Federal Reserve Bank as its service provider. As its first major customer, the contract would have involved the movement of a large amount of checks around the United States daily. Despite the failure to get the contract with the Federal Reserve Bank, Federal Express eventually became the premier carrier of high-priority overnight delivery in the market.

Information management has become one of FedEx's core business assets. FedEx created a new business model that focuses on the capability to complement physical and electronic transactions, to transport assets under time-definite requirements, and provides excellent information control that is transparent to employees and customers alike. For the next decade, FedEx is currently in pursuit of a few major goals as an information company. One such goal involves FedEx's desire to provide "e-care" which would allow its customers to provide their end customers with excellent service. With FedEx's systems currently in place, customers (such as DoD and Federal agencies) should be able to provide their end users with customized products on a JIT basis, while maintaining minimal inventory. Consequently, FedEx wants to develop global information systems available for use by its customers. These systems will be integrated with the customers' systems so that customers will be unable to determine where their systems end and FedEx's systems begin. FedEx must meet customers on their own terms, for example, by tracking shipments by customer order numbers. The company also intends to develop an "information super hub" which will allow FedEx to warehouse

the information it collects in an intelligent manner and utilize that information to predict industry trends and to provide its customers with useful intelligence.

With annual revenues of $23 billion, FedEx is the premier global provider of transportation, e-commerce and supply chain management services and has the world's largest air cargo fleet involving 643 various aircraft serving 366 airports worldwide, along with a ground fleet of 43,500 trucks and vans. FedEx is the largest express transportation company, handling more than 3.3 million documents, packages and freight daily, and employs more than 138,000 employees in 215 countries. Last year, FedEx ranked highest in the J. D. Power and Associates 2002 Small Package Delivery Service Business Customer Satisfaction Study in the categories of air, ground, and international delivery services (FedEx Web page, 2003).

As a WWX carrier, FedEx became the first express carrier to provide data to the military's GTN system. This enabled the war fighter to track critical parts within the FedEx system using GTN and compliments the capability of tracking FedEx packages over the Internet. Data provided to GTN involves over 8,000 account numbers identified as shippers of materials for all the military services. As shown in Figure 9, FedEx's U.S. Government Tracking webpage provides DoD users all the necessary tools and resources required for government shipping via FedEx delivery service such as delivery tracking through the use of Transportation Control Number (TCN).

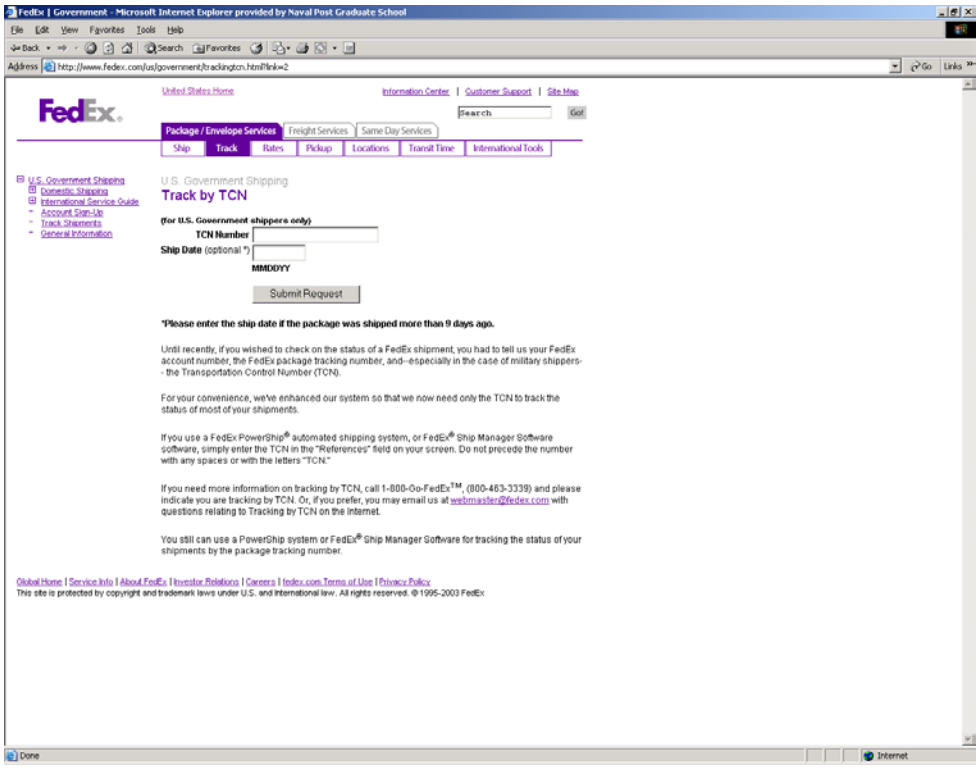


Figure 9. Federal Express Package Tracking Webpage (From the FedEx Tracking Website)

b. DHL Worldwide Express

Founded in 1969, Adrian Dalsey, Larry Hillblom and Robert Lynn (D, H, and L) created DHL Worldwide Express with the innovative concept of providing door-to-door express service for bills of lading between San Francisco and Honolulu. The express service involved sending out documentation in advance of cargo arriving using ocean shipments, thereby allowing the merchandise to clear through ports faster. The company grew rapidly as service expanded to the Philippines, Japan, Hong Kong, Singapore and Australia. Steady expansion continued in the 1970's as DHL extending the door-to-door express service to Europe, Latin America, the Middle East, and Africa.

DHL's extensive domestic and international parcel express service coverage support involves more than 5,000 offices, of which over two-thirds are owned and operated by DHL, far greater than any other company in the air express business. This key advantage is significant in comparison to other carriers involved in global package movement who utilize more third party agents in the foreign countries they serve. Most important, DHL is also a licensed customs broker in over 140 countries

resulting in faster transit times, streamlined customs clearance, effective tracking of shipments, and simplified billing process.

DHL maintains its position as the world's leading international air express network with service to 120,000 destinations in over 220 countries and territories. The company operates a global system of 118 hubs and 238 gateways, and maintains an aircraft fleet of over 250 airplanes operating for or on behalf of DHL and a ground fleet of more than 60,000 motorized vehicles. The firm has a worldwide team of over 150,000 employees supporting DHL's global network that handles an annual average turnover of $5.1 billion and delivers 160 million shipments. In 1999, DHL celebrated its 30th anniversary by capturing an approximate 40% market share of international express traffic – more than FedEx, UPS, and Airborne combined. DHL and the United States Postal Service announced an alliance for the air express delivery to deliver Priority Mail Guaranteed Service to more than 200 countries from more than 20,000 U.S. Post Offices.

In April 2003, Deutsche Post World Net acquired DHL and initiated a merger with two other major Deutsche Post Companies, Danzas and Euro Express, into a repositioned DHL brand offering the world's broadest range of express delivery and logistics products, from courier and express services to heavy tonnage forwarding and tailor made IT-supported logistics solutions. The merger provided an additional road-based service through an extensive and reliable European road network for both business and private customers.

In May 2003, DHL commenced operations in Iraq following the lifting of economic sanctions by the UN Security Council and became the first express and logistics company to enter the country. DHL offers both air cargo express delivery through DHL Express, and heavy freight and logistics through its DHL Danzas Air and Ocean division. DHL promises to play a major role in assisting the local and international communities and U.S. military efforts to rebuild the country's infrastructure and economy and improve the transportation of humanitarian aid. Most important, DHL's air express service operations would facilitate the critical transportation service required to support the war fighter by commencing operations soon after the lifting of the sanctions.

Services include up to six daily flights from Bahrain to Baghdad with approximately over 100 flights per month being flown. Trucking services to and within Iraq, with 40-foot trucks are flown daily from the Middle East through Kuwait to service the southern part of Iraq such as Basra, Talil and Umm Qasr. Moreover, DHL assigned a Baghdad-based cargo aircraft to operate exclusively within the Iraqi territory and provided services from Baghdad to Kirkuk, Mosul, Talil, and back to Baghdad three times a week. (The service has been temporarily suspended due to the damaged a DHL plane recently sustained from a shoulder fired Surface-to-Air missile.) DHL Danzas Air and Ocean also established five different hubs in Iraq's neighboring countries to be used as interstations. Relief and humanitarian traffic will transit through the hubs in Kuwait, Jordan, Syria, Lebanon and Turkey, depending on the origins of the goods. Jordan will remain as the sole gateway for commercial cargo.

In August 2003, DHL acquired Airborne, Inc.'s ground operations for $1.05 billion to increase competition to the U.S. express delivery marketplace. DHL plans to work diligently to integrate operations over the next 12 to 36 months. For the time being, DHL and Airborne shipments will move through their respective operations network. Apart from DHL uniformed couriers picking up and delivering Airborne packages in certain locations, little has changed for the Airborne customers, and they will continue to maintain the company contacts they have had in the past. Inevitably, all services, products, and guarantees will be integrated after conducting a thorough review of all of the company's locations to determine how best to serve its customers. As shown in Figure 10, shippers can continue to monitor packages through the use of Waybill tracking numbers in the Government Package Tracking web page section of each respective DHL and Airborne websites with no immediate changes in this regard.

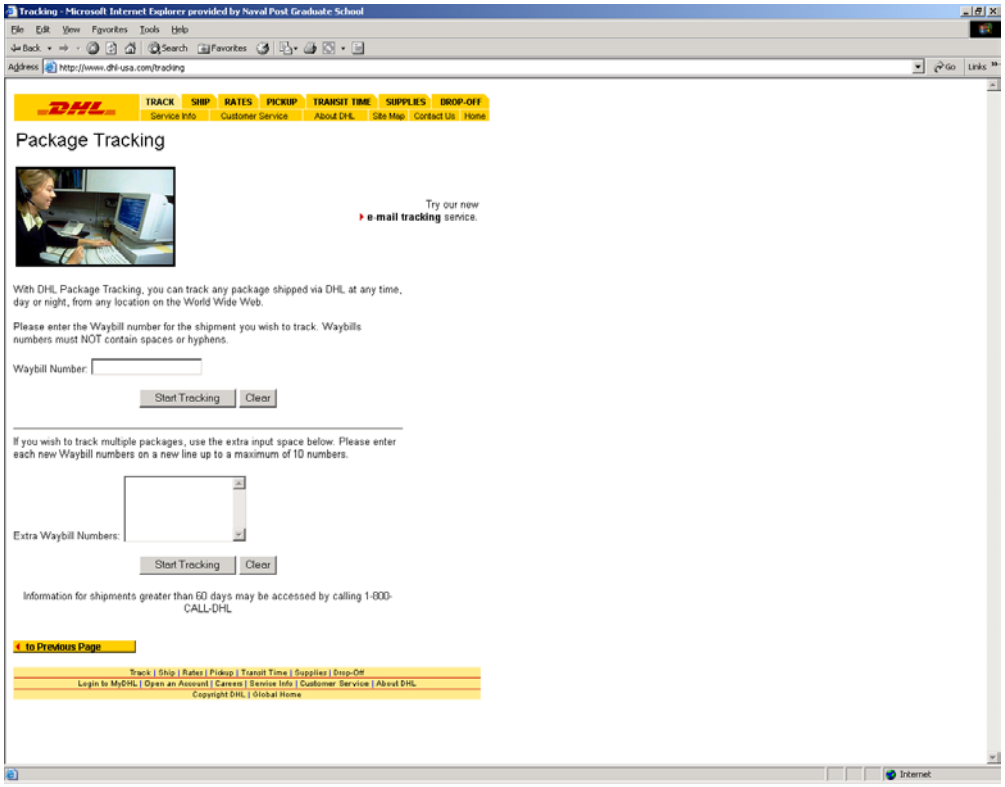


Figure 10. DHL Package Tracking Web Page (From the DHL Tracking Website)

c. United Parcel Service

United Postal Service (UPS), one of FedEx's main competitors, also maintains a large presence in both the airfreight and airmail market. The origins of UPS go back as early as 1907 when a young entrepreneur named James E. Casey borrowed $100 from a friend and created the American Messenger in Seattle, Washington. The company began as a bicycle-based delivery service to meet an increasing need for private messenger and delivery services; six years before the creation of the United States Parcel Post system. During its first service expansion in 1919 to Oakland, California, the company changed its name to United Parcel Service. The word "United" was chosen to serve as reminder for being part of the same company, "Parcel" represented the company's line of business, and "Service" identified the service the company offered. Casey also selected the color brown to represent a symbol of style and first-class travel at the time. The brown color also was less likely to show dirt.

UPS operated a short-lived air service starting in 1929 and was discontinued due to the 1939 stock market crash and a failing economy after only eight

months. However, the company began sustained air cargo operations to major East and West coast cities offering two-day delivery service via its UPS Blue Label Air (now UPS 2nd Day Air) in 1953. UPS Blue Label Air flourished and continued until by 1978 the service became available in every part of the country, including Hawaii and Alaska. In the 1950's, UPS began the process of expanding its delivery services by acquiring "common carrier" rights for the entire country.

Expansion into new territories, increasing demand for air package delivery, and subsequent federal deregulation of the airline industry in the 1980s led to new business opportunities for UPS. Despite moderate success in 1975 with its international delivery services in Canada and additional operations in Germany a year later, the 1980s signaled UPS' entry into the international shipping market by quickly establishing a presence in an increasing number of countries and territories in the Americas, Eastern and Western, Europe, the Middle East, Africa, and the Pacific Rim. Consequently, UPS began investing in its own fleet of aircraft and began offering overnight air delivery services by 1988. Overnight air delivery service became available in all fifty states, including Puerto Rico. UPS also began international air service between the United States and six European nations.

With the rapid growth of Internet and information technology, non-package operations make up the fastest-growing business component at UPS. These operations include supply chain management, logistics services, and development of e-commerce services. Subsidiary UPS Logistics provides supply chain re-engineering and transportation management, and UPS has launched e-Ventures to develop businesses that will expand the company's role in e-commerce.

As its capabilities continue to grow, UPS is now the world's largest package delivery company that offers an extensive range of supply chain and logistics services. Headquartered in Atlanta, Georgia, UPS has 1,748 operating facilities with an all-cargo fleet involving 265 various aircraft and a ground delivery fleet of 88,000 motorized vehicles to serve some 1.8 million shipping customers. The company employs more than 360,000 personnel (320,000 U.S.; 40,000 International) and transports more than 3 billion parcels and documents per year (13 million per business day) throughout

the United States and to more than 200 countries and territories. UPS earned $31.3 billion in fiscal year 2002. The company dominates the U.S. in ground delivery of parcels and is steadily gaining on U.S. leader FedEx in air-delivery market share (UPS Web page, 2003).

In comparison to the other two WWX carriers, UPS website also offers a U.S. Government Shipping area, as shown in Figure 11, providing all DoD shippers all the necessary resources required for government shipping such as real-time Internet tools to assist customers to track goods through UPS tracking numbers.

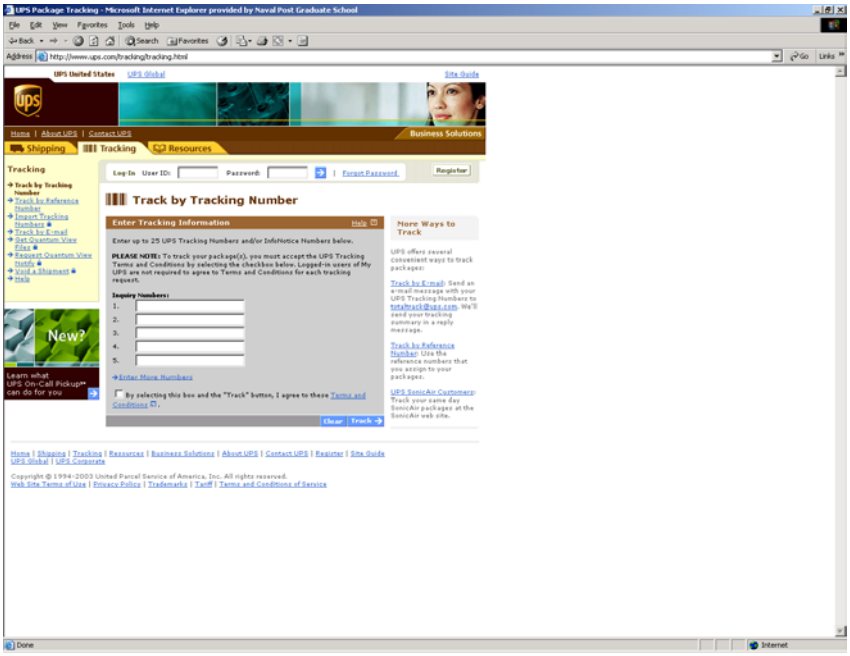


Figure 11. UPS Package Tracking Web Page (From the UPS Tracking Website)

5. Industry Trends for Small Parcel Service

Current industry trend points towards rapid growth of demand for freight transportation. Over the past ten years, freight ton-miles have grown another 23 percent closely trailing the growth in the U.S. economy. Although the huge increases in truck and rail freight together accounted for most of this growth, the aviation industry grew by more than 70 percent. While it remains a very small part of freight transportation by tonnage, aviation accounts for about 30 percent of the value of U.S. merchandise trades, and this share will certainly increase.

This projected growth in freight transportation also introduces a daunting challenge in the form of infrastructure modernization and forecasted workforce shortages. E-commerce and increasing economic globalization indicates a higher transportation demand. Just-in-time inventory systems are likely to transport even more inventory out of warehouses and into the transportation system, requiring both system capacity and greater reliability. Furthermore, our country's economic production (GDP) is likely to grow by 84 percent by 2005. Given all these factors, the freight transportation industry anticipates to grow to just over 5 billion ton-miles by 2025 as illustrated in Table 4.

Forecasts Past and Future	1975 Actual	1990 Coleman forecast	1990 Actual	2000 Estimated	2025 Forecast[13]
Transportation Context					
Population (millions)[1]	215	247	249	275	338
GNP (constant 1975 $, billions)[2]	$1,598	$2,830	$2,409	$3,049	$5,486
GNP Per Capita (1975 $)[2]	$7,417	$11,457	$9,675	$11,087	$16,240
GDP (constant 2000 $, billions)[3]	NA	NA	NA	$9,942	$18,258
Passenger Transportation					
Passenger-Miles (billions)[4]	2,560	3,850	3,946	5,036	8,438
Passenger-Miles Per Capita[4]	11,881	15,600	15,847	18,313	24,979
Licensed Drivers (millions)[5]	130	161	167	190	243
Vehicles (millions)[6]	138	170	193	219	262
Freight Transportation[7]					
Total Ton-Miles (millions)	2,285,000	4,394,706	3,196,000	3,959,432	5,098,888
Rail*	754,252	1,845,777	1,033,969	1,416,446	1,484,802
Water (domestic ton-miles)	565,984	1,010,782	833,544	763,540	NA
Water (domestic and foreign tons)	1,695	NA	2,164	2,453	3,429
Truck (intercity	454,000	703,153	735,000	1,130,132	2,121,837
Air	3,470	8,789	9,064	15,904	33,925
Pipeline	507,000	834,994	584,000	633,410	797,950

Table 4. National Transportation Statistics Report Past and Future Forecasts (From the Bureau of National Statistics Website, 2002)

Despite the optimistic growth projections, industry trends also point towards further shifts in how freight is moved and management of freight transportation. First, largely integrated freight transportation providers that offer full logistics/transportation services using multiple modes will focus in large volume of smaller shipments to meet low or non-inventory production and distribution requirements and express package delivery. Second, there will be increased growth in trucking resulting in improved point-of-sale, just-in-time inventory systems. Third, sustained air cargo growth is anticipated due to e-commerce and economic globalization. Larger wide-body aircraft will carry cargo in both dedicated freighters and passenger airlines.

Since the air cargo industry is a major element of the transportation infrastructure of the country, it continues to have a dramatic impact on the DoD. Not only has transportation played a vital role in our nation's economic development, but also our future will continue to rely upon an efficient and integrated transportation network. In an era of shrinking budgets, limited assets, and a lean military fighting force and infrastructure, the market for air cargo service will continue to expand and attract more businesses to keep up with growing demands from both the commercial and the DoD sector. Recent industry trends leading to higher demand in small parcel service are influenced by growing DoD requirement, economic globalization, technological improvements, and business practice modernization.

a. Growing DoD Requirement

The DoD depends almost exclusively on the commercial transportation industry to meet defense transportation requirements within CONUS. The DoD transportation policy states, "commercial transportation will be employed by the military departments for the movement of persons and things between points within the United States when such service is available or readily obtainable and satisfactorily capable of meeting requirements." Hence, the availability of a diverse, efficient transportation industry is crucial to national security in which the DoD annually spends over $8 billion for transportation services. Today, there is a growing need by the DoD for the commercial transportation industry to meet defense transportation requirements to

support the operating forces of the U.S. Army, Navy, Air Force, and Marine Corps, outside the continental United States.

Current logistics systems that support our operating forces are responsive and robust. Nevertheless, serious considerations must be recognized when command units are operating remotely from our standard operating supply points or established visit locations. During wartime contingencies, the DoD must account for extra consideration to the capability of the support site to sufficiently enlarge their infrastructure to support the material build-up that will be required in the theater of operations. Unit commanders will have to closely evaluate this ability in order to match the throughput requirements and the number of supply assets available with their concept of operations and operating plans.

Military logisticians must fully consider the total capabilities and limitations of the available transportation network when placing material requirements on the physical commercial distribution system. Recognizing that each tactical operation is different due to location and maturity of the theater, the availability of the WWX commercial shippers enables the unit commander or other government transporters to choose between the options to optimize operational flexibility for long term and sustained military operations. Force sustainment is the force multiplier that enables deployed units to remain on station or quickly move from theater to theater without capability degradation.

In a U.S. Navy ship, Material Control Officers and Supply Officers are responsible with expediting and tracking ordered parts to and from battle group ships as well as screening battle group ships for urgently required material. Once a ship or squadron sustain a “casualty” resulting in the requirement of a replacement part, it is critically important for supply officers to locate that urgently required material in order to maintain command operational capability and mission readiness. Upon finding the replacement part, in some cases, the use of WWX small parcel shipment may be the quickest method of delivery for replacement part acquisition. Of course, an alternative to WWX is to transport the material through the Defense Transportation System shipment channels. Under normal conditions, DTS could provide the fastest delivery method to get

the critical replacement part if there are prior arrangements made to expedite military parts without going through customs. However, this case is normally geographically limited due to fewer DTS endpoints than WWX endpoints. Thus, Supply Officers and Material Control Officers can track the ordered part based on the location of the end-user and location of the final shipping destination. By having the WWX commercial shipping option readily available to the war fighter, this additional capability to transport items facilitates not only the material in the casualty reporting system, but also benefits the Just-In-Time delivery process that strives to eliminate warehousing and double handling costs.

Current trends point toward the increased use of WWX by command units. According to a 1991 survey conducted on Pacific and Atlantic Fleet Aviation Type Commanders Deputy Force Supply Officers deployed on aircraft carriers, 82 percent of the respondents rated WWX as outstanding and excellent regarding its capability to meet delivery schedules. Similarly, overall confidence level concerning whether ordered material will arrive when expected by using WWX services received a majority rating of both outstanding and excellent with each scoring 46 percent of the participant's responses. More important, 77 percent of the participants chose the WWX transportation method if given the choice in comparison to AMC (received 15 percent) and other transportation methods (received 8%). Overall, WWX was clearly the preferred method of transportation with high confidence levels for service performance standards and expectations. Survey participants also rated In-Transit Visibility (ITV) for WWX through the use of the Internet significantly increased reliability for status information as compared to GTN and AMC information. Despite the survey not fully representing the entire DoD user population, it certainly provides a clear indication of customer confidence and preference for WWX (Grandjean, 2001).

b. Economic Globalization

Advances in communication and transportation technologies have been major drivers enabling rapid growth in globalization and economic integration worldwide. Decreased transportation costs and higher levels of service and speed have contributed to widely dispersed production and distribution facilities managed by large international firms. The trend toward globalization is also highlighted by the increase leisure and business-related air travel.

The integration of manufacturing facilities around the globe has been associated in many countries with the growing divestment of national firms from government ownership. Increased practice of liberalized free trade and reduced protectionism by these integrated and interdependent national economies are contributing to the rapid growth in air cargo delivery with the Intra-Asia region becoming the largest true airfreight market. In fact, despite having the recent Asian economic crisis airfreight traffic grew at approximately six percent per year. Asia air cargo traffic indicates strong growth with the largest Asian airports reporting 20-25% gains in 2002 over the much weaker 2001 level. According to the Aviation and Aerospace Almanac 2002, as China's economy grew by 7.8% in the first half of 2002, air cargo grew by 14%. Moreover, the rapid growth in international trade has increased trip length, which is closely associated with lower traffics per mile. As regulatory liberalization spurs price competition, lower tariffs further stimulate air cargo demand causing airlines to focus on lowering unit costs.

As an example, facing increased competition and falling real yields in which revenue per ton-mile averages a 2.5% decline, largely integrated express carriers such as FedEx and UPS are continuously expanding to international markets as shown in Figure 12. Today, express package shipping giant FedEx has been expanding rapidly in the small package delivery business historically dominated by UPS. Package shipping giant FedEx has been expanding rapidly in the small package-delivery business historically dominated by UPS. FedEx saw a 10.8% increase in daily package deliveries in its second quarter and expects ground package volume growth to approach 20% in the third quarter ended Feb. 28. Both FedEx and UPS put in place a 3.5% ground rate hike in January, a month earlier than in recent previous years. Volumes for FedEx are also

expected to climb as a result of the increased volume it carries for the U.S. Postal Service.

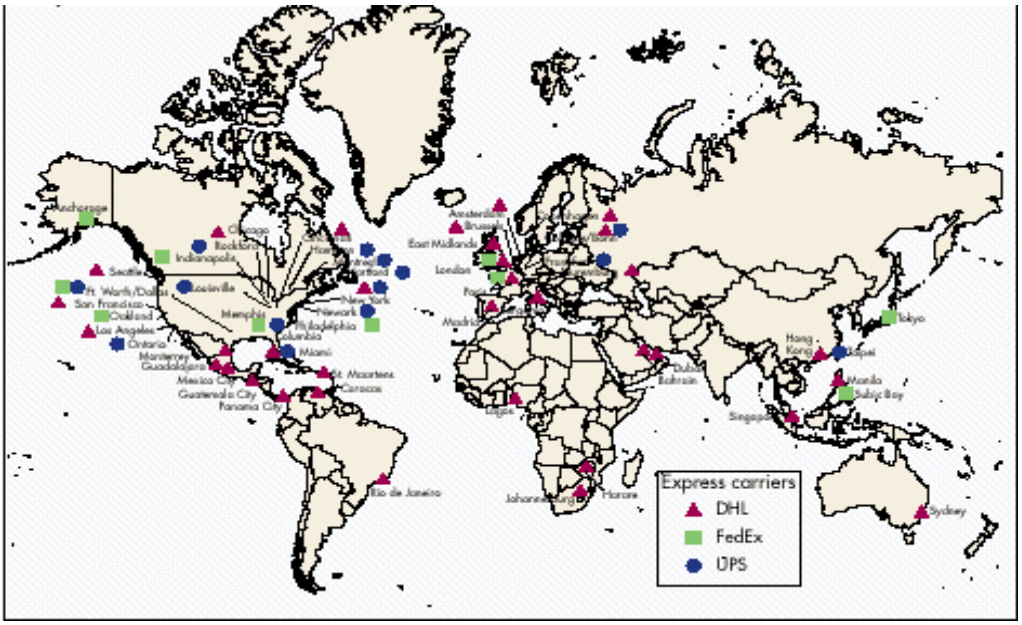


Figure 12. WWX Express Carriers Hubs (From the WWX Webpage, October 2003)

Despite the U.S. economic slowdown and the 9/11 terrorist attacks, an important driver influencing higher air cargo demand involves the sustained overall economic growth particularly in the imports and exports sector of world trade. Historically, there has been a steady increase of 2 to 2.5 percent in world trade with each 1% increase in total Gross Domestic Product (GDP). Airfreight trade has been growing even faster due to regional differences in economic growth resulting in an average of 7 to 10% annual growth in world airfreight traffic since 1993.

In the next twenty-five years, globalization will gain more momentum as advanced information technologies and financial markets link nations. This trend has significant implications for global transportation, bringing efficiency and competitive marketing to the forefront as criteria of operating decisions. Deregulation and privatization have amplified the pressure on airlines and ocean shippers either to merge or to conclude marketing alliances across national boundaries. Continued advances in computerized reservations, container shipping technology, and on-demand airfreight have

put a competitive premium on seamless integration of logistic services. Future commercial carriers may have major operations in all modes and all regions of the world.

c. Technological Innovation

Technology has played a critical role in enabling change. Today, we have reached an era where firms direct their resources toward finding solutions to problems through technological innovations and enhanced efficiency. Future use of Global Positioning System (GPS) technology, Intelligent Transportation Systems (ITS), and a continuous trend to imbed all applicable technological advancements in transportation systems operations and management will inevitably have a dramatic impact in the rapid growth for air cargo service.

During the past quarter century, the aviation system has moved to satellite-based communications, navigation, and surveillance systems. GPS technology has provided major advances in positioning accuracy for maritime shipping, railroads, and highway vehicles as well. The accurate characteristics of GPS in real-time navigation and tracking are heavily influencing the development of several advanced systems across all modes of transportation. In about twenty years, GPS technologies will spread through all modes of transportation.

Advancements in ITS currently are being widely deployed to improve the mobility and safety of our surface transportation systems. Technological innovations such as ramp meters, electronic surveillance, and signal synchronization and pre-emption, advanced weather and road condition information, computer-aided dispatch systems, commercial vehicle technologies, and a list of infrastructure and vehicle innovations promise to reduce congestion, improve efficiency, and make travel safer.

The current trend of integrating new technologies into the operations and management of the transportation systems will continue over the next twenty-five years. Today, the management of transportation systems is becoming increasingly automated and real-time. Although congestion remains a challenge, advances in communication technologies enable increased telecommuting options. Technological advances allow for the real-time pricing of transportation facilities to increase efficiency and reduce

congestion delays. Information technology plays a major role both in shaping future transportation demands and in enabling advanced management and operations of transportation services in an era of constrained development of physical infrastructure.

d. Business Practice Modernization

Changes in the way goods and services are produced and distributed in our economy, such as globalization, customized mass production, lean inventory management, rapid customer response, and growth in e-commerce, among others, are pushing commercial shippers to take advantage of technological transportation service modernization with such features as differentiated time-definite service options, inter-modal service, ITV and data integration with the management systems of customers. Significant investments in information technology enabled package carriers to provide to customers the ability to track a package's movement from origin to destination. Other advances included combining logistics, freight and financial services with traditional package delivery in order to offer customers full supply chain management solutions.

Lean inventory strategies are pushing vertically integrated air cargo operators like FedEx and UPS for reduced order-cycle times through various business models, Just-In-Time delivery, and "Make to Order" business practices. The focus of the business practice is now less inventory stock on hand to avoid production shutdowns and retail stock outs. As a result, increased demand for airfreight will continue to shorten delivery times to customers.

Many firms are shifting from the traditional 'push' systems where production decisions are based on forecasts to 'push/pull' systems where the assembly of finished goods is based on actual customer demand with parts and raw materials inventory replenished based on forecasts. The move to 'push/pull' systems is indicative that more firms are shipping products directly to customers, thus bypassing traditional supply chains. With more direct-to-consumer-business, many firms need to adjust their transportation mode away from bulk shipments toward 'parcel' shipments, creating an increase in demand for small package delivery as more consumers shop on the Internet.

Replacement parts providers are also taking advantage of the value-added services from small package carriers. Chicago-based parts supplier W.W. Grainger prides itself on its same-day delivery, which Grainger officials say is needed to compete in the replacement parts market. Grainger has a close relationship with UPS for both inbound and outbound shipments and last year began a $200 million redesign of its shipping network to locate its inventory closer to its customers, using nine strategically located distribution centers. Grainger took into account where the closest UPS hubs were located when selecting the location of their distribution centers. Grainger also took its sales and customer history data and processed it through a UPS software system to estimate the next-day delivery capabilities from the new distribution centers to its existing customers. Having parts suppliers ship to nine Grainger distribution centers expedites rush shipments and gets them closer to customers faster.

Similarly, UPS reports increased interest in some of its existing value-added services, as shippers try to get more out of the dollars they spend with carriers. Not long ago, many small or medium-sized shippers may not have considered that online technologies were applicable to their businesses, but those same shippers are rethinking that decision in today's economy. For example, UPS says its WorldShip software is increasingly gaining interest from parts suppliers for its ability to print out bar code labels for outgoing shipments. It also sends a proactive e-mail notification to the receiver notifying them the package has been shipped. This service greatly reduces the number of incoming calls to the shipper requesting information about a package.

Recently, UPS hosted a tour of the massive 'Hub 2000' construction project, a 4-million square-foot facility designed to handle the sorting of 300,000 packages per hour. The estimated cost for Hub 2000 is $1 billion, making it the largest UPS construction project to date; engineers at UPS used a computer simulation to determine the optimal layout and design of the facility. In conjunction with small package delivery, UPS has also entered into other business activities such as service parts logistics. UPS has transformed itself from a package delivery service into a technology-based business that moves goods, provides information and arranges the transfer of funds for delivered goods. This transformation has served to strengthen the relationship

between UPS and its customers. With a dedicated work force, UPS has positioned itself to meet the anticipated increase in demand for small package shipments resulting from the increase in Internet-based retailers (UPS Web page, 2003).

I. COMMERCIAL SHIPPING CONCERNS

1. Background

The original intent and purpose of the Open Market Corridor was to facilitate the purchase of supplies and services by Federal, State and local government users, on-line through the use of electronic catalogs and embedded contract templates accessible via the World Wide Web.

To make a difference in the area of DoD procurement, the scope of the responsibility to deliver the best value product or service to the war fighter on a timely basis is significant. Force sustainment enables our nation to pursue regional coalition building and collective security efforts, including the ability to influence action globally. Sustained forward deployment includes a wide range of logistic support for our military forces operating at sea, ashore, or in littoral regions. The continuous replenishment of our operating forces is the backbone that enables deployment of military operations at great distances and sustainment at a high readiness posture for extended periods. More importantly, the engagement in joint and multinational logistics efforts is increasingly vital to support mutual readiness and capability, enhancing the efficiency and effectiveness of our combat operations, particularly in our continued war efforts against terrorism.

Currently, WWX commercial carriers can deliver critical materials to deployed units in mature theaters with safe and available commercial airports quickly and effectively. However, movement of materials into contingency areas, particularly in semi-mature and immature theaters, presents considerable challenges. This research explores the effectiveness and limitations of using commercial carriers and the Defense Transportation System (DTS) to move material into the contingency areas as well as how effectively OMC can interface with the DTS and commercial logistics systems to increase the visibility of material for the contingency contracting officer.

2. Customs

a. History

Customs manages the physical movement of everything sent in and out of a country. With regards to customs concerns, there are several organizations that started the battle of customs issues as it relates to international trade. Customs is a critical area of commercial shipping because there is no exact set of international rules for either commercial or military shipments. A few of the more influential organizations with experience that dates back to the early 1900's are still in existence today, in an environment where many more rules and regulations have been imposed by numerous countries.

The International Chamber of Commerce (ICC) was founded in 1919 with the aim "to serve world businesses by promoting trade and investment, open markets for goods and services, and the free flow of capital" (ICC Webpage, October 2003). ICC's initial momentum came from its first president, Etienne Clémentel, a former French minister of commerce. Under his influence, the organization's international secretariat was established in Paris. He was also instrumental in creating the ICC International Court of Arbitration in 1923. ICC has expanded since those early post-war days when business leaders from the allied nations met for the first time in Atlantic City. The original representatives of Belgium, Britain, France, Italy and the United States, have expanded to become a world business organization with thousands of member companies and associations in more than 130 countries. Some of the members include many of the world's most influential companies and represent every major industrial and service sector. ICC's mission is to assure effective and consistent action in the economic and legal fields in order to contribute to the harmonious growth and the freedom of international commerce.

In 1951, the International Bureau of Chambers of Commerce (IBCC) was created. The IBCC quickly became a focal point for cooperation between Chambers of Commerce in developing industrial countries and took on added importance as the Chambers of Commerce of Transition Economies, responding to the stimulus of the market economy. The World Customs Organization (WCO) was established in 1952

with seventeen countries, but has grown to include more than 159 countries. These are just a few of many organizations that have led the battle of customs issues for commercial trade. Additionally, these organizations have had a tremendous effect on the DoD policies and procedures regarding the movement of supplies when transported through commercial businesses.

b. Current Situation

The main focus of this section is to evaluate the issues and concerns involved with customs for the Department of Defense, commercial carriers, customs brokers and husbanding agents' roles when using the WWX program, and how they can effectively minimize associated customs while facilitating the process of getting material through customs in an efficient and expeditious manner.

Major portions of supplies sent to deployed American forces are handled via military assets. But continued quick and efficient sustainment and re-supply of these military units have to be supplemented by commercial carriers subject to customs. Commercial customs standards for DoD involves the commercial shipping agents, such as UPS, FedEx and DHL, who utilize customs brokers to expedite their goods through foreign customs and pay additional customs duties required in each country. In contrast, the U.S. military does not pay customs duties but is required to provide additional paperwork and is subject to possible long delays in most countries.

A key issue at hand is whether it is more cost effective (money vs. time) to utilize the current systems used by commercial carriers, even though it equates to paying customs duties? According to current air cargo industry trends and an AMC/WWX Customer Survey results collected from military personnel onboard Pacific and Atlantic Fleet aircraft carriers deployed to the Arabian Gulf, the military increasingly uses commercial carriers and has been required to pay the additional costs for customs services anyway (Grandjean, 1991). The key advantage of using WWX is that these commercial carriers have already established firm arrangements with the participating countries allowing them to move materials through customs in almost every region around the world with minimal delay.

Supply and maintenance officers find this advantageous because the Navy faces these issues everyday. Most deployed military personnel agree that the extra cost far outweighs the additional time it takes to get the material being sent and the costly delays in receiving critical parts through foreign countries due to customs related problems. These delays can quickly turn into a logistics nightmare in terms of degraded mission readiness and operational capability. In the maintenance world, maintainers can appreciate the cost savings of having the parts and materials available as quickly as possible to complete repairs in order to have a combatant ship and/or aircraft fully mission capable.

c. Areas of Concern

As the Department of Defense reestablishes military posturing to address the emerging threats of the 21st century, as outlined in Joint Vision (JV) 2020 there are some serious challenging issues that need to be addressed to assure that the expectations of JV 2020 are achieved. One of those issues is the possible effect that customs delays have upon the logistical support requirement for a faster, more lethal, and more precise military force of JV 2020. Problems causing customs delays included lack of modernization for customs transaction processing, inadequate use of customs brokers, and improper shipping documentation.

The DoD describes future military operations as "full spectrum dominance" that will enable U. S. forces "to conduct prompt, sustained, and synchronized operations…" through "Focused Logistics…ensuring delivery of the right equipment, supplies, and personnel in the right quantities, to the right place, at the right time to support operational objectives" (Joint Vision 2020, 2000). The implication of this statement directly involves the movement of material efficiently to and from points of conflicts and all future points of conflict as defined by the DoD arising in different contingency locations, including nations that the U.S. has no diplomatic or military relations. With the military's heightening reliance on efficient transportation of parts and supplies vice inventory management, variances within logistics become increasingly costly. Its importance translates to ensuring that "boots on the ground" have the necessary equipment and supplies to not only ensure their combat effectiveness, but also

their sustainability and survivability. To meet the sustainment requirement of military operations in previously unknown areas of operations, customs becomes a vital link in logistics support due to the variances in customs clearance time, predictability and transparency, or lack of information. Moreover, as nations increase their customs requirements, commercial shipping agencies range of services have to increase to provide transparent interaction between nations and interoperability of information to become a crucial link in logistical support to our deployed forces.

In the corporate sector, civilian firms closely measure customs clearance time in hours versus days or weeks. Any delays in predictability can severely interrupt or shut down an entire production line at enormous cost due to the shift from maintaining large volumes of inventory to new supply management model measures such as Just-In-Time (JIT) delivery. Along those lines transparency of information between nations increasingly becomes a key factor to ensuring quick clearance times and predictable deliveries. Therefore, as the DoD endeavors to adopt best business practices to improve logistics management and support, it must also endeavor to search for solutions to problems and issues relating to customs.

3. Material Movement

a. Delivery Tracking

The Government desires the capability within the procurement process to track small parcel items ordered through the system until delivery. However, government transporters have limited capability of tracking their order efficiently and effectively. For the most part, current systems and procedures require the government shipper to call the contracting office, which in turn must call the vendor for status.

In a deployed environment, current web-based information systems are not sufficient for all unanticipated situations. Presently, the lack of visibility of in-transit shipments necessitates a need for a new asset visibility system that could produce an electronic manifest that can be uploaded into an information system, which is accessible down to the unit level either by transmission of specific asset visibility to each unit or accessed through a network to a centralized information point. Handling elements moving the item update the information of the asset visibility system by scanning the bar

coded label, thereby providing current delivery status of the material. One way to improve the system is for commercial carriers to equip military handling elements high-volume receivers with scanners and software. This is similar to the current requirement of commercial carriers to provide shipping systems to accounts shipping an average of twenty-five or more contract shipments per week. If this is feasible, this capability could ensure the necessary automation for WWX parcel receipt at the centralized receiving facilities that could provide enormous benefits to deployed mobile units, particularly in immature contingency locations.

In Operation Iraqi Freedom (OIF), deployed military units often experienced a degraded delivery tracking capability due to continuous maneuvering requirements on the battlefield resulting in the inadequate communications infrastructure to support supply communication requirements. According to a recent United States Marine Corps' After Action Report for OIF, the distribution of supplies was the single greatest failure of the supply chain during OEF/OIF due to failures that are closely linked to the inadequate packaging, documentation, and tracking capability. With limited asset tracking capability during continuous maneuvering conditions, Battalion/Squadron level supply officers indicated that current web-based information systems are not viable for total asset visibility in a deployed environment for all situations. As previously mentioned, receipt of high-volume receivers with scanners and software equipment by the military handling elements from commercial carriers could provide a viable solution in the battlefield.

b. Delivery Packaging

All deliverable materials must be packed and shipped in accordance with the best commercial practices in a manner that affords adequate protection against physical and environmental deterioration and damage during shipment. Inventory capability, advertised fill rates, requisitioning objective correlation, and other statistics related to the performance of the supply blocks are rendered completely useless if the requisitioning unit does not receive the supplies they have ordered.

The importance of having appropriate, durable packaging is critical since ground units usually do not deploy with any credible packaging capability (typically,

only insufficient wood, boxes, and other packaging materials). The inability to package supplies for delivery, and for storage once in theater, was a significant degrader to effective supply support. Furthermore, material handling of requested supplies involved handling more than sixteen times prior to delivery to the requisitioning unit, causing extreme damage. Military units should be able to specify, in each individual order, special requirements for containers, packing and unpacking, handling, and labeling to WWX commercial shippers.

c. Delivery Documentation

Improper and inadequate documentation on the majority of individual parts and boxes significantly contributed to the failure of the supply chain distribution in a deployed environment. Currently, there are various methods by which documentation was affixed to individual items, causing some parts to be delivered to intermediate supply units without additional documentation identifying the designated requisitioning unit.

Shipping, documents, containers, correspondence and packages must be marked with the following information: contract number, proposal title, individual order number, short titles of contract line items, and point of contact. Moreover, each supply material must have a packing slip that is solidly affixed to the item, able to withstand extreme weather conditions, external helicopter lifts, and multiple handling of the item. The packing slip must be standardized across all military services and contain a bar code representing the document number for the material. Each package having multiple parts, require bar coded labels, and must contain all associated document numbers located inside the package.

AMC delivered packages are never delayed in supply for customs clearance. This differs from the commercial WWX shipments, which inherit an additional customs clearance task. Country-specific customs procedures vary by region and are affected by current diplomatic relations with the United States (although these variations and challenges may be resolved in much of Europe, as the European Economic Community (EEC) increasingly becomes the primary customs authority). Nevertheless, WWX packages must be formally authorized as official government property by using a T1 commercial customs bond form in order to be processed duty-free. The U.S.

Government is exempt from paying customs duties and fees when government owned materials are contained in the shipment. All other material owned by personnel or contractors is subject to customs duties and/or taxes. WWX carriers are responsible for listing all the government items included in the shipment on the T1 form. An authorized U.S. customs agent will visually inspect both material and documentation for customs compliance and provide a signature on the T1 indicating U.S. verification that all items on the form are official government property. It is very important for WWX carriers to list only official government items on the T1 form since they transport both official government and personal small parcel shipments. Hence, it is critical to differentiate the official parcels from personal packages to prevent personal shipments from clearing customs as official government property. Failure to do so could endanger the excellent working relationship that the United States currently enjoys with foreign customs officials.

In a telephone interview with Robert Butherus, USMC's WWX Agency Contracting Officer Representative, he highlighted the fact that shippers can eliminate some costs by being better aware of the high charges incurred for additional services such as address corrections, missing account numbers and exceeding maximum weight limits. Such costs have skyrocketed recently as carriers try to make up for increases in insurance and security costs. In fact, other major small package carriers have increased accessorial charges more than 150% on average since 1996 and these unplanned charges can quickly add up for a large shipper if not monitored closely.

J. DEFENSE TRANSPORTATION SYSTEM

The Defense Transportation System (DTS) is an integral part of the total global transportation system and involves procedures, resources, and interrelationships of several DoD, Federal, non-U.S., and commercial activities that support DoD transportation needs. Support of the National Military Strategy (NMS) must include modern, flexible, responsive global transportation that is capable of integrating military, commercial, and host-nation resources. DTS is multi-faceted, resulting in a versatility that supports the entire range of military operations. (CJCS, vii)

DTS consists of those common-user military and commercial assets, services, and systems organic to, contracted for, or controlled by DOD. Combining the capabilities of common user transportation assets into an integrated network optimizes the use of air mobility, sealift, and land transportation resources, provides greater visibility over operations, and expedites the transition from peace to war. Transportation procedures and responsibilities as they relate to peacetime and wartime requirements should remain unchanged regardless of the type of operation conducted.

Transportation processes and procedures are performed in accordance with the DoD Regulation 4500.9-R, *Defense Transportation Regulation*. This standardization allows transportation forces to train during times of peace in the same manner in which they operate during war or a contingency and provides the inherent flexibility to effectively and quickly support any type of military operation. In this regard, the aggregate transportation capability exercised through the DTS is a critical enabling instrument that allows DoD to support the objectives and strategies of the President and Secretary of Defense (SECDEF). USTRANSCOM is assigned the mission to provide air, land, and sea transportation for the DoD, both in times of peace and war. In this capacity, except for those assets that are Service-unique or theater assigned, Commander, USTRANSCOM exercises combatant command (command authority) of the assigned transportation assets and is the DoD single manager for transportation. He aligns traffic management and transportation single manager responsibilities to achieve optimum responsiveness, effectiveness, and economy. Commander, USTRANSCOM also establishes and maintains relationships between DoD and the commercial transportation industry. Geographic combatant commanders who have transportation assets assigned to their commands should ensure that the assets are managed, controlled, and capable of full integration into the DTS. The principles and considerations discussed in Joint Publication (JP) 4-0, *Doctrine for Logistic Support of Joint Operations*, provide useful guidance to this end. It describes the essential nature of a logistic function that can "integrate the national and theater effort to mobilize, deploy, employ, sustain, reconstitute, redeploy, and demobilize the forces assigned and attached to a combatant commander." (CJCS, vii)

1. Airlift

Air Mobility Command (AMC) is the single manager for air mobility in DoD. AMC's mission is to provide airlift, air refueling, special air mission, and aero medical evacuation for U.S. Forces. AMC also supplies forces to theater commands to support wartime tasking as the Air Force component of USTRANSCOM (www.public.af.mil). Some of the assets used by AMC are the C-9, C-12, C-20, C-21, VC-25, C-32, C-37, C-137, C-141, C-17, C-5, and the KC135.

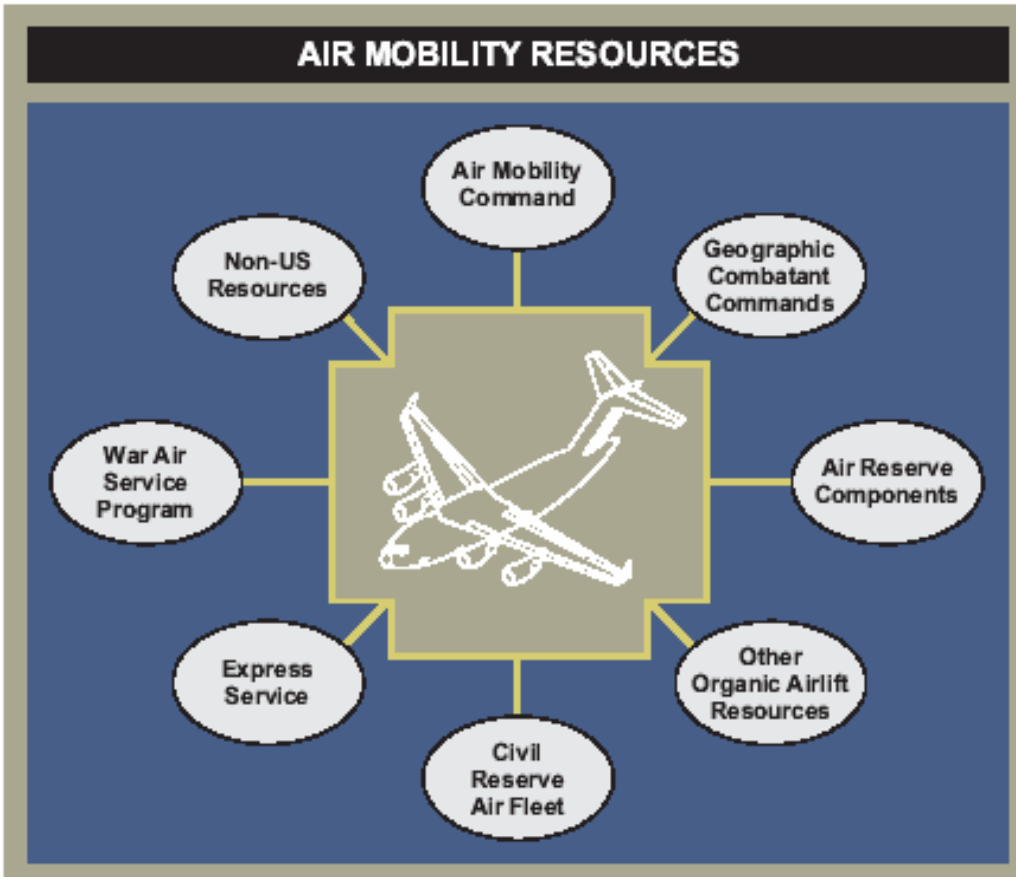


Figure 13. Air Mobility Resources

2. Sealift

Sealift resources of DTS can be classified as belonging to three separate pools of resources: United States Government (USG), U.S. flag, and foreign flag assets. USG assets can be found in both DoD and Department of Transportation (DOT). In DoD, the Military Sealift Command (MSC) is the primary provider and operator of sealift

resources. In the DOT, the Maritime Administration (MARAD) is the primary provider of sealift resources. Its mission is to strengthen the U.S. maritime transportation system—including infrastructure, industry and labor—to meet the economic, and security needs of the nation. MARAD programs promote the development and maintenance of an adequate, well-balanced United States Merchant Marine, sufficient to carry the U.S's domestic waterborne commerce and a substantial portion of its waterborne foreign commerce, and capable of service as a naval and military auxiliary in time of war or national emergency. MARAD also seeks to ensure that the United States maintains adequate shipbuilding and repair services, efficient ports, effective inter-modal water and land transportation systems, and reserve shipping capacity for use in time of national emergency

MSC is the transportation provider for the DoD with the responsibility of providing strategic sealift and ocean transportation for all military forces overseas. MSC's Naval Fleet Auxiliary Force (NFAF) Program is composed of fleet ocean tugs, fast combat support ships, oilers, combat stores ships and ammunition ships plus two hospital ships. The NFAF provides direct support for Navy combatant ships allowing them to remain at sea for extended periods. These ships perform underway replenishment services for Navy battle groups and deliver food, fuel, spare parts and ammunition. Some NFAF ships provide ocean towing and salvage services. NFAF ships are crewed by civil service mariners and each ship carries Navy departments ranging in size from four to forty-five people (NFAF, www.nvr.navy.mil). MSC resources available to the DTS beyond MSC's active peacetime fleet are fast sealift ships (FSS), large, medium speed roll-on/roll-off (LMSR) ships, and pre-positioned ships.

3. Surface

Military Traffic Management Command (MTMC), another component command of USTRANSCOM, which maintains transportation agreements and all commercial carrier costing information necessary to move shipments within CONUS via surface transportation, controls surface resources such as trucks and rail in DTS. MTMC's

functions also include approving commercial carriers to conduct business with the DoD, evaluating carrier performance, and maintaining carrier tender information.

There are numerous transportation and mobility resources available to geographic combatant commanders overseas. The type and number of sources vary by theater. They include supporting and/or supported Combatant Commander theater requirements, HNS, Acquisition and Cross-Servicing Agreements (ACSAs), and multinational civil transportation support organizations and structures.

4. Ports

Critical components of the DTS are military and commercial ports supporting the air and maritime movement of unit and non-unit personnel, equipment, and cargo. These ports could be owned and operated by MTMC, AMC, a Service, geographic combatant commander, or commercial or Host Nation authorities. They may be either sophisticated fixed locations or heavily dependent on deployable mission support forces or joint logistics over-the-shore assets to accomplish the mission. The significant surface and air cargo handling capabilities that exist in the Services should be used jointly rather than in isolation to maximize the throughput capability of these essential transportation modes.

The extensive use of containers and 463L pallets makes container handling equipment (CHE) and material handling equipment (MHE) essential elements of the DTS. Ensuring that these assets are available early allows for the efficient loading and unloading of ships and aircraft and increases the rate at which a port can be cleared. Without these assets, the DTS may come to a halt.

5. In Transit Visibility

In transit visibility (ITV) is the ability to track items in the logistics pipeline from vendors to CCOs. ITV is paramount to keeping down cost since it provides CCOs the ability to view where their items are in the shipping pipeline, enabling them to gain reliance in the supply chain, avoiding circumvention of DoD's acquisition process. Automated information technology (AIT) and automated information systems (AIS) are vastly improving DoD's ability to achieve total asset visibility. The conceptual automated process leading to this capability consists of gathering and maintaining timely

and accurate source movement data. The timeliness and accuracy of data within management systems depends on the communications systems used to convey the data throughout the system and the frequency with which the data must be re-entered into the system. Ideally, data should be entered once into the system and then perpetuated throughout the automation continuum via the communication and logistics information systems. This is not the case with most legacy DTS logistics information systems and one of the reasons for the inefficiencies experienced by the DTS.

Nevertheless, having visibility of every item in the DoD logistics pipeline is not cost-effective or necessary. Some areas with visibility blind spots may be acceptable. These areas include an item that is inexpensive or easily procured, or the time period is so brief that tracking the product is not cost-effective. A good example is office supplies. The general non-criticality of these items, their general availability, and short time that visibility is lost suggest that gaining visibility is not cost-effective, especially since the ability to use information to influence a transaction is negligible. So criticality of the items being shipped and their overall value to the unit must be considered prior to incurring the added expense of ITV.

Another area of concern in ITV is the initiative by DoD to outsource some of its logistical functions to 3PL providers. One of the drawbacks from this is the minute control and visibility over 3PL shipments that DoD receives from these arrangements. Generally, 3PL providers do not use DTS procedures, systems, and standards. This situation makes achieving an ITV capability for 3PL-managed shipments particularly challenging (JTAV website, October 2003).

6. DTS Information Systems

The first and foremost technological component required to enhance ITV within DoD is a seamless automated management system, including assured communications that support transportation and other logistic functions from origin to destination. Furthermore, in order to cut cost, lessen the time of cargo in the logistics pipeline, build confidence in the supply chain, and achieve its mission efficiently and effectively, DoD must leverage information technology to provide contingency contracting personnel with the tools they need to complete there mission as quickly, safely and efficiently as

possible. The link between information technology and people is critical and is required for the success of any contingency operation. DoD must integrate emerging technologies with AIS to meet organizational goals and provide world-class support to the warfighter. Examples of these technologies and information systems are:

a. Global Transportation Network (GTN)

USTRANSCOM's GTN gives its customers, located anywhere in the world, a seamless, near-real time capability to access – and employ – transportation and deployment information. GTN is an automated command and control (C^2) information system that supports the family of transportation users and providers, both DoD and commercial, by providing an integrated system of ITV information and command and control capabilities. GTN collects and integrates transportation information from selected transportation systems. The resulting information is provided to the National Command Authorities (NCA), combatant commanders, USTRANSCOM, its component commands, and other DoD customers to support transportation planning and decision-making during peace and war. In keeping with modern technology, GTN is completely available on the Internet's World Wide Web and SIPERNET. Figure 14 illustrates some of the information systems that interface with GTN.

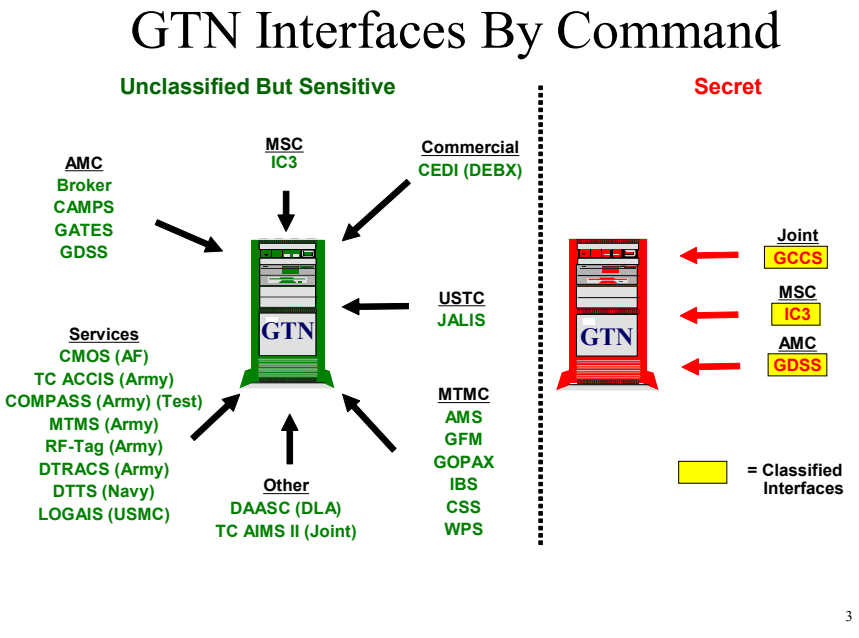


Figure 14. GTN Interfaces (From the GTN Website, October 2003)

Change is just over the horizon for the users of the Global GTN, however. In about eighteen months the fielding of GTN 21, the successor to the current legacy system will be available for DoD use. USTRANSCOM is aggressively working the development of this new system to enhance asset visibility. The system's architecture will contain the latest technological advancements available to date.

The current system debuted in October 1996 as a solution to the asset visibility challenges experienced during DESERT SHIELD and DESERT STORM. GTN continues to meet this challenge by providing vital ITV information on passengers, patients, cargo, and conveyances moving in the DTS—movement information that is critical to military operational missions worldwide.

Since September 2001 and with the increase in contingency operations worldwide, there has been a significant increase in the number of personnel using GTN. For example, customers performing queries on unclassified data jumped 61 percent to over 11,000, while users of classified data soared 92 percent to more than 2000. Moreover, end-user queries have risen to more than 120,000 per month compared to 40,000 before September 2001. Despite this huge increase, GTN continues to serve the military well. However, it is now being stressed beyond original design capabilities.

On September 26, 2002, Northrop Grumman Information Technology was awarded a $204.4 million contract to build GTN 21. Initial operational capability (IOC) is scheduled for December 2004, with full operational capability planned for 2006. The operational missions of today require a more robust, flexible, and user-friendly system and GTN 21 promises to be the answer.

Some of its enhanced features will include a user-tailored application. GTN 21 will deliver a user-friendly functionality with a much better look and feel. Whether you are a land, sea, or air user, the user will be able to select the desired data fields that fit the line of work. Another feature is improved C^2 information to support warfighter decisions. GTN 21 will contain an active data warehouse with two years of historical data. This is a significant improvement over the existing system, which only stores ninety days of data. It will also support over twenty customer application systems

and will support multiple command post exercises simultaneously. (GTN Website, October 2003)

Today, GTN aggregates data from twenty-five government and nearly fifty commercial source systems to provide customers ITV on passengers, patients, cargo, and conveyances moving through the DTS. GTN 21 will receive data from these same sources, but has been built to easily expand to enable additional capability. GTN was only designed to process three million data transactions per day, which is not sufficient to support today's operations tempo. GTN 21, on the other hand, will process up to 7.2 million transactions per day—more than doubling processing capacity. Most impressively, the Northrop Grumman engineers are designing GTN 21 with the architecture capability to expand processing well beyond the above stated requirement. (GTN Website, October 2003)

But how does GTN communicate with commercial carriers in order to provide ITV to its users? In order to communicate with commercial carrier systems, GTN uses the Commercial Electronic Data Interchange (EDI) format to exchange data. The DEBX (Defense Electronic Business Exchange) checks to ensure the EDI coming from the commercial carriers is in the correct IC (Interchange Convention) format. When the commercial carriers send status messages to GTN, GTN links the TCN or Bill of Lading number to the data received from the Global Freight Management (GFM) system. GFM is a MTMC system that provides visibility of bills of lading, government and commercial. GFM contains data on the material inside the package being shipped. In GTN, you can see where the cargo is moving, and what is inside the box (known as level six detail). GTN also provides visibility of the information in the systems with which it interfaces as shown in Figure 14 above. This provides the user (e.g., CCO, warfighter, etc.) a complete picture while their cargo moves through the DTS pipeline (Interview with Mike Ashton, 2003). Some exceptions to this process are 3PL providers, which are being used more and more by DoD acquisition units to outsource some of their logistic functions and to replace inventory with information. Unfortunately, even though USTRANSCOM is developing GTN 21 to become the single defense database for ITV

information, 3PL providers are not contractually obligated, in most cases, to provide asset visibility.

One of the drawbacks of GTN, as in many DoD and commercial information systems, is the frequency in which data is updated in the system. Depending on the contract the commercial carrier has with DoD, it can take from one to twenty-four hours to receive critical ITV data on cargo traveling on commercial carriers to DoD points of debarkation (POD).

b. Joint Total Asset Visibility (JTAV)

For several years, many DoD organizations had developed asset visibility capabilities, creating *islands* of visibility within the DoD logistics system. JTAV has bridged the legacy systems and is facilitating the development of new capabilities to fill voids in those systems. Although mainly used for organic material, JTAV is set to begin receiving data from commercial carriers in the near future. Below is an illustration of proposed and in place data flows between JTAV and other AITs, AISs, and Logistic Information Systems, both organic and commercial.

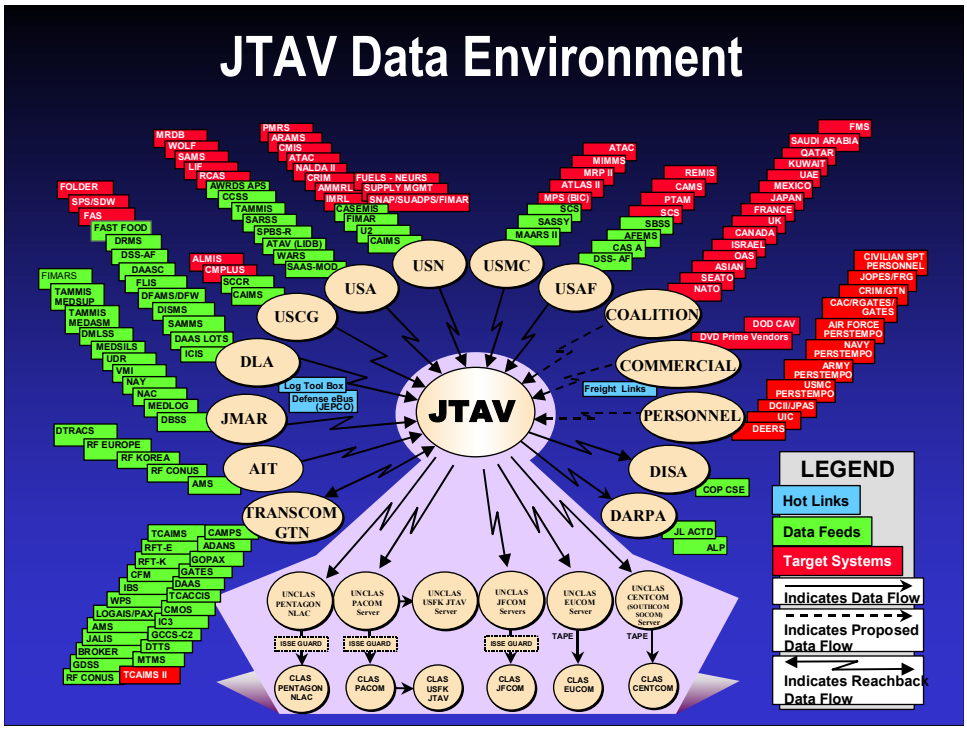


Figure 15. JTAV Data Environment (From the JTAV Website, October 2003)

The DoD plan that first addressed the need for total asset visibility (TAV) was the *DoD Total Asset Visibility Plan* published in 1992 (DoD, 1995). The plan served as an excellent first document to lay the foundation for the current efforts. It established many JTAV ideas, such as the concept of establishing visibility of in-storage, in process, and in-transit assets, that continue today.

In March 1993, OSD formed a DoD Asset Visibility Integration Group composed of all military services, Defense Logistics Agency (DLA), Joint Logistics Systems Center, USTRANSCOM, Joint Staff, and Defense Information Systems Agency (DISA). The group capitalized on related DoD component efforts, began the integration of the Logistics Information Processing System (LIPS) with GTN, and sponsored fast payback efforts that could be implemented by legacy systems. For example, one effort was the visibility of consumable items at Navy and Air Force retail units by DLA. This effort required agreements on visibility and business rules as well as the integration of data in legacy systems. The agreements were achieved by making the process a win–win experience for all participants. In April 1995, the Deputy Undersecretary of Defense for Logistics (DUSD(L)) selected the Army as the Executive Agent for JTAV and established the JTAV Office.

The office continued the development of JTAV–IT and deployed it to U.S. European Command (USEUCOM) in March 1996 in support of Operation Joint Endeavor and other peacekeeping operations in Bosnia and Central Europe. In addition to JTAV–IT, the office has sponsored initiatives to redistribute reparable assets among the military services and monitor convoys and trains supporting Operation Joint Endeavor with radio frequency identification (RFID) devices and satellite technology under Defense Transportation Reporting and Control System (DTRACS). DTRACS is an Army information system that tracks surface movements with a satellite-tracking network that provides remote monitoring, tracking, and location of organic assets in support of United States Army, Europe (USAREUR) and European Command (EUCOM).

In June 1998, the executive agency for JTAV was transferred from the Army to DLA. The JTAV Office continues to make steady progress and achieve regular

successes. The current status of the JTAV initiative is best described in terms of JTAV–IT, Global JTAV, and JTAV's relationship to the Global Control Support System (GCSS). GCCS is an AIS designed to support deliberate and crisis planning with the use of an integrated set of analytic tools and the flexible data transfer capabilities. JTAV–IT is the capability being developed for combatant commanders, Joint Task Force (JTF) Commanders, and service components to use in an overseas theater. Global JTAV consists of additional functions, including wholesale supply and depot maintenance, for which the JTAV Office is working to improve asset visibility.

Another consideration the DoD should consider is the inability of JTAV to communicate with its Allies logistics information systems. If the United States plans to take full advantage of agreements with coalition forces, information concerning logistics support should be exchanged with friendly foreign forces. This concept requires JTAV to be able to transmit and receive data from foreign systems. (JTAV website, October 2003).

c. JTAV–IT

JTAV–IT provides combatant commanders, JTF commanders, and service components with a view of the assets in a theater. Initially, JTAV–IT included assets in the retail storage facilities of all four military services as well as war reserves in the theaters. As JTAV–IT has matured, the customer requirements have increased. Today, JTAV–IT strives to include wholesale and worldwide retail visibility. Additionally, GTN provides information on assets in-transit to a theater. Automatic identification technology devices, through associated AISs, provide enhanced asset visibility to a theater of operation and ensure assets can be tracked from industry to foxhole. GTN and JTAV incorporate AIT capabilities into their system architectures, thus providing CONUS to theater asset visibility tracking information. JTAV–IT was deployed to USEUCOM and United States Central Command (USCENTCOM) in 1996 and to U.S. Atlantic Command (USACOM) in 1997. Although operationally oriented, the deployments to USCENTCOM and U.S. Army Command were also intended as part of a rapid prototyping strategy. The deployment to USEUCOM, on the other hand, was

aimed primarily at providing operational support to Operation Joint Endeavor. In February 1998, JTAV–IT was also deployed to the U.S. Pacific Command (PACOM).

d. Global JTAV

The Global JTAV mission is to ensure the required level of JTAV capability is provided to DoD's sustaining base organizations, operational units, defense agencies, and their commercial counterparts. When fully deployed, Global JTAV will track in-storage, in process, and in-transit assets and assist in improving DoD's logistics practices. Primary Global JTAV redistribution initiatives include the interservice visibility of consumables, repairables, and maintenance activities, and should be able to expand to incorporate the visibility of commercial carrier data in the future with little difficulty.

7. DTS Information Systems Interfacing With Commercial Information Systems

GTN 21 will integrate information, from DOD and commercial automated transportation systems used in current transportation processes, to satisfy ITV and C^2 information requirements in peace and war. GTN 21 will collect and display transportation information from selected source systems on a recurring basis. The collected data will include supply, cargo, forces, passenger, and patient movement requirements; schedules with closure estimates and actual movements of airlift, air refueling, aero medical evacuation, and surface lift (land and sea); operation plan data; location and operational status of transportation assets, transportation infrastructure, and summary level financial information. GTN-21 will interface with commercial carriers through EDI. The only difference between GTN and GTN-21 on this effort is the DEBX will only check to ensure the EDI coming from the commercial carriers is in the correct IC format. On the current GTN, the DEBX is also reformatting the data so that GTN can accept it. GTN21 will receive the data the way it comes from the commercial carrier. When the commercial carrier sends status messages to GTN, GTN links the TCN or bill of lading number to the data we receive from the GFM system. We also make links on the data from the carriers between many other systems that feed GTN. This provides our

user (warfighter) a complete picture while their cargo moves through the transportation pipeline.

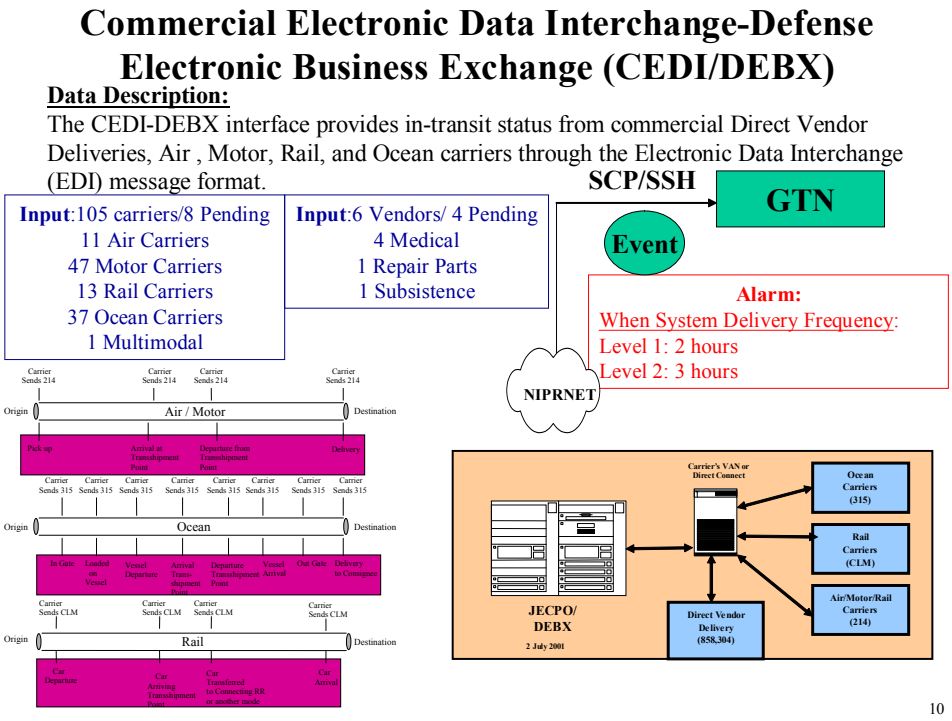


Figure 16. Commercial Electronic Data Interchange/DEBX (From the GTN Website, October 2003)

8. Issues From Contingency Contracting Officer Perspective

The following information was gathered via interviews with three CCOs and one transportation officer in the Middle East operation area. These men had very different perspectives about some of the topics presented. One of the topics mentioned was asset visibility. One officer, LCDR Tom Armstrong, SC, USN, was not very interested in ITV. He is currently serving in Dijbouti, receives commercially purchased items about 30-45 days after purchasing, and never wonders where in the logistics pipeline these items are at any given time. The transportation officer serving in Bahrain was not that interested in ITV either. Even though he had been serving in this area for over three years dealing with various transportation and logistics issues, he still was not cognizant of the paramount importance of having ITV as much as possible. On the other hand, another officer who recently served as a CCO on the Office for Reconstruction and Humanitarian Assistance (ORHA) staff in Iraq as was constantly concerned with ITV. With items

traveling via commercial carriers, ITV was outstanding until it was received in Kuwait and became a part of DTS. This was a constant frustration of a Marine CCO, Major McGowan who visited Naval Postgraduate School in September 2003. His units, however, in the early part of OIF, were without AIT and AIS access and fully dependent on the Kuwait Theater Distribution Center (TDC) for information on incoming cargo until they obtained iridium phones for telecommunication access to commercial vendors.

Another interesting topic of discussion among these officers was the use, or non-use of the previously mentioned information systems such as GTN and JTAV. In the case of the transportation officer in Bahrain, LCDR Michael Kinney, even though he had a JTAV account, stated he never used this account because the users he dealt with most frequently, whether at sea or ashore, hardly ever used this system either. He did use GTN and Global Air Transportation Execution System (GATES) extensively, however, and they worked fine for him. GATES is an AMC system that provides a single interface for cargo and passenger manifests.

Major McGowan, of course, had no means to use these systems since no durable laptops or wireless communication were delivered to the Marine units in Iran until later on in the OIF campaign. LCDR Richard Pacquette, who was on the Office of Reconstruction and Humanitarian Assistance (ORHA) staff, did have a laptop with Internet access, as well as wireless communications, and was able to use GTN for ITV.

The last interesting tale mentioned by LCDR Cody Hodges, who also was an ORHA CCO, was the difficulty in getting the few commercial items he did purchase outside of Kuwait into the country past customs. (Customs issues are discussed earlier in the chapter.) He stated that only two Majors had the authority to allow items past customs. If either of their signatures were not on the paperwork accompanying items coming through Kuwaiti customs, they were not allowed in without a "payment" to the Kuwaiti customs officials. This is not an uncommon practice in this area of operation from talking to other CCOs in this region.

K. ISSUES AND RECOMMENDATIONS

1. Contingency Contracting Functions

Organization and control of assets is a major concern in any contingency operation (whether combat or natural disaster) for the theater Combatant Commander. Establishing the contracting and logistics organization is no different. Current regulations provides the theater commander the option to establish a unified theater organization as it relates to contingency contracting or allow the various services to establish their own logistics structure. A unified structure is recommended, but in either structure having a process to coordinate efforts is a must. In this environment, OMC has the potential to solve the coordination issues.

One of the most difficult problems for the contracting officer at an unfamiliar deployment site is locating capable contractors to fulfill unit requirements. The following are suggestions a contracting officer may use to solve this problem: (NAVSUP, page 11)

a. Investigate the possibilities of initiating a contract for husbanding services with a local source to assist in the identification of and conduct of business with local vendors.

b. Use the knowledge of an interpreter/guide regarding local businesses. This person is a logical first choice for obtaining sources; however, the CCO must be careful to avoid a conflict of interest with local contractors and the translator.

c. The U.S. Embassy or consulate (if available) can be an excellent source of information. The Defense Attaché Office in most embassies or consulate can help with currency conversions and storage of funds, as well as providing a source list of reputable contractors. In addition, the Embassy General Services Officer (GSO) may be able to provide some contracting support particularly if the contract is to be written with the host country.

d. Site surveys are an excellent tool to speed up the contracting process. CCO's should add sources to the site survey list, as they become known.

e. There are a multitude of creative methods of identifying sources available to the CCO. Some successful methods (although not all inclusive) include contacts with the chamber of commerce (or equivalent), business associations, local clergy, citizens, and local government leaders such as the mayor. Consider running advertisements in local newspapers describing expected general offices, which can help locate local sources of supplies. In addition, there is nothing wrong with asking other contractors where certain requirements might be obtained. The local yellow pages are a valuable source of information on local firms as well.

f. A "bid board" must be posted in a public place at the contracting office for the purpose of displaying solicitations and announcing awards and proposed contracts.

g. Coordinate and assist local trade associations in disseminating information to their members.

h. Since most major U. S. deployments receive considerable publicity, many firms with international offices will contact the CCO to offer their goods and services. Also, it is recommended that large procurements be advertised via newspapers within the area of operation

OMC can supplement all of these methods of source selection and build a local module with selected vendors. In mature environments with well-established infrastructures, sources of supply are typically readily available. As such OMC developers can establish regional modules tailored to support the contingency and built with local sources of supply, from which CCOs can readily choose. Optimally, local vendors would have access to the database as well, so that solicitations and award acceptance could all be handled electronically, streamlining the contracting process and expediting delivery and acceptance of material. Payments can be handled electronically via OMC also. Unfortunately, in immature or semi-mature environments, access by vendors and payment to vendors electronically may not be possible.

In locations where the infrastructure is not as well established, such as in semi-mature or immature environments OMC can still be effective in obtaining vendor support. Results of site surveys can still be built into the system to assist the coordinatoin

the efforts of regional contracting offices. Where local sources are not readily available due to lack of infrastructure in immature environments or in areas devastated by natural disasters, OMC provides a link to sources outside the contingency area. Transportation issues, as discussed later in this chapter and resources such as the Electronic Procurement Palette Setup (EPPS) as discussed in Chapter Five supplements the effectiveness of OMC deployment in the contingency environment.

These tailored modules can support the theater logistics concept for the theater combatant commander or the lead agency involved in disaster relief. In this regional module warranted CCOs can be built into the module at the discretion of the HCA or PARC depending on the size of the contingency (and a list of local vendors from which to procure supplies). The combatant commander may also elect to use a joint theater logistics management element or establish a contract clearinghouse such as utilized by the U.S. Pacific Command (PACOM). The clearinghouse recommends standardized policies and procedures for contingency contracting during regional contingencies, joint theater exercises, and natural disaster relief in the PACOM AOR. Additionally, a warrant for a CCO from the various service components is recognized by the other service components. This allows a joint contracting cell to begin work quickly without having to re-warrant everyone on the joint contracting team. Furthermore, only one set of PIINs is used for each exercise or operation. Business rules can be built into the regional module to fulfill the tenets of this regional concept. OMC provides the benefit of a tailored consolidated database to coordinate ordering of scarce resources in an austere environment and provides continuity of information during the course of CCO turnovers.

The turnover of contracting personnel in a contingency environment continually presents unique challenges that plague the contracting force. To compound the situation, numerous activities from which the contracting officers originate insist on providing their deployed contracting officer with PIINs from the home office to utilize in the field. Consequently, when the deployed CCO returns home, parent commands insist on the files, which document the use of the PIIN, to return as well; therefore, the field contracting office looses continuity on the items contracted for the deployed force. Again, a more logical setup is the utilization of a common contracting database. OMC

provides an excellent fix for this aspect of the contingency operation. Due to the multi-tiered construction and the mirrored sites provide by Networld Exchange, Inc. (Networld), if utilized, OMC maintains a database of all generated requirements and contracting actions resident in the contingency area of operation. The visibility of requirements allows for leveraging by the contracting cell through consolidated purchases rather than competion for scarce resources. Additionally, continuity is maintained on all contracting actions despite the constant turnover of contracting personnel.

Additionally, vice deploying with PIINs from the parent commands, OMC could be used for PIIN generation. The system can automatically provide a PIIN for each contract action. If utilized by the regional contracting offices and the ordering officers, PIINs would not be duplicated. Since the files are backed up electronically in a central database as well as mirrored sites outside the volatile area of operation, the documents are secure and available for relieving contracting personnel entering the contingency environment.

2. Defense Shipping Function

Through its use of air, surface, sea, DTS is a significant resource to DoD and needs to leverage its logistics systems with global commercial and DoD emerging AIT and AIS in order to meet the needs of its users in the areas of responsiveness, ITV, efficiency, and effectiveness. With the growing number of contingency operations in immature environments, DTS will continue to play a major role in delivering cargo, passengers and other critical items to CCOs and warfighters.

DoD continues to reengineer logistic processes via integration of time and location with cost, customizing service for individual customers, outsourcing to 3PL providers, and through the formation of strategic alliances. This reengineering will require GTN capabilities to be accurate, timely, flexible, and robust. The use of coalition forces in contingency operations may be the model for future military engagements. Such an organizational structure creates logistics challenges that include nonstandard formats, potentially incompatible communications links, and unfamiliar business processes. In addition, a reliance on allied forces also brings an attendant reliance on foreign vendors and HNS. Visibility requirements need to be refined continually to satisfy customer

requirements using the latest technological advances, but with wisdom so that there is always value added in the ITV received.

Customs is a major deterrent to U.S. forces obtaining critical parts and supplies in a timely manner. In order for DTS to be effective in future operations to the fullest extent possible, this issue must be resolved through negotiations with Allied countries in times of peace or before another major conflict erupts. The use of Customs Brokers and treaties seems to be the simple solutions, but other solutions may be explored for feasibility and cost reductions.

The final recommendation for DoD is to decide on what AIT and AIS work well for all the Services and gradually phase out the other stovepipe AIT and AIS systems in the Services so that there are only a few systems being used by everyone in the military. This will reduce cost, time, and resources, increase reliability, sustainability and maintainability of the few systems in use and provide the superior logistics service our Service personnel deserve. JTAV and GTN 21 seem to be the best overall systems at the moment, but DoD should strive to continually update these systems to keep them viable for not only contingency operations but also all DoD missions, now and in the future.

OMC can serve as a force multiplier in this scenario. With the scalability and functionality offered by OMC, this system can serve as an integrator between the commercial and defense-shipping world, capitalizing on the advantages of both. Its ability to interface with external legacy systems allows it to communicate with the shipping services and provide the shipping information in a single interface to the CCO.

3. Commercial Shipping Function

As the military restructuring continues to evolve, the Department of Defense can ensure the viability of Focused Logistics and effective use of the WWX by aiding and supporting the modernization of the of customs transactions, increasing the use of customs brokers and improving the Government Bill of Lading documentation.

First, the interoperability of information is an important requirement to meet the needs of military sustainment because after the initial surge of personnel and supplies are positioned near the point of conflict the utilization and reliance upon commercial carriers

greatly increases. Hence, it is vital to maintain a good customs transparency between nations and continually modernize to ensure military supplies are not delayed when using the WWX due to inaccurate or incomplete administrative documentation. In a recent Quadrennial Defense Review (QDR) completed by the Department of Defense Inspector General (DoD IG), the study identified several discrepancies:

- ✓ In February 1998, DoD sustained $600 million in outstanding bills.
- ✓ 40% of shipping documentation arrived after the cargo reached port.
- ✓ 20% of shipping documentation contained inaccurate data.
- ✓ Carriers' collection costs for DoD were double compared to commercial customers.
- ✓ Average payment process time for DoD to pay carriers was 60-90 days (IG-DoD, November 1997).

One way to avoid the continuation of this costly scenario is to encourage the DoD to promote better relations among nations of interest to create a common desire to modernize national customs agencies. By supporting customs modernization and creating buy-in from other nations the DoD can ensure its success to sustaining possible U. S. military actions through the use of the WWX especially in unknown contingency locations.

Secondly, the utilization of customs brokers can also remedy the gap in information and transparency further assisting the effectiveness of commercial carriers' time definite delivery service. Customs brokers are utilized by the DoD but only in a limited capacity such that combatant commanders use their services only as a last resort after U. S. Customs Agents are unable to meet the units' needs. Currently, there are only twenty-five countries where U.S. Customs agents are stationed that are major military hubs, and they are generally unfamiliar with other nations customs regulations, acting mainly as intermediaries for the transfer of military shipments. With the shift of military forces and possible military actions in to nations where the United States has not historically executed military operations, their customs rules and regulations become waypoints for commercial shipments of military supplies unless the commercial carrier

has customs services, customs brokers within its business process. Furthermore, since the U. S. Customs Office has been placed under Homeland Security, the major emphasis on funding has shifted on security as opposed to improving customs information processes. Failure to improve the use of customs brokers will keep commercial carriers from investing their limited resources on their respective customs services and contacts, vice on possible improvements to the delivery process of the WWX program for the war fighter in contingency locations (e.g., Iraq and Afghanistan).

According to recommendations submitted by deployed units to the Arabian Gulf, one method to expedite package delivery involves shipping parts via the WWX program (e.g. FedEx or DHL overnight services) directly to the Naval Air Station Terminal at Naval Air Station Norfolk, Virginia, for further transport to Bahrain, which will then be placed directly on the next available AMC flight. AMC is an Air Force Command, with flights scheduled to depart on Mondays, Tuesdays, Wednesdays, Fridays, and Saturdays. Tuesdays and Saturdays flights provide one-day delivery to a central location in Bahrain called the Banz Warehouse, which is controlled, by the Commander, Logistics Forces, Naval Forces Central Command (COMLOGFORNAVCENT), allowing the package to by pass customs. Navy shore detachments ensure final delivery of the parcel(s) to deployed units in the surrounding area and to ships at sea. Shipping overnight to the NAVAIRTERM in Norfolk, VA for further transport via AMC takes four to five days to arrive at the Banz Warehouse in Bahrain. With perfect timing, the package arrives prior to the Tuesday or Saturday departure and takes as little as two days for delivery but is not guaranteed.

An alternative method to expedite a package to the Arabian Gulf is by shipping the package directly to the Banz Warehouse. FedEx and DHL Worldwide Express are two commercial carriers able to express deliver to Bahrain. DHL's Middle Eastern hub is located at Bahrain International and packages should arrive there in two days. Federal Express' hub is located in Dubai, United Arab Emirates, and warranties delivery in four days. DHL applies fewer restrictions on packages (HAZMAT, weight, size, etc.) and reportedly has better working relations with Bahrain customs due to its early establishment of the company in the region. The package normally takes two to three

days to clear customs except during the Islamic weekend and all Islamic holidays. At times, shipping directly to the Banz Warehouse results in delays despite DHL's fast delivery service due to customs holding the package for more than three days as a result of inaccurate or incomplete documentation, which nullifies the advantage over the AMC flight. Despite the commercial carriers' potential advantage in speed, AMC provides reliability to bring packages into the country and out to the ships at sea.

Package delivery to ships at sea provides a different challenge due to the variability factor of organic transport assets to ships. Whichever method is chosen, the home guard squadron or support unit initiates the shipment at DHL or FedEx. In both cases, the shipper relays the Transportation Control Number (TCN) to the receiving unit to assist in tracking the shipment through the commercial shippers' webpage and to utilize the Global Transportation Network (GTN). Furthermore the TCN can be provided to NAVTRANS and/or a support unit to request assistance in expediting the package through customs and providing transport to the ships at sea. The GTN is an automated system that gathers information from transportation users and airlift providers (DoD and WWX commercial carriers). USTRANSCOM, its component commands and customers, can access this integrated network to locate packages in the shipping pipeline. GTN brings together transportation information from various unrelated systems into a single integrated view for the Defense Transportation System. One common factor among all the data sources is the TCN. GTN users can track the status of a shipment by requisition number or TCN. For the transporter and end-user, GTN data contains an abundant source of information for assessing and monitoring global system performance.

Order tracking is an inherent feature of OMC. The order-tracking function provides a variety of ways for both the buyer and seller to manage orders through the fulfillment process. Various types of shipping status can be provided tailored to the needs of the DoD user. For a long-term solution to tracking shipment status, Networld will have to integrate to the suppliers to extract any shipping information they may provide. This may necessitate a trigger that will activate a "package delivered" message, which requires implementation of a new process (or more likely many unique processes

that reflect the differences in how each supplier ships its products). These modifications to the order tracking process can be made in a relatively short time.

Integration to major commercial shippers like Federal Express, UPS, DHL, Emory Worldwide and others will likely result in OMC being able to provide shipment-status reports at every transition point from initial pickup to final delivery. At the other end of the spectrum, small suppliers using their own trucks for local deliveries most likely would not be able to provide much more than a simple email stating when a product was shipped, and where it was delivered, and who signed for the delivery.

In lieu of an integration process to communicate shipment information, Networld routes an email message to the supplier, along with the Purchase Order, asking for notification when the supplier ships the goods purchased. The email also asks for information such as a shipping date, how the goods were shipped, with what company, and an estimated time of arrival.

Thirdly, improvement of the Government Bill of Lading documentation is another way to prevent unnecessary delays in the WWX program to deliver supplies to its final destination. One source of delay for material delivery involves incomplete or improper documentation. In a telephone interview with Department of the Navy's Pierre Kirk of the Naval Transportation Support Center, a common source of errors is the failure to properly identify the specific branch of service as the shipper, addressee, or consignee in the shipping documentation. Based on prior agreements established with the host countries, packages that contain simple additional annotations in the remarks section such as "The Property of the United States Government" resulted in administrative ease when dealing with customs.

III. GOVERNMENT-WIDE PURCHASE CARD USE IN THE OPEN MARKET CORRIDOR

A. INTRODUCTION

In today's logistics environment, "the need to reduce the time and effort required to process low value purchases remains one of the key purchasing challenges facing organizations today. By improving how they manage low value purchases, organizations can begin to redirect their efforts toward value-creating activities that result in competitive market advantages while simultaneously reducing the costs associated with low value purchases" (Trent, p. 6). Value creating activities for DoD logistics activities are focused on supporting the warrior, the operator in the battlefield, whether that is by ensuring that a continuous supply of water is available for the troops on the field or tracking spare parts for the Chief Engineer.

The DoD EMALL provides customers (in this case the logistician supporting the operator) web enabled ordering for a variety of products, especially low value items. OMC is an offshoot of the DoD EMALL and focuses on low value item buys allowing the customer to go on-line and pick from, potentially, over 277,000 catalogues. With OMC focusing on simple, low-priority buys, automation and purchase cards are an alternative for payment and purchasing in this area. Advocates of this method argue that "automation releases personnel focused on transaction management from this task; purchase cards further reduce transactions costs, particularly when bundled with auditing and reporting support from issuing banks." (Camm, p. 237)

While the DoD EMALL, and especially the OMC, are relatively new products, Governmentwide purchase cards have been in use since the mid 1980s. Since its inception, the purchase card program has been constantly evolving. This chapter focuses on the status of the current DoD purchase card program and how the OMC can improve the process. To increase the reader's understanding, the history of the Government-wide purchase card program is discussed, the current method of establishing and running a purchase card program at the command level is illustrated, and the current benefits and weaknesses of the program are identified. The chapter then addresses GAO cases dealing

with current problems which include fraudulent and improper use by cardholders, security breaches to cardholder accounts, improper management by the Agency Program Coordinator (APC) and Approving Officials (AOs) and poor reporting techniques to paying activities causing delays in payment and reconciliation thereof. With the problems identified, the chapter provides OMC's solutions to these problems.

Finally, this chapter addresses purchase card use overseas, evaluating two areas. The first area is contingency operations and how the purchase card is used as an effective tool in an environment that calls for flexibility. Secondly, the "sustained" environment, in which a program has been set up at a base of operations and processes and regulations are fully in place. In both areas, the effectiveness of using the purchase card is analyzed. Also, the problems associated with Currency Exchange Rates, bank transaction lead times, and Value Added Tax and how OMC corrects these problems is discussed.

B. HISTORY OF THE GOVERNMENT PURCHASE CARD PROGRAM

1. Background

Prior to the establishment of the Government Purchase Card Program, "micro-purchases", purchases under $2,500, of non-stock numbered items were cumbersome and time consuming. The "old system" was associated with long wait times, high administrative costs, tracking difficulties, and a limited number of vendors willing to accommodate the extra paperwork and slow payments. The end user had to provide detailed specifications to Government procurement offices, which would then determine the best source of supply. It often took several weeks for the customer to receive the required goods. (Leard, p. 10) The "old system" was inefficient and acquisition reform was required to streamline the process.

On March 17, 1982, President Reagan issued Executive Order 12352 on Federal Procurement Reforms. (Joint Report, p. 3) This document directed executive agencies to reduce procurement administrative costs and proposed that purchase cards be implemented as part of the effort.

2. Pilot Program

In 1986, a pilot program was conducted by several agencies on the use of a purchase card to reduce procurement costs. The pilot program goals included simplifying procurement, improving productivity, enhancing internal controls, and supporting government-wide operations. The agencies found the pilot program successful. Specifically, they found the purchase card process less costly and more efficient than other methods. The end user could go directly to the vendor instead of through the procurement office. Great savings in time and effort were realized over the traditional process of preparing the requisition, sending it to the procurement office, waiting for the office to issue the purchase order, and preparing receiving reports. (Joint Report, p. 3)

3. First Purchase Card Contract

As a result of the pilot program, the first government-wide commercial purchase card contract was awarded by the General Services Administration (GSA) in 1989 to the Rocky Mountain Bank Card System (RMBCS) and was titled I.M.P.A.C., International Merchant Purchase Authorization Card. (Joint Report, p. 3) The card was not widely used under this first contract due to high administrative fees that agencies had to pay under the contract.

The next milestone for the purchase card program came in 1993 with Vice President Al Gore's National Performance Review (NPR) "From Red Tape to Results-Creating a Government that Works Better and Costs Less." The NPR identified the purchase card as a major acquisition reform and recommended that all Federal Agencies increase usage of cards for small purchases, which were defined at $25,000 or less, to cut the normal "red tape". In addition, it also recommended that the FAR be amended to promote purchase card use. (Joint Report, p. 3)

4. Federal Acquisition Streamlining Act/Executive Order 12931

Up to this point, the purchase card still saw limited use. However, in 1994, there were two events that greatly stimulated the use of the purchase card, the Federal Acquisition Streamlining Act of 1994 (FASA) and Executive Order 12931 dated October 13. (Joint Report, p. 3)

FASA established a "micro-purchase" threshold of $2,500 and reduced or eliminated most of the restrictions for purchases valued at or below the threshold such as the Buy American Act, competition, and certain small business requirements. As long as the micro-purchase meets the fair and reasonable price goal, it is exempt from the usual requirements. Also, under FASA, non-procurement personnel can make micro-purchases without becoming procurement officials as long as they did not exceed $20,000 in a twelve-month period.

Executive order 12931 directed agencies to expand the use of purchase cards and delegated micro-purchase authority to program officials. (Joint Report, p. 4) As a result, the purchase card program was here to stay.

5. 1994 to Present

In February 1994, GSA re-competed the contract and again awarded it to RMBCS. The administrative fees were eliminated and GSA established guidelines for agencies using the program. In particular, internal controls, spending limits, and operating procedures had to be established at the agencies before issuing the cards. (Joint Report, p.4) Also, interim FAR rules were issued that cited purchase cards as the preferred method for making micro-purchases and an accepted method for making payments over the micro-purchase threshold. FAR Part 13.301, Governmentwide Commercial Purchase Card, has since been added. (Joint Report, p. 4) Throughout the DoD various names have been used to refer to the Governmentwide Purchase Card Program. For the rest of this chapter, the Governmentwide Purchase Card Program will be referred to as "the purchase card program".

As stated in the introduction to the chapter, the purchase card program is constantly evolving and a number of changes to operating procedures have taken place over the years in response to different problems discovered by GAO audits, which is discussed later in this chapter. Currently, the Navy is using Citibank as their credit card provider while the Air Force and Army are using U. S. Bank.

C. PROGRAM ESTABLISHMENT AT THE ACTIVITY LEVEL

1. A Navy Unit as an Example

Once all the legislation was in place and the Executive Order was given, it was time to implement the program at the individual unit level. For the purposes of this thesis, a Naval vessel is used as an example of establishing the purchase card program. This process also carries over to shore commands. Once the Commanding Officer determines the need for a purchase card program to support the command mission, the Supply Officer sends a request to the HCA. In the case of an afloat unit, the HCA is the Type Commander's Purchase Card Program Manager. The HCA sends the approval to the Supply Officer via the Commanding Officer. Next, the Supply Officer is normally appointed as the Agency/Organization Program Coordinator, A/OPC, who is responsible for the management of the program on behalf of the Commanding Officer. In addition, a Reviewing Official, normally the Executive Officer, is appointed to perform reviews of certified invoices within the purchase card program. The next step in the process is for the A/OPC to complete required training and establish or become familiar with the local procedures for the command. Once the local policy procedures are signed by the Commanding Officer, the A/OPC establishes the program with the bank and is now ready to open accounts.

The A/OPC appoints the Approving Official, AO, and the cardholders. The AO is an individual who has a number of cardholders report to him or her. The AO is responsible for reviewing and approving the cardholder's monthly transactions to ensure that they were necessary Government purchases in accordance with the FAR and all other pertinent policies. A cardholder is issued a card in his/her own name for accountability purposes, and is responsible for making the actual purchases. See Figure 17 for graphic representation of establishing a purchase card program. Once the program is initially established, positions can be turned over as personnel leave the command.

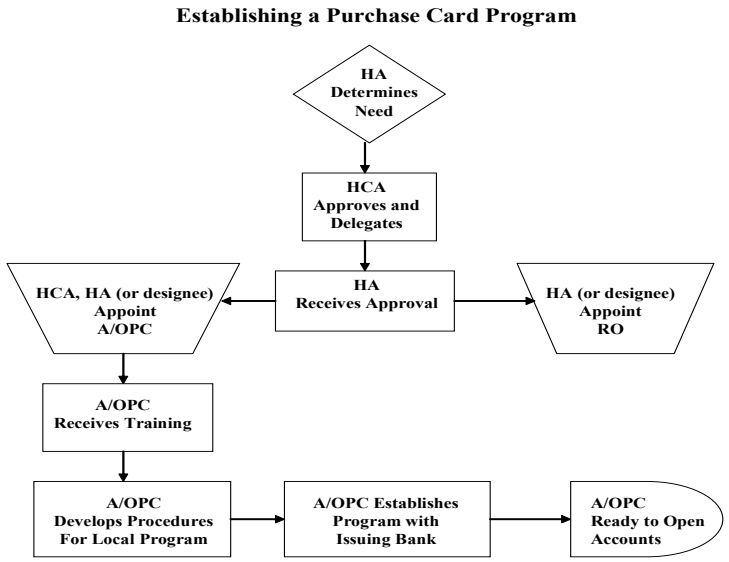


Figure 17. Establishing a Purchase Card Program (From the DoD Purchase Card Website, October 2003)

After implementation, the command is ready for the cardholders to start making purchases fulfilling customer requirements. Figure 18 represents the typical purchase process and is important in the discussion of the GAO cases.

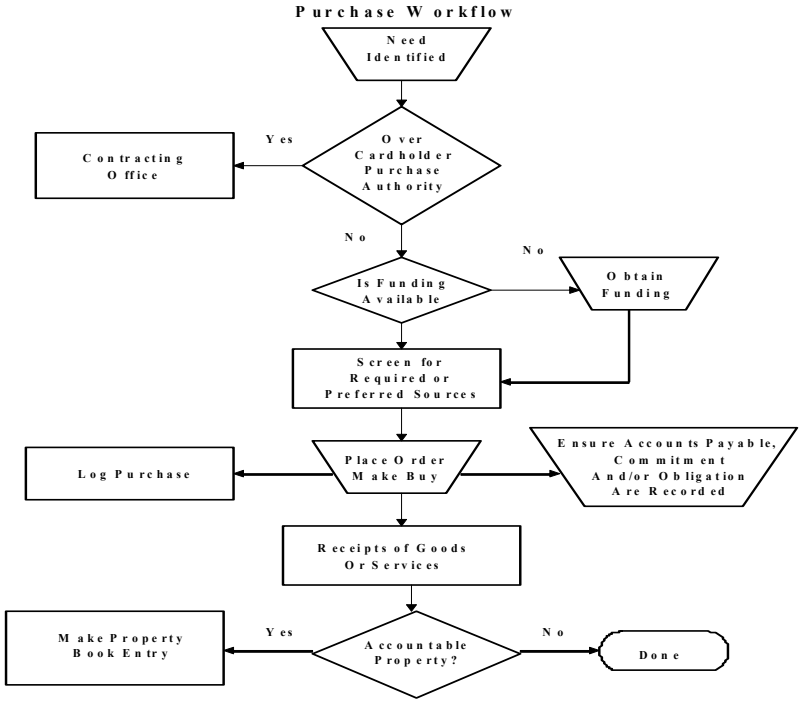


Figure 18. Purchase Workflow (From the DoD Purchase Card Website, October 2003)

D. BENEFITS OF THE PURCHASE CARD PROGRAM

1. List of Benefits

Since more than 90 percent of all Government purchases are under $2,500 and only 2 percent are over $100,000, there are great benefits to be gained through the purchase card program. Reportedly, the purchase card has the following benefits (Leard, p. 13):

- ❖ Worldwide acceptability
- ❖ Immediate access to commercial goods
- ❖ Streamlined procurement process
- ❖ Improved payment process
- ❖ Audit trail
- ❖ Decreased cost to process payments to vendors if card is used as a method of payment.

The goal of OMC is to capitalize on these benefits in a more efficient manner as compared to existing DoD systems such as DoD EMALL and GSA Advantage.

2. Additional Benefits and How OMC Can Increase the Benefits

As a result of FASA, the purchase card is now a viable alternative for micro-purchases and simplified acquisition. Since micro-purchases are no longer subject to the Small Business Act and the Buy American Act, Procurement Administrative Lead Time (PALT) and paperwork have been greatly reduced. A Navy study found that the average lead-time for receipt of needed items was reduced from thirty days or more to only six days. (Joint Report, p. 4) The "old system" was characterized by inefficiency and could turn a $5.00 purchase into a $60.00 purchase with administrative costs. There was an instantaneous increase in customer satisfaction with the purchase card program. The program grew, and by the end of 1995, purchase cards were used by virtually every Federal Agency. The goal of OMC is to further reduce PALT through increased efficiency and reduced transaction costs by allowing one purchaser to increase the number of transactions that can be processed in a given time period.

Another significant benefit of the purchase card program is the cost reduction associated with processing a requisition. A 1994 civilian interagency study showed internal costs were cut by more than half as compared to purchase orders. Additional studies have shown an average administrative savings of $53.00 per transaction when compared to the "old system". The savings become significant when the growth of the program is considered. DoD purchases with the purchase card grew from $2.5 billion in FY97 to $6.1 billion in FY01. Additionally, purchase card transactions grew from 5 million in FY97 to 10.6 million in FY01. (Task Force, p. 2-1) As a result, DoD has saved over $954 million on administrative costs by using the purchase card over the last eight years. The card usage is increasing which means increased savings in the future. The goal of OMC is to further reduce transaction cost by reducing transaction fees charged by card issuing banks.

A third benefit of the purchase card program is increased competition. Since the small business set aside was eliminated for purchases up to $2,500, large businesses are now a viable source for 90 percent of government purchases that were previously open only to small businesses. Additional competition was automatically introduced to the purchasing process since there were so many more vendors available to choose from with the participation of large businesses. Also, small businesses started accepting purchase cards and became more competitive since they lost the advantage of small purchase set asides. (McMahon, p. 30) Although the cardholder was not required to get three competitive bids for a micro-purchase, competition was inherently built into the system since there were more choices of vendors, each wanting to give their best price. However, cardholders are encouraged to get three bids when practicable. OMC greatly enhances competition due to the fact that there are some 277,000 vendor catalogs in the database. As a result, the cardholder has instantaneous access to well over three suppliers for each purchase and can do a comparison based on any number of factors with which the buyer wants to query the database. Since OMC enhances the process of competition and gives the purchaser increased access to suppliers, OMC can lead to additional cost savings in the purchase card arena.

A fourth benefit of the purchase card program is realized when the card is used as a payment method for purchases over $2,500. The process is very simple only requiring agreement by the vendor to accept the card as payment and a clause in the contract stating that the vendor will be paid via purchase card once proof of shipping is provided. The payment method using OMC benefits both the government and the vendor. The government benefits because the payment is processed electronically reducing manpower requirements previously needed to process the payment manually through DFAS. Also, late charges and interest payments are avoided since the payment is processed at the time of purchase. The vendor benefits because the funds are in the business's checking account within two days. Accounts Receivable personnel do not have to spend time tracking the payment through DFAS. The payment process using OMC is described in eight steps as written by James Smith in his Networld Exchange brief, Outline of Financial Alternatives:

1. The online customer finds the merchant's website and adds products to a shopping cart. When the customer is ready to check out, the customer may enter billing information on a secure page on the merchant's website.

2. If the merchant does not have a secure page the customer can be transferred to the merchant's secure payment gateway, where the customer can enter the billing information into a secure form. If the merchant does have a secure site then the information will be "passed" to the payment gateway without the customer ever leaving the merchant's site.

3. Once the billing information has made it to the payment gateway it is then transmitted to MerchantWarehouse.com's (or other third-party) processor.

4. MerchantWarehouse.com's (or other third-party) processor will then pass that information onto the bank that issued the credit card. The issuing bank will check to see if the card is valid and see if the amount requested is available on the card and set aside the amount of the purchase for the merchant.

5. The issuing bank will send back an approval number or a decline message back to MerchantWarehouse.com's (or other third-party) processor.

6. That information will then be passed back to the payment gateway. It will take approximately 3-15 seconds to complete steps 2-5.
7. The payment gateway will then pass the approval code back to the merchant's site. If the merchant does not have a secure site, the payment gateway will give the customer the approval information. At this point, the merchant can also choose to have the payment gateway email the customer a payment receipt.
8. At the end of the day, the payment gateway will "settle" all of the day's transactions. Once the settlement process is initiated, the funds will be transferred from the card-issuing bank and MerchantWarehouse.com (or other third party) will electronically deposit the funds into the merchant's checking account. It typically takes 2 business days from the time of the original transaction for the funds to reach the merchant's checking account.

To review then, the three variations on the payment-gateway theme are:

1. Enter information on a secure page on the online merchant's site and pass it in real time to a payment gateway.
2. Transfer entire payment process to a payment gateway (redirect to a different site for payment).
3. Enter information on non-secure page on the merchant's site and the pass that information securely to a payment gateway. (Smith)

Figure 19 is a graphic representation of the payment process using OMC.

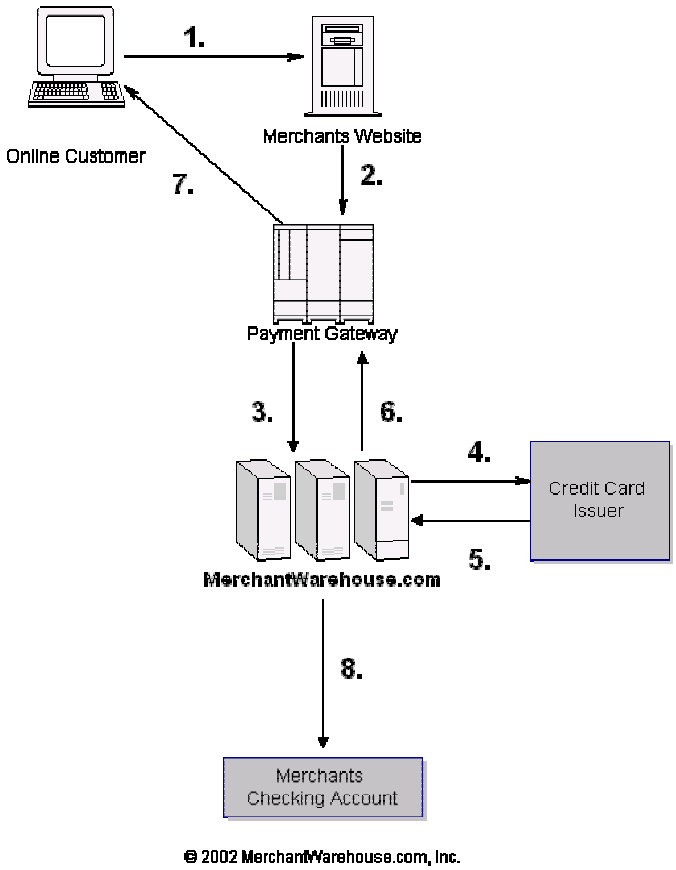


Figure 19. OMC Payment Process (From MerchantWarehouse.com)

E. WEAKNESSES OF THE CURRENT PROGRAM

1. Introduction

Along with the benefits, the purchase card program has weaknesses, which are targets of current reform. First, this section identifies the weaknesses and section G addresses how OMC can correct these weaknesses. The weaknesses can be traced to management controls. Causes include inadequate command emphasis, poorly enforced internal controls, and lack of personal accountability. (Final Report, p. VI) Since card usage is growing so rapidly, agencies must have adequate controls in place to ensure that the cards are not misused. While these weaknesses are not common at all agencies, they are common to the agencies that make the evening news and are subject to Inspectors General (IG) and GAO audits.

2. Lack of Review and Approval Process

One major weakness identified by the IG is the lack of a review and approval process. (Oversight, P. 78) To ensure that a purchase is for official government purposes only, the AO should review and sign the purchase request prior to the cardholder placing the order. According to the DoD Government Purchase Card Concept of Operations, the AO is responsible for reviewing his/her cardholder's monthly statements and verifying that all transactions were necessary government purchases and in accordance with FAR and all other policies. However, a recent IG Audit of a Navy unit found that some AOs were not requiring cardholders to obtain authorization prior to making purchases. Since cardholders were not required to get pre-approval for purchases, the command had no way to prevent abusive purchases.

For example, the IG Audit identified a number of potentially abusive transactions. These were purchases of items supposedly for official use but without documented determination to show whether the items were necessary for government use whether they were to satisfy personal preferences. Specifically, cardholders purchased nine flat-panel computer monitors at a total cost of $13,192. However, adequate monitors could have been purchased from the GSA schedule for a total cost of $2,700. (Control Weaknesses, p. 28) In this case, there was no documentation that the GSA monitors would not meet the requirement and the flat-panel monitors were required.

Instances of this type are typical of IG findings. If a pre-approval process were put into place, there would be no doubt whether the requirement was legitimate or just fulfilling personal preferences of the cardholder. Commands run into problems when standard management controls are not followed, and unfortunately, not all AOs are following proper procedures. One excuse given by an AO at the Navy unit under IG investigation was that there was not enough time to review transactions. This is an area, addressed in section G, where the automation provided by OMC can eliminate the problem of lack of time to review the requests prior to purchase.

3. Span of Control

Related to the problem of the AO's lack of time to review transactions is the issue of span of control. Span of control deals with how many accounts over which any one individual has charge. IGs have found that some AOs are in control of too many cardholders. As a result, the AOs were merely signing monthly statements without reviewing purchases or viewing supporting documentation. One particular IG audit found that an AO was responsible for certifying billing statements for 1,153 cardholders. (Oversight, p. 79) Specifically, the one AO was responsible for certifying over 700 monthly purchase card statements relating to these cardholders. (Control Weaknesses, p. 25) While this is an extreme case, it is clear that it is virtually impossible for the AO to have reviewed all transactions to ensure that the purchases were legitimate.

Another IG report found that 3,463 AOs oversaw more than seven cardholders and thirty-one of these AOs oversaw more than 100. (Acquisition, p .1) The common problem in these IG investigations is that the AOs were in charge of too many cardholders. As a result, the AOs lost management oversight. These examples demonstrate that the weakness was not in the program itself, but in how managers, at individual commands handled, or failed to handle, purchase transactions. DoD allowing no more than seven cardholders per AO was implemented a recent solution to the lack of AO control. In addition, A/OPCs will have no more than 300 cardholders under them. The chapter later addresses how OMC takes the burden off the A/OPCs and AOs to enforce this regulation.

4. Lack of Documented Training

The next major weakness is lack of training in the use of purchase cards. FASA allows the purchase card to be used by non-procurement personnel. While this is not necessarily bad, problems can result from a lack of training. Navy and DoD policy state that cardholders and AOs must receive initial purchase card training and refresher training every two years. However, this does not always take place, especially at the commands that were subject to the IG investigations. Investigators found commands with inadequate or non-existent training programs that lacked documented training. Additionally, the training programs were not standardized or enforced DoD wide.

The lack of training becomes a serious problem when non-procurement personnel are allowed to make purchases. Personnel who were not familiar with basic practices and regulations, thereby allowed mistakes, intentional and unintentional, to go unnoticed. Another major problem arises when the A/OPC is not familiar with procurement regulations. The A/OPC is supposed to be the one in charge of the program at the command level. If the A/OPC is unfamiliar with policy and regulations, how can he/she possibly train subordinates in the proper procedures or how would the A/OPC know if something was wrong? The recently published DoD Concept of Operations presents a solution. It is now required that the A/OPC has knowledge of contracting policy and procedures along with financial policy and procedures. (Concept of Operations, p. 54) The OMC provides a solution to the issue of ensuring training is conducted and documented and is discussed in the specific problems for OMC to address.

5. Ineffective Monitoring At the Unit Level

The next weakness to be discussed is ineffective monitoring at the unit level. To have an effective, successful program, continuous monitoring is required. Naval Supply Instruction, NAVSUPINST 4200.85C, which governs the Navy purchase card program, requires that internal audits be conducted at least semi-annually. The audit should cover all aspects of the program including adherence to internal operating procedures, training requirements, micro-purchase procedures, receipt procedures, and statement of certification on the monthly cardholder statements signaling that they have been reviewed by the AO. In addition, the A/OPC should review the cardholder accounts to verify that the purchase card is actually required for the cardholder to perform his/her duties. Investigations have found cards in the hands of personnel who do not even perform purchasing functions. Also, the A/OPC should verify single purchase limits and monthly spending limits to verify that they are in line with the cardholder's needs and experience level. Furthermore, the A/OPC should verify the merchant code assigned to each cardholder. The merchant code allows the A/OPC to restrict the usage of the purchase card for unauthorized purchase card transactions such as cash advances, airline tickets, bars and restaurants, or any other type of merchant that the A/OPC wants to restrict the

cardholder from purchasing through. In addition, an official list of unauthorized items is included in the DoD Government Purchase Card Concept of Operations.

Again the IG investigations have found that the troubled units were not following the published guidelines requiring internal monitoring. (Oversight, p. 80) For example, one IG found that the command under investigation did not perform any systematic reviews of the program for an entire year. The APC said that monitoring efforts consisted of scanning some monthly invoices for duplicate payments, split purchases and other suspicious payments. However, these minimal actions were not even documented. (Control Weaknesses, p. 29) Also, at this same command, cardholders were making split purchases to circumvent the $2,500 micro-purchase threshold by having vendors ring up purchases a few minutes apart. Since AOs and APCs were not thoroughly reviewing monthly statements, these actions went undetected. (Control Weaknesses, p. 47) The OMC has numerous ways to address these internal monitoring requirements including the Order-Management Website and the Purchase Reconciliation System, which are covered in the following section.

6. Waste, Fraud, and Abuse

While the purchase card program is a more efficient and cost effective procurement tool compared to the "old system", it is subject to abuse as identified by the above weaknesses. As a result, it is imperative that purchase card management personnel are properly versed on internal operating procedures and are aware of indicators of fraud. In general, fraud is the intentional misrepresentation of facts, or a deceitful practice. In the case of purchase cards, intentional use of the card for other than official Government transactions constitutes misuse, and depending on the facts, may involve fraud. (Blueprint, p. 2) The purchase card program has checks and balances built in to deter fraud. However, if management does not follow the guidelines, the door is opened to misuse and possibly fraud. OMC can be most helpful in the detection of fraud.

If fraud or misuse is detected, the A/OPC should cancel the purchase and take disciplinary action as appropriate. Also, depending on the facts involved, personnel may be subject to fine or imprisonment for actions relating to purchase card misuse or fraud. For example, if convicted under 18 U. S.C 287, a person is subject to a fine of not more

than $10,000 or imprisonment for not more than five years, or both. Additionally, military members may be subject to court martial under 10 U. S.C 932, UCMJ Article 132. (Blueprint, p. 2) Misuse of the card includes: purchases which exceed the cardholder's limit, purchases not authorized by the command, purchases for which there is no funding, purchases for personal consumption, and purchases that do not comply with the FAR and other applicable policy. Purchase card misuse and fraud may have the following potential consequences for the cardholder: cancellation of the card, reprimand, low performance marks, suspension of employment, termination of employment, counseling, or criminal prosecution. (Blueprint, p. 3)

Since misuse and fraud are such serious offenses, management must be aware of the indicators when reviewing monthly transactions. These indicators include: incomplete records for review, multiple even dollar amount purchases, multiple purchases with the same vendor, transactions on non-workdays, hitting or exceeding monthly spending limits, lack of receipts, transactions with two merchants of different names but the same address, and the use of the card by other personnel. (Blueprint, p.14) While this list is not all-inclusive, nor does the occurrence of these events guarantee misuse or fraud, the AOs and A/OPCs should be aware of and look for these indicators when conducting monthly transaction reviews. Section G addresses how automation employed by OMC will help the AOs to detect fraud when auditing monthly statements thus serving as a deterrent to misuse and fraud.

As stated earlier, IGs found that a lack of management controls can lead to misuse. To illustrate what can happen, two examples are provided.

On April 10, 2002, a director for a defense agency field site was sentenced to 30 months confinement, 3 years supervised release and restitution of $581,997 by U.S. District Court. The conviction and sentencing are the result of an investigation into allegations that the former director used his privately owned business to make $310,410 in fraudulent charges to Government purchase cards held by his subordinates. The director was the AO for the cards. In addition, the director embezzled $271,587 in Government funds by allowing businesses to make fictitious charges to the cards and then divided the proceeds with the businesses.

A supply technician pled guilty to a single count of theft of Government property in U.S. District Court and agreed to restitution in the amount of $29,053. Investigation revealed that the individual purchased a number of items for personal use, including a motorcycle, with a Government purchase card. Investigation also revealed that the individual had altered documentation to substantiate the purchases. Sentencing will be held at a later date and could include a maximum of 10 years imprisonment and a fine of $250,000. (DoD Purchase Card Website)

These examples are just two of the recent findings through IG audits, but are typical of problems encountered. In addition, these examples point out the need for preventive measures to be carried out DoD wide. The preventive measures are practices that can eliminate the weaknesses in the program and will help to prevent fraud and misuse. OMC addresses the lack of review and approval process, span of control, lack of documented training and ineffective monitoring at the unit level providing an e-business based solution, which helps to detect fraud and misuse. In addition, OMC can be implemented DoD wide so that all commands follow the same set of standards.

F. OMC WILL ADDRESSES WEAKNESSES AND IDENTIFIED PROBLEMS

1. Introduction

Based on the weaknesses described above, OMC proposes using commercial off-the-shelf e-procurement tools to assist in reducing purchase card program weaknesses. Reducing the weaknesses, in turn, reduces the possibility of misuse and fraud. The proposed system uses an Order-Management Website (Storefront) and Purchase Reconciliation System. The system as a whole aids in compliant purchasing and detection of fraud, waste, and abuse by using a front-end website, or storefront, providing purchasing-authorization tools, a Reverse Auction, and a back end Purchase Reconciliation System to ease the burden of A/OPCs and AOs. (Networld Purchase Card Initiative, p. 1)

In addition, the system provides product menus that offer only authorized products integrating FAR-compliant sources, displaying FAR-compliant products at the top of the list in each category, with special icons to emphasize the source. Also, the

system automatically replaces product catalogs at regular intervals specified by each supplier. OMC improves the current purchase card program in the following ways:

- Provides an online entry point for Purchase Card activity
- Facilitates compliant purchasing and competitive pricing
- Lightens workload by purchasing through the storefront
- Enforces existing procedures while adding a verification element
- Enables automated detection of waste, fraud, and abuse
- Employs artificial intelligence to improve its own business rules
- Records data required for control of the Purchase Card Environment (Networld Purchase Card Initiative, p. 2)

2. Order-Management Website

The purpose of the Order-Management Website is to enforce existing Purchase Card procedures to restrain problem purchases before they are made. The website is the online entry point for all purchase card activity. In order for the cardholder to access the site to begin the purchase process, he/she must have a username and password, which is only given to the cardholder after successful completion of the required purchase card training. This is one method that OMC employs to help correct the problem discovered in numerous IG audits dealing with the lack of documented training. Once the user is on the website, activity is tracked automatically by username, password and training certification number. This allows the A/OPC and AO to have easy access to all transaction activity performed by a cardholder. In addition, the storefront provides an automated analysis of procurements against purchase card restrictions routing irregularities to AOs for inspection. (Networld Purchase Card Initiative, p. 2) The storefront also reduces the burden on all users by providing forms to record User Authorization, Need Justification, Purchase Card Log, Open-Market Approval, Accountable Items, Problem Transactions and Program Reviews.

If a cardholder needs to make an Open-Market purchase, the website provides a portal to participating retail sources. The cardholder is able to obtain secondary approval

from his/her AO for Open-Market procurement through the storefront. The cardholder simply completes an online form and presents it electronically, or in person to the AO. Approvals are then recorded on the storefront automatically. AOs may then use the pre-approval forms as a tool when investigating listings on the Exception Report, which is produced monthly as part of the audit process. One benefit of this process is that the AO can screen Open-Market purchases before they are made. This was one problem noted by an IG. Abusive purchases were taking place because AOs were not reviewing purchases before the fact. OMC corrects this problem with the Order-Management Website. In addition, the Pre-Approval process fosters communication between the cardholder and the AO about planned purchases, and serves as a permanent record of the purchases. (Networld Purchase Card Initiative, p. 3) With improved communication, the chance of waste, fraud and abuse will most likely be reduced.

The Order-Management Website monitors current restrictions on Purchase Card use and alerts A/OPCs and AOs when potential violations occur. Also, the A/OPCs and AOs can manage their cardholders' accounts in terms of spending limits and Merchant Category Code restrictions. These are two areas the IG audits pointed out as problematic. As noted earlier, commands had too many cardholders with excessively high monthly and single purchase limits and were able to purchase for any type of vendor. While a system already exists for an A/OPC or AO to manage these functions, the results of IG investigations seem to point out that they were not being used effectively. The goal of OMC is to make it simple and efficient for the managers to manage the accounts. Currently, the Order-Management Website embodies the following restrictions on Purchase Card use:

- Single-purchase limit by cardholder
- Splitting purchases to defeat the $2,500 micro-purchase threshold
- Cardholder purchases against non-authorized Merchant Category Codes
- Unauthorized transaction types (Cash Advances, Internet, Travel, etc)
- HAZMAT procurement

- Pricing reasonableness check
- List of prohibited/special items (Networld Purchase Card Initiative, p .4)

Finally, additional benefits of using the Order-Management Website include:

- Website allows custom "shopping lists" of frequently purchased products
- Catalog integration processes eliminate unauthorized products
- Products supplied by preferred suppliers (National Industries for the Blind, GSA, Federal Prison Industries, etc) receive priority display in each product category, along with a special icon emphasizing the source. (Networld Purchase Card Initiative, p. 3)

3. Purchase Reconciliation System

The Purchase Reconciliation System is the back-end application that helps the AO to reconcile monthly Purchase Card statements with the data entered through the Order-Management Website Purchase Card Log. The system relies on Card Number, Amount, Vendor and Date to match the storefront-recorded purchases against the purchases shown on the cardholder's monthly statement. If there are purchases on the monthly statement, but no matching entry in the storefront-recorded purchases, an exception report is generated. The AO uses the exception report to investigate the problem. Also, a secondary exception report lists purchases made from unauthorized Merchant Category Codes. These reports allow the AO to concentrate on those cardholders who have purchased outside the system rendering proper disciplinary action. (Networld Purchase Card Initiative, p.6) This system can act as a deterrent for cardholders since they will know that the AO can easily see all transactions that fall outside of regulations. Although this process takes place at the back end, the ease of the process for the AO will discourage cardholders from making the questionable purchase in the first place.

4. Lack of Review and Approval Process

OMC addresses the problem of a lack of a review and approval process through the Order-Management Website. Since the website is the single entry point for all cardholders' transactions, the AO has oversight of everything that is happening with his/her cardholders. The A/OPC and AOs can set restrictions on individual cards as described above. As a result, the cardholder is not able to make purchases that the

A/OPC or AO would not approve had the cardholder personally gone to the AO before trying to make the purchase. If there is an emergency requirement, the AO can easily lift the restriction. Additionally, the OMC has a method of monitoring Open-Market purchases through the Order-Management Website. The cardholder is required to fill out a form to submit to the AO for pre-approval of the purchase. If the cardholder does not fill out this form and log it in his/her log, an exception report is generated during the monthly AO reconciliation allowing the AO to investigate the purchase. If fraud or misuse is discovered, the cardholder is faced with disciplinary action.

The Order-Management Website is a powerful tool for the A/OPC and AO to control the review and approval process. However, the A/OPC and AOs must be proactive in setting up all of the cardholders' parameters prior to the cardholders making transactions. In addition, the A/OPC and AOs must act on exception reports generated by the OMC. Finally the A/OPCs and AOs can use the flexibility of OMC to tailor the system to meet their individual needs.

5. Span of Control

Currently, OMC does not address the span of control problem. The DoD Government Purchase Card Concept of Operations requires a reduction in the span of control allowing no more than 300 cardholders under an A/OPC, and no more than seven cardholders under an AO. (Concept of Operations, p. 4) In order for OMC to ensure that commands comply with these restrictions, a modification to the program would have to be incorporated to follow the Concept of Operations allowing no more than the maximum number of cardholders under an A/OPC or AO. This shortcoming may be off set by an increase in efficiency generated by the system. With an operational test of OMC, it will be possible to determine if the number restrictions can be raised.

6. Lack of Documented Training

The OMC partially addresses the problem of the lack of documented training. As mentioned earlier, the Order-Management Website requires a user to have a current username and password, which is assigned to the cardholder after successful completion of required training. However, the Order-Management Website does not store the training information in the database.

In order to correct the problem, OMC should be modified to include a tool for the A/OPC and AO which tracks each cardholder's training status alerting them when a cardholder's training certification is about to expire. This allows the AO to administer the proper training before the cardholder is decertified. The Order-Management Website should have a training page for the A/OPC and AO to track the status of all cardholders instantaneously. This links the fulfillment of the training requirement directly to the assigning of the username and password, and the Order-Management Website. When the cardholder's training expires, access to the website expires ensuring that no untrained personnel can make purchases. In addition, this information will help inspectors determine if the command is following the training requirements.

7. Ineffective Monitoring At the Unit Level

OMC addresses the problem of ineffective monitoring and the unit level through both the Order-Management Website and the Purchase Reconciliation System. OMC can generate monthly audits for the A/OPC and AO. In addition, the system is based on management by exception. It is incumbent on the A/OPC and AO to act on the information that OMC points out. As long as a command properly uses the tools provided through these two resources and acts on the exceptions when they are identified, effective monitoring will be present.

8. Lack of Level Three Data Under the Current System

Under the current DoD purchase card program there is no way to capture Level III purchase data (the current program uses Level I data, which shows the date of purchase, the amount, and the location). Level III data allows the A/OPC, AO, and cardholders to see exactly what items were purchased on the monthly statements. Currently, the A/OPC and AO can only see where the cardholder made the purchase, on what date, and how much was spent. With Level III data, it will be easier for the A/OPC and AO to detect fraud and misuse.

In addition to detecting fraud and misuse, there is another problem created due to the lack of Level III data. The DLA Purchase Card Manager stated that his agency does not currently maximize its purchasing dollars as well as it could. (Conneen, 11 September 2003) Many purchasers are buying the same commodities using different

methods. For example, some purchasers may use a credit card, while others use a GSA schedule, and still others will write a contract to purchase the same commodity. Some commands do not even have a standard policy on how to make purchases. Using single vendors could save a large amount of money. The purchasing system would be much more efficient if there were contractual vehicles in place that all cardholders could use to make similar purchases, i.e., one source for one commodity. Level III data would help purchasing agents at DLA to determine what items their many different customers are purchasing. Thus, the purchasing agents would then be able consolidate all of the demand data and get better pricing when writing a contract for the demanded commodity through bulk purchasing. These savings would then be passed down to the DLA customer in the form of lower pricing. (Conneen, 11 September 2003)

OMC incorporates Level III data into the purchase card program. The Purchase Reconciliation System uses the Level III data to alert the AO of any actions that warrant further review based on parameters set in the program through regulation and A/OPC guidelines. As a result, the chance of fraud or misuse going undetected is greatly reduced under the OMC program. In addition with the use of OMC Level III data, purchasing agents will be able to consolidate demand and set up central contracts, passing savings on to the customers.

9. How to Increase the Usage of Purchase Cards in OMC

"Our primary goal in terms of e-business is to take out administrative costs...we do have a catalog ordering system for strategically sourced supplier agreements. It has 30,000 users and is still growing. We [United States Postal Service Procurement Office] do realize that with a user base that size, you can't just encourage e-use – you really have to drive it and we hope to do more in that regard." (Strange, p. 3) With OMC being introduced as an e-business resource, the relationship between the database and the purchase card is one in which the purchase card is an enabler, a tool that a customer can use to make the process easier.

A survey conducted in commercial businesses found that "the number of purchasing organizations buying and experimenting with online sourcing and procurement tools is growing, but the actual amount of spending being put through online

tools has remained relatively flat..." (Hannon, p. 49) Thirty-three of the companies surveyed used online marketplaces, twice as many as 2002 while 45% of those surveyed felt that they had the skills to make the best use of internet purchases, a decline from 57% in 2002. (Hannon, p. 49) Based on this survey, an assumption can be made that an effective and efficient enabler, such as the purchase card, will increase the use of OMC as a purchasing tool.

OMC can be seen as an Enterprise Resource Planning System, meaning that the ultimate goal is for a customer to make all simplified purchases using OMC. The purchase card is a legacy system with which a majority of DoD agencies have a high comfort level. Therefore, OMC can only increase its opportunity for success if it uses this legacy system. Based on current observation though, this does not seem to be the case. The use of the credit card needs to be pushed. Thomas Graham, Networld Chief Operating Officer, states that test sites currently using OMC make 10 -15% of their purchases using the credit card. The remainder use fund cites as a method of payment. Networld would prefer using the credit card because they would receive their payments quicker. (Graham, 2 October 2003) Networld needs to have a pilot program conducted that focuses on the purchase card so commands can see the benefits and spread the word. Once the system has been proven, the amount of credit card purchases through OMC should increase.

Challenges facing OMC include acceptance of the product by the contracting community as well as political issues in the government, for example, higher-level officials pushing for different software or focusing the budget on other issues. On the other hand, an advantage provided by OMC with regards to the relationship between Government and contractor revolves around the requirements of recognizing Small Business entities. "The existence of a web-based system, with all suppliers providing their information and the Government having instant access to that information, provides far greater options to the government buyer, as well as providing higher visibility and fairness to the process. In fact, it has even been found that these shifts yield a larger share of the business going to the smaller, innovative firms." (Gansler, p. 12) OMC can be the web-based system of choice for the DoD purchase card program.

G. OVERSEAS USAGE

1. Contingency Environment

A contingency contracting officer faces many challenges while setting up and working in an immature environment during a humanitarian assistance or post hostilities mission, especially overseas. LCDR Harold Valentine, COMLOGRON 2, returned from serving as an Officer in Charge of a Special Boat Unit in Baghdad, Iraq supporting Operation Iraqi Freedom. Working for the Office of Reconstruction and Humanitarian Assistance (ORHA), his duties also called for him to be the Contracting Officer and AO of the purchase card program. He had two cardholders with a $300K limit per purchase and a $2.5 million monthly limit. It also helps that DoD recently raised the "micro-purchase threshold from $2,500 to $25,000 for commercial purchases of supplies or services made outside the United States. The majority of task force level requirements fall under the $25,000 micro-purchase limit" (Womack, 4). LCDR Valentine's APC operated out of the Pentagon in Washington, D.C., limiting the ability to communicate effectively. A system such as OMC would have allowed LCDR Valentine to manage his program more effectively, while still providing the necessary information and reports to the A/OPC back in Washington.

Other challenges he faced with regards to using the purchase card ranged from having appropriate hardware and software on-line to being forced to purchase products made in the U.S. due to the Buy American Act. Hardware and software issues included having a computer available, issuing IP addresses, having the appropriate bandwidth and having limited access to satellite fixes, which made getting on line very difficult at times. In this case, there was a 50 percent failure rate. LCDR Valentine observed the need for three essential items to have in the contingency environment: a laptop, cell phone and Internet access. Other essential items include the FAR, required forms and other regulations and guidelines installed onto the cardholder's laptop as well as other items mentioned in the contingency contracting support kit mentioned in Appendix F.

Other problems centered on outside agency policies. For example, Army and Air Force policy regarding the requirements for a cardholder are more stringent than the Navy's. Since the contracting officer and his cardholders were working in an Army

AOR, cardholders were required to have a warrant. If it were a Navy lead contingency contracting structure, the A/OPC could issue a card to a person who has completed the required credit card training. This was the main reason that LCDR Valentine had only two cardholders limiting his team's flexibility. (Valentine, 11 September 2003)

Receiving the purchased items from orders placed in the U.S. is a problem in this environment. Less than 50% of the items ordered outside the local economy were received on time, in the right quantity or the correct specifications. Considering that over 90% of the items purchased were from local vendors, this situation can be tolerated to a certain extent. One reason for this problem included the delays due to customs inspections, especially when purchasing from a prime vendor. (Valentine, 11 September 2003) Recommendations to customs issues are mentioned in Chapter 2.

Currently, a majority of purchase card transactions in the contingency environment revolve around material buys, while services are purchased using different methods. OMC will benefit the contingency contracting officer since it can provide one stop shopping fulfilling requirements, including services, expeditiously.

2. Operating in a Mature Environment

In a mature environment, personnel and administrative support elements are in place and programs are run out of offices either at a forward military base or a contracting center in the region. For example, Naval Regional Contracting Center, Naples is the regional purchase card manager for the European theater and "can assist in those instances where the only known source does not accept credit cards" and assists commands in establishing the purchase card program (NRCC web page). NRCC Naples also provides guidance, instructions, training and conferences to units with a program in place. In general, the purchase card program is operated, as it would be in the United States, in accordance with guidelines and regulations promulgated by DoD and service agency offices. Differences focus on limited availability of vendors who accept the purchase card, currency exchange rate differences (explained below) and limited or different technological tools.

Remote sustained sites are becoming more common, especially over the last 10 years. In Operation Iraqi Freedom, a "contract cell" provides base support for Camp Doha in Kuwait. DCMA has contracting personnel assisting with purchasing other contract administration duties. The "contract cell" assists the contingency contracting officer with purchase card buys and other issues. They can use OMC to increase support to the contingency contracting officer without facing the barriers of limited Internet access and bandwidth.

3. Currency Exchange Rate (CER)

Currency exchange rate problems in both the mature and contingency environments can be a common occurrence without proper management by the A/OPC and AO. The purchase card manager in Europe states that "due to daily differences in the rate of exchange a cardholder could potentially exceed his/her authority when obligating at the CER, because when the charge hits Citibank, the CER could have changed and we're charged at the rate the bank uses. For example, a cardholder with micro-purchase authority makes a local purchase in local currency for the equivalent of $2,490. By the time the transaction is posted at the bank, the CER could have changed in favor of the local currency and the amount gets posted as $2,515. Technically, the cardholder has exceeded his/her authority.

Over the past year there has been a significant change in the CER; the U. S. Dollar has gone from $1 = EUR1.16 last year to $1 = EUR0.88. The day-to-day changes are not that significant. Most of our activities do not have the authority to use other methods of purchase. Some activities here have limited cardholder's to $2,400 per transaction; others have trained their cardholder's to be careful when obligating at close to their single transaction limit. Sometimes they reduce quantities to ensure they don't exceed their authority." (Harris, 16 Sep 2003) This problem and the OMC solution are further explained in the next section.

4. Bank Transaction Lead Time

The lead-time between the actual time that the transaction occurs using the purchase card and the time that the transaction is processed for payment is greater in Europe due to the method of transferring funds. Transactions in the U.S. use electronic funds transfer (EFT), and the entire process is completed in one day. In Europe, funds

are transferred by wire, adding 2 - 3 days (and potentially more) to the process time. The CER could fluctuate at a greater than normal rate during this period, magnifying the problems described in the previous section. Networld's solution is described in the following statement:

"DFAS Kaiserslautern is the office we deal with in Germany and they have a 'Fluctuation Account' that protects the DOD customer's budget from the daily fluctuations in the 'in country currency.' For example the current EURO rate is about '0.89 Euro' for every U.S. Dollar. However, the rate that (DFAS) Kaiserslautern pays the DOD customer is '1.14 Euro' for every U.S. Dollar. They do it this way because the DoD Code budgets a certain amount for expenditures in Europe and other OCONUS locations on an annual basis. With fluctuating currencies worldwide, there could be no certainty that those budgets would hold against a volatile currency especially if the dollar is in a negative position vis-à-vis that currency. To address this issue and to work seamlessly with DFAS, we work with major U.S. Banks including Citibank to provide us accounts and corresponding banks in all countries and in all local currencies that the U.S. Government does business and that impact DFAS. For example, we have the capability to do contracts with local vendors in every country that DFAS Kaiserslautern handles. That includes 29 countries in Europe and North Africa. By doing it this way, there is no issue with fluctuation regarding how we pay local vendors as we book the contract in the local currency and pay in the local currency using DFAS' fluctuation account as the benchmark. As we have a 'Merchant Bank' that does business globally and as we track to a fund cite that is supported by the DFAS fluctuation account, the only time we would have a problem is if we tried to move funds out of the transaction before we get paid by DFAS and before we pay the vendor." (Graham, 27 Oct 2003)

5. Value Added Tax (VAT)

Another issue that is presented overseas is the VAT that some European countries place on all purchases (Italy uses a similar tax called the IVA tax). "VAT is a general consumption tax assessed on the value added to goods and services." (EURUNION webpage, p.1) VAT rates range from 15% to 25%, depending on the country. (EURUNION webpage, p.1) Since it is DoD policy to "secure, to the maximum extent

practicable, effective relief from all foreign taxes including when the purchase card is used to purchase supplies and services for official Government use", DoD units are exempt from the VAT with the proper documentation. (NRCC webpage) Networld and their sub-contractors, based on the current process, are not. So when a purchase is made using OMC, Networld and the sub-contractors make the payments using the credit card and pay the applicable VAT rate. Networld reimburses the sub-contractor.

"VAT is one of those things like death and taxes; it's all in the interpretation. DoD is exempt from VAT, as it has SOFAs with most European Countries where U.S. Forces operate that exempts those forces from VAT. Consequently, the Contractor doing business directly with the DoD in country would not have to pay VAT, however, as that Contractor does business with a sub-contractor, they incur a 'VAT event', meaning there is a VAT payment due to the sub as the sub has to collect and pay VAT since the prime contractor is not the U.S. Government. Even though the U.S Government is the final buyer, the prime has to pay VAT to the sub-contractor and recover that VAT payment from the German Government. In other words, there is a cash flow issue where we pay VAT and recover it after 30-40 days. In the last year working in Germany, we've become 'experts' at the implications of VAT as we do business with the Army there. Another wrinkle that we haven't faced yet is that not all U.S. Government transactions overseas are exempt from VAT. In some countries, only those involving the Department of Defense are." (Graham, 27 Oct 2003) There are currently no tools in place to remove or reduce the amount of VAT for U.S. commercial entities operating in Europe.

H. RECOMMENDATIONS

1. Introduction

The DoD assigned a task force to review the current status of the purchase card program and their final report, dated 27 July 2002, provided a list of problems and recommendations. A year prior to the report "the Department took a number of actions to strengthen the purchase card program. The impact of these actions was reviewed by the Task Force in its evaluation of the current state of the program. The Director, Defense Procurement and Program Manager, Purchase Cards, has directed a number of actions to strengthen the purchase card program. These include:

- Establishing a limit for the span of control of approving officials of one approving official for every seven cardholders.
- Instructing the Defense Components to minimize risk by establishing reasonable spending limits on card accounts.
- Reiterating the requirement to tailor each card so that merchant category codes that are not needed or inappropriate are blocked.
- Expanding a joint fraud detection and prevention program to cover Purchase Card transactions.
- Reiterating the need to provide installation purchase card program coordinators appropriate resources to allow them to discharge their duties.
- Expanding audit coverage and requesting the Inspector General of the Department of Defense (IG DoD) to become the focal point for all DoD purchase card related audits." (DoD Task Force, p. 2-7)

At a lower level, each Service has acted on its own taken a number of actions, for example:

- The Army has issued a policy memorandum on Internal controls in response to GAO/IG DoD queries.
- The Army is working on the Army Standard Operating Procedure (SOP) to incorporate IG DoD/GAO recommendations on strengthening the management controls, and systemic issues found.
- Army Major Commands (MACOMs) and installations are aggressively reviewing policies and procedures to address account limits, blocking of cards and reviewing transaction declines. Policy has been issued directing that all accounts not active for at least 4 to 5 billing cycles must be cancelled.
- The Navy issued a message on August 31, 2001, emphasizing accountability at all levels of the program. It also directed a Purchase Card Stand-down day, during which training on policy and procedures and the potential for fraud, misuse and abuse were emphasized.

- The Navy directed the suspension of cards for any cardholder who lacks documented evidence that the training required by the August 31, 2001, message was completed.
- The Navy mandated on April 15, 2002, that every Department of the Navy activity conduct a current audit of its purchase card program to confirm the adequacy of procedures and controls and have the results reviewed/validated by higher authority.
- The Air Force has re-emphasized the need: 1) for systematic surveillance and fraud detection activities, 2) for appropriate discipline for violators of purchase card rules and regulations, and 3) for informing base leadership of the health of the purchase card program on their installations.
- The Air Force Logistics Management Agency will soon publish a reference guide for agency program coordinators
- The Air Force is in the process of revising its instructions on the purchase card to strengthen internal controls and address findings from a recent Air Force-wide audit of its purchase card program." (DoD Task Force, p. 2-8)

OMC has studied the Task Force recommendations and offers a tool to help commands incorporate these into daily practice. The Order-Management Website and Purchase Reconciliation System provide the means to accomplish this task. If OMC is implemented for the purchase card program, it can prove to be a valuable managerial tool when A/OPCs and AOs use it properly to manage their programs.

2. OMC as a Centralization Tool

Centralization of the purchase card program can occur along different levels. At the executive level, "the DoD Purchase Card Joint Program Management Office (PMO) was established within the Army as the executive agent for DoD purchase cards and as such, reports directly to the Director, Defense Procurement. It developed and deployed a standard DoD-wide card management and reconciliation system for DoD. The PMO's on-going responsibilities include promoting purchase card use, coordinating contract requirements with the GSA, managing delinquencies, developing and recommending policy changes resulting from internal control weaknesses identified by audit communities, and developing DoD-wide training programs" (DoD Charge Card

Final Report). PMOs can use the tools offered by OMC to help implement policy and training requirements DoD-wide.

OMC can provide assistance to commands at the local level dealing with reduced manpower and resources, which inhibits a command's ability to effectively manage a purchase card program. One solution is to consolidate the purchase card programs in a certain region or a common chain of command to a central contracting activity. This has been an effective tool as noted by the manager below:

"My last job was at FISC Puget Sound. I ran two branches: a Simplified Acquisition Procurement (SAP) branch and a credit card branch. The credit card branch was created using reimbursable money to the FISC because several big commands TRF, SWFPAC, and COMSUBPAC did not want their people buying for them, nor did they want the management oversight. The FISC paid for the oversight and APC out of their mission-funded budget... Our credit card branch processed over 1800 requisitions per month (sometimes more) and streamlined purchasing to a highly efficient point with only 5 GS 5-7 buyers. We had a 1-2 day turnaround for high priority and a no more than 4-day turnaround for normal priority buys. I also used the credit card as a payment method and it was a superb management tool. I can't tell you how many times, I soothed ruffled feathers by doing a quick mod to pay someone via credit card when DFAS bureaucracy wouldn't pay. Also, I used the credit card as a payment method on any and every SAP purchase that we could. We did SAP for the entire region, which included 7 ships, Bremerton, Whidbey, Bangor, TRF, SWFPAC, Everett and many cats and dogs in the region. You can use the credit card as a method of payment no matter who holds the card. It's very simple. You put a clause in the contract saying to the vendor, roughly, 'contact so and so customer when you ship the material and they will pay you via their purchase card.' You put the cardholder and their phone number on the contract. There is no dollar limit up to some odd million (can't remember since I never got close and it's been a while). The card number is never revealed until the vendor shows the customer proof of shipment. Our ships in the PNW (Pacific North West) frequently avoided the DFAS hassle this way. However, no matter how good the program is, it always comes down to the management of the credit card. I believe the end user should have the credit

card. There are some cases when they don't want it and that's where the FISC customer service comes in. No matter who holds the card, the management must still be there. No oversight, no integrity, then, you have disaster." (Ebright, 12 September 2002)

Another manager discusses both the advantages and disadvantages of centralizing the purchase card program:

"In my days as SUBLOGSUPPCEN Det. P.H. Ops officer I can say that credit cards can be both benefit and bane. We ran a small purchase (credit card) support branch for the twenty-four Subs that were home ported out of Pearl Harbor (95-98). SUBPAC, at that time, wanted control of the cards at a SUBSAT level so none of the boats had their own and even COMSUBPAC used our buyers from time to time. We had three buyers; two Civilian GS-5s and an E4/E5 (rotated twice while I was there), and processed between 300 to 800 buys each month. For several reasons this was a good way of doing business:

- We were the invoice address so the boats didn't have to worry about being underway and not being able to process their statements
- Overall work load reduction for the boats (still a big issue, especially with 'smart ship' on its way); although it did involve some shuffling between the boat and the FISC where we were located. We took care of a large management issue for them
- The DET OIC and I were APCs so we not only reduced the boats workload we also had a standard method of reviewing the documentation and invoices
- Centralized the buying so our personnel were very familiar with local sources
- Unauthorized commitments, although still present, were few in number, about three a year

Problems with this method:

- If the buyers are tied to the SUBSAT or other support organization (e.g. FISC) they cannot leave with the card to conduct business (i.e. at that time the card was still fairly new, so some of the local business wanted an imprint of the cards numbers, we

had to cancel a few requisitions because business would not take our word that it was 'a valid card')

- Of the few unauthorized commitments that did occur, we had to process them through the P.H. FISC CO which seemed to take longer than those commands who had their own cards (we being a third party had to interview all the concerned parties and that sometimes took a while due to underway schedules)
- Some of the Boat Chops hated having to come to us to process their buys (of course they didn't miss the paper work)
- Depending on the Boat, it was sometimes difficult to reconcile receipts (or to even receive them) with their invoices (poor management of receipt file)
- Our buyers were generally busy and end of the year spending normally swamped them." (Csorba, 12 September 2002)

OMC can act as a force multiplier for the central contracting activity allowing them to take on additional customers while maintaining high quality service levels to all customers.

3. Implement a Pilot Program Focusing On the Purchase Card Tools in OMC

To date, there has not been a focused Pilot Program for the Purchase Card program. The optimal solution calls for combining the functions of OMC with the DoD purchase card program, since OMC has incorporated the tools that would enable the A/OPC to manage his program more effectively including Level III data, the Order-Management website, and the Purchase Reconciliation System. This would entail a number of steps that each of the services would have to place in motion in order to succeed.

The first step would include awarding a single DoD-wide contract for the purchase card program that incorporates the OMC software. The next step calls for the update of all purchase card regulations and guidance, specifying the auditing and reconciliation tools from the OMC software. The third step requires that all agencies and commands with the purchase card program in place or in the process of adopting the

program train all cardholders and A/OPCs. Finally, the A/OPCs would order new cards and have the new and improved program in place. The biggest constraint in this process centers on the amount of time needed to implement this program. On the other hand, the benefits gained from this outweigh the costs and addresses all of the weaknesses noted including the currency exchange issue and VAT for overseas commands.

Networld is in the process of implementing a pilot program for OMC at Camp Pendleton that will incorporate the purchase card to test the effectiveness and weaknesses of the program. "We're currently working out all the details regarding the test there and we are hoping that the test will involve all aspects of OMC, including Credit Cards. We don't have the final Project Plan in place yet, however, we're working on it. I would anticipate that as soon as we're finished with the Camp Pendleton Pilot, we will implement across DoD." (Graham, 3 Nov 2003) Initiating a pilot program, especially with the purchase card as the main method of procurement, allows OMC and DoD to see the effects of the program on that agency, and to see if it can be adapted and transferred to DoD, "i.e. ensuring that DoD changes in a way that allows it to benefit from the Best Commercial Practices (BCP)." A pilot program allows DoD to "refrain from introducing BCP's too close to its core combat-related activities so that any failures will have no more than limited effects on DoD…" (Camm, p. 226 – 227)

The Pilot Program is described below with portions of the Statement of Work documents from Networld:

The proposed prototype uses an Order-Management Website and a Purchase Reconciliation System as described earlier. The system as a whole aids in compliant purchasing and detection of fraud, waste and abuse. The Order-Management Website enforces existing Purchase Card procedures to restrain problem purchases before the fact. The Purchase Reconciliation System is the deterrent arm, and automatically sifts through monthly statements, creating reports on suspect purchases.

The prototype as configured consists of three unique parts: The Order-Management Website, providing purchase-authorization workflow tools; a Reverse Auction; and a back-end Purchase Reconciliation System designed to ease the burden on

Agency Program Coordinators and Approving Officers. Business rules used by the Order-Management Website filter procurement data to deny incorrect use of the Purchase Card. Purchases that pass these rules are automatically recorded in the Purchase Card Log. Cardholders wishing to make purchases outside the storefront may seek pre-approval using a form provided on the storefront. After approval is secured and the purchase completed, the purchaser manually enters purchase data on the Log.

The Purchase Reconciliation System is a custom integration process for monthly Purchase Card statements, automated analysis of that data and exception reports about cardholders who violate Purchase Card regulations. The Purchase Reconciliation System filters monthly bank statements by comparing actual purchases to those recorded in the Purchase Card Log, creating an exception report indicating possible fraudulent, wasteful and abusive purchases. The reconciliation system should have a strong deterrent effect against would-be violators.

The prototype improves the current Purchase Card environment in the following general ways:

- Facilitates compliant purchasing and competitive pricing
- Lightens workload for cardholders who purchase through the storefront
- Enforces existing procedures while adding a verification element
- Enables automated detection of fraudulent, wasteful and abusive procurement
- Employs artificial intelligence to improve business rules
- Records data required for control of the environment

In addition, the prototype provides product menus that have been pre-filtered for unauthorized products. These menus integrate FAR-compliant sources, displaying FAR-compliant products at the top of the product list in each category, with special icons to emphasize the source. The system automatically replaces product catalogs at regular intervals specified by each supplier.

Proposed website storefronts present commodity-specific product menus to individual purchasing activities. In addition, storefronts also provide portals to

participating retail sources of supply, and host essential forms intended to capture purchase information, route approval and provide a framework for subsequent purchase auditing. Storefronts also host a Receipt Capture utility for physical scanning of receipts.

a. Specifications for Order-Management Website and Key Elements of Concept

The proposed system is configured to enforce all existing Purchase Card rules by implementing business rules functionality and scalability using the framework architecture developed by Networld. In addition, the website is configured for ease of use by the average Purchase Card holder and restrict access to unauthorized users. This system interfaces with the Maintenance Activity and Cost Tracking System (MACTS) to allow for integrated financial data flow. Following is a listing of key elements to the system.

- Access to site (username and password) only given after training completed. User activity on the website is tracked automatically by username, password and training certification number. The access to this system is through MACTS.
- Online "home", or record keeping database tool for Purchase Card activity
- Automated analysis of procurement data against Purchase Card restrictions and routing of the data for quick mass approval or detailed inspection of irregularities
- Artificial intelligence analyzes patterns in purchase approvals and denials, and suggests new business rules for decision-makers.
- Website provides forms for recording the following: User Authorization, Need Justification, Purchase Card Log, Open-Market Approval, Accountable Items, Problem Transactions and Program Reviews.
- Website provides portal to participating retail sources.
- Website provides for secondary approval enabled for single or multiple off-website (Open Market) procurement. Configured functionality allows approval to take place before or after purchase. Optimal effectiveness of approach requires that after-purchase approvals take place within a reasonable period after purchase, e.g., three to seven days.

- Website allows procurement using normal Navy supply channels. Integration processes filter through existing supply data to create commodity-specific product menus and larger DoD product catalogs.
- Website allows user-configurable "shopping lists" of products
- Catalog integration processes eliminate products not authorized for Purchase Card procurement.
- Products supplied by preferred providers (National Industries for the Blind, Federal Prison Industries, GSA) receive priority display in each product category, along with a special icon emphasizing the source.

b. Secondary Approval for Open-Market Purchases

Definition: For the purposes of this initiative, an Open-Market purchase is one of the following:

- Walk-in buy at point of purchase (physical store)
- Online purchase
- Mail-order purchase
- Telephone purchase
- Other credit card transaction

The system enables a user to secure secondary approval for an Open-Market buy. The user accomplishes this by completing an online form and presenting it electronically or in person to the approving authority. Approvals are then recorded on the storefront automatically. Approving Officers may use these Pre-Approval forms as a secondary tool when investigating listings on the Exception Report. On occasion, a compliant user might forget to make the manual entry to the Purchase Card Log after an Open Market Purchase, in which case this transaction would appear on the Exception Report. Having a recorded Pre-Approval for the transaction allows the Approving Officer to recognize the oversight and enforce the appropriate level of discipline for the offense. In addition, secondary approval fosters communication between the cardholder

and Approving Officer about planned purchases, and serves as a permanent record-keeping tool for those communications.

c. Business Rules

As mentioned earlier, the Order-Management Website embodies current restrictions on Purchase Card use, including, but not limited to, the following:

- Single-purchase limit by cardholder
- Splitting procurements to defeat $2,500 micro-purchase limit
- Cardholder purchases against non-authorized Merchant Category Code.
- Unauthorized transaction types by cardholder (OTC, telephone, fax, Internet)
- Special-item procurement (petroleum, HAZMAT, Foreign Military Sales)
- Pricing "reasonableness" check in relation to past "like" purchases
- List of prohibited/special attention items

d. Reverse Auction

Networld's prototype incorporates Reverse Auction functionality. However, this is not recommended for inclusion in the pilot program. The function appears to add a level of difficulty for the average cardholder and may be an area open to misuse. Further research should be done in this area before determination is made. Once the system is tested, perhaps this function can be added at a later date.

e. Portal to Retail Sources

In addition to all suppliers of choice, the website provides links to participating retail sources of goods and services commonly purchased by users of the Purchase Card program.

By employing cXML "PunchOut" technology, users are able to fill shopping carts on the supplier's website, and then bring requisition data back into the Order-Management Website, where it can be pushed through the Business Rules and recorded permanently in the storefront database. This capability depends upon the

participation of retailers, who must adopt a designated format for data exchange and allow remote shopping from another website.

f. Storefront Forms

The system provides at a minimum the following online forms to enable necessary tracking and controls in Purchase Card use. The system controls access to forms according to user permissions. Because the system is scalable, other forms may be added as necessary:

- *User Authorization*: Records who received training and when training was completed.
- *Need Justification*: Records rationale for purchase of "special-need" items.
- *FAR-8 Screening*: Records efforts to locate product or service from FAR-8 sources.
- *Purchase Card Log*: Records purchase details by cardholder.
- *Open-Market Approval*: Records reasoning for requesting an Open-Market purchase. Provides a feedback form for approving authority to state reasons for denial.
- *Accountable Items*: Records specific details about accountable items received.
- *Problem Transactions*: Records details of problem purchases and corrective actions.

g. Workflow Authorization and Automated Routing

The system analyzes purchase data entered by the user on the Open-Market Approval form, employing the restrictions described in the Business Rules. After analyzing the procurement data, the workflow engine routes the form to a decision-maker, marked for pre-approval or red-flagged for more detailed inspection. Artificial intelligence working in the background analyzes purchase decisions made over random and/or predetermined periods of time, and suggests new rules for approval or flagging. For example, if a particular cardholder's activity is repeatedly red-flagged, the system reports and asks: "Always red-flag purchases by Lt. John Doe?"

h. Catalog Integration and Product Menus

The system integrates catalogs from multiple sources of supply, including commercial vendors, FAR-8 preferred providers (NIB, NISH, FPI, GSA) and the Federal Supply Catalog. These catalogs are updated automatically on a periodic basis through back-end integration to the suppliers with the supplier's cooperation. Integration processes eliminate products not authorized for Purchase Card procurement. Product menus force priority in each product category listing the products supplied by FAR-8 preferred providers, and emphasize these products with a special icon and text. In addition, product menus are customizable by commodity (subsistence, aircraft parts, electronics) and by activity (Officer's Mess, Enlisted Mess, CPO Mess). Users may also configure their own "shopping lists" of products they purchase frequently, which is a significant timesaving feature.

i. Reports

The system supports greater accountability while easing the burden of Purchase Card Management by providing a variety of reports. Types of reports to be generated by the system include but are not limited to the following:

- Purchase Pre-Certification Report
- Purchase Exception Report
- Problem Transactions, with Corrective Actions taken
- Training, who received Purchase Card training, when
- Monthly Certifications by Cardholder and Approving Authority
- Receipt/Order/Purchase Reconciliation
- All purchases by Cardholder
- All purchases by Activity
- All purchases by Supplier
- Accountable Property Purchases

❖

j. Purchase Reconciliation System

The Purchase Reconciliation System is the back-end application that reconciles monthly Purchase Card statements with the purchase data entered through the Order-Management Website (Purchase Card Log). The Purchase Reconciliation System relies on Card Number, Amount, Vendor and Date to match the list of storefront-recorded purchases against the actual purchases shown in the monthly cardholder statement—a simple exception report by card number outputs all card numbers for which there are purchases but no matching data from the Purchase Card Log. A secondary exception report lists purchases made from unauthorized Merchant Category Codes. These reports allow Approving Officers to concentrate disciplinary measures on those card numbers and card users who purchase outside the system, and provide the preliminary data needed to discover problem users. The Purchase Reconciliation System depends upon cardholder statement information. (Networld Pilot SOW)

4. Contractor Purchasing Through OMC

Another possibility for increased savings to the Government is to allow contractor access to OMC. "Anyone who follows trends in government management knows that contracting is becoming an increasingly important way that government gets its work done. A number of agencies, including Defense, Energy, and NASA, spend a majority, in some cases an overwhelming majority, of their budgets on contracted products and services. NASA spends 78 percent of its budget this way, while Energy spends 94 percent." (Kelman, p. 1) "Since the early 1990's, DoD has used contractors to meet many of its logistical and operational support needs during combat operations, peacekeeping missions, and humanitarian assistance missions, ranging from Somalia and Haiti to Bosnia, Kosovo and Afghanistan." (Military Operations, p. 4) With the growing number of contractors working on government projects and the decrease of the Acquisition Workforce in Government, the contractors should have the option of purchasing items to support the contract through OMC taking advantage of preferred government pricing. This works by having a contracting tool in place that allows the contractor to make purchases using a credit card and the OMC software and including the

charges on the contract or requesting for a reimbursement. The key to this is based on the type of relationship that the agency has with the contractor. Ergo, is it an arm's length relationship based on trust and with both parties working toward similar goals? "The technical functionality is there to create sub-contractor (contractor) economy of scale, however, politically, this may be problematic. The way I see this working is that as we save money for the contractors, those savings will be passed on to the Government client as well, this documented return on investment would add to the Government's purpose as well." (Graham, 3 November 2003)

To further illustrate the benefit of having contractors using OMC as a tool for purchasing, there were over 3300 purchases with a value of over $47 million made by Kellogg Brown and Root (KBR) in support of OIF from March through May 2003. A majority of the purchases used a seven step process that extended the procurement cycle time unnecessarily. (Valentine, 11 September 2003) If KBR is allowed to use a purchase card to procure small value items and peripheral items for use on larger contracts through OMC, it will reduce the procurement cycle time considerably and save the Government money.

I. CHAPTER CONCLUSION

With the increased attention on fraud and abuse cases with users of the purchase card in DoD, the natural inclination for Congress, DoD, and agencies is to place more controls over the process in general. This has been the case throughout the history of the United States. During the Revolutionary War, Congress "wished to improve control of supplies and thereby strengthen the army while protecting the public purse. Control and protection were apparently visible to Congress in records." (Middlekauf, p. 515) The current DoD wide push for "transformation" and the movement towards e-commerce has created a perfect opportunity for an enabler like OMC to step up and provide the tools and resources available for the A/OPC to implement a purchase card program that helps him manage the program efficiently and in accordance with regulations. The short run consequences would emphasize more oversight by agencies such as GAO, as currently the case with SPAWAR (they are currently audited every quarter), but as the concept of OMC's control mechanisms become integral parts of every A/OPC, AO or card-user's

routine, the long term benefits would take hold. The focus would shift from the A/OPC and AO spending needless hours worrying about fraud and abuse to servicing the customer and ensuring, for example, that the statement of work is well defined, other alternatives are considered because of better quality or price, and the product or service is delivered on time and in accordance with the customer's request.

This chapter has outlined the history of the credit card program including the strengths and weaknesses of the current program. The developers of OMC have focused on the problems with the program pointed out by GAO audits to construct a one-stop solution. The goal of the one-stop solution is to provide superior automated management tools so the A/OPC and AO can effectively monitor their programs. The OMC acts as a detector and deterrent of fraud and misuse of the purchase card. A second goal of OMC is to provide a standard system agency-wide so that all commands are working with the same system. With all agencies working under one system, large economies of scale can be realized. Finally, we re-emphasize the importance of running a purchase card focused pilot program to test the potential benefits of OMC prior to making any decisions about agency-wide implementation. Future studies should be conducted at NPS to evaluate the effectiveness of any purchase card pilot programs conducted.

IV. INTERNET SECURITY

A. INTRODUCTION

Networld Exchange Incorporated (Networld) is providing the implementation and management of an Electronic Storefront, which uses the Internet for ordering, delivery, tracking and billing of commercial supplies and services ordered through the Storefront. The Storefront is known as the Open Market Corridor (OMC).

Online tools are a tremendous resource, and to maximize their value simple precautions to protect against security breaches must be addressed for both the OMC network and e-mail access. Three areas require evaluation: Internet connection, The E-mail system, and the web site.

1. Internet Connection

Networld has an "always-on" Internet connection thru T1 lines and other high-speed access, which make it vulnerable to intruders. These vulnerabilities go beyond simple firewall software.

2. E-mail System

Security is not a concern for the vast majority of people sending e-mail. Its common use encourages most people to send a variety of documents without concern for security. Hijacking of e-mails or information in attachments is considered rare, but could potentially prove very valuable to terrorist monitoring troop spending to determine their next deployment area and schedule. Typing the correct address and using encryption software such as Pretty Good Privacy (PGP) can provide basic security for email. Networld does not currently employ encryption protect on their emailed documents.

3. Web Site

As host of the OMC, Networld should insure that measures are in place to thwart security breaches from outside and inside its organization. Networld uses database tier residing on Dell 6450 four-processor servers running Windows 2000 Advanced Server and Microsoft SQL Server 2000, each configured with 2 gigabytes (GB) of RAM. Over

60,000 of these servers have been a target of attack for several big worms and viruses this year alone. (Mercury News, 8/11/03)

Areas to be focused on in the Information Technology (IT) section are:

- IT Security Management
- Internal and External Security Procedures

B. IT SECURITY MANAGEMENT

Secure IT management and operations are the primary line of defense available to Networld to protect themselves from threats to their operating systems and servers. IT management can be broken down into four critical categories:

1. Security Patch Management
2. Operating System and Application Hardening
3. Proactive Virus Detection
4. Intrusion Detection

Each is part of an effective defense in-depth strategy that is required to reduce Networld's exposure to computer crime today. Viruses and worms such as Klez, Nimda, Sobig, Code Red, and SQL Slammer targeted Networld's servers. It is difficult to quantify the cost of security breaches because Networld would not report these attacks. However, the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) performed an annual computer crime and security survey that tallied more than $201 million in quantified financial losses in 2002. Among respondents, the most frequently cited forms of attack were viruses (82 percent) and insider abuse of network access (80 percent). Theft of proprietary information caused the greatest financial loss, with an average reported loss of $2.7 million. (CSI/FBI, 8/29/03)

The consequences of these attacks on Networld could be severe, resulting in damaged data and assets, business interruption, and infiltration and access to confidential and classified resources. After a computer is infiltrated, applying the security patch is no longer a sufficient remedy to guarantee its security. A successful recovery from an attack may require the complete reinstallation of every compromised asset. These

vulnerabilities also provide opportunities for attackers to compromise information and assets by denying access to valid users, enabling escalated privileges, and exposing data to unauthorized viewing and tampering. All of this could lead to a breach of corporate security and the resulting loss of credibility with customers, partners, Federal and State governments.

1. Security Patch Management

The term patch management describes the tools, utilities, and processes for keeping computers up to date with new software updates that are developed after a software product is released. Security patch management describes patch management with a focus on reducing security vulnerabilities.

Proactive security patch management is a requirement for keeping your technology environment secure and reliable. Microsoft issued several security patches for the servers utilized by Networld. The following is the security bulletin released by Microsoft July 2002 (Microsoft, 10/15/03):

- Who should read this bulletin: System administrators using Microsoft® SQL Server 2000.
- Impact of vulnerability: Three vulnerabilities, the most serious of which could enable an attacker to gain control over an affected server.
- Maximum Severity Rating: Critical
- Recommendation: System administrators should install the patch immediately.

As part of maintaining a secure environment, Networld should have a process for identifying security vulnerabilities and responding quickly. This involves applying software updates, configuration changes, and countermeasures to eliminate vulnerabilities from the environment and mitigate the risk of computers being attacked. The nature of many attacks requires only a single vulnerable computer on Networld's network, so this process should be as comprehensive as possible. Microsoft has established a handbook with detailed steps to set up security patch management procedures. Figure 20 gives an overview of the steps to be taken (Microsoft 2/28/03).

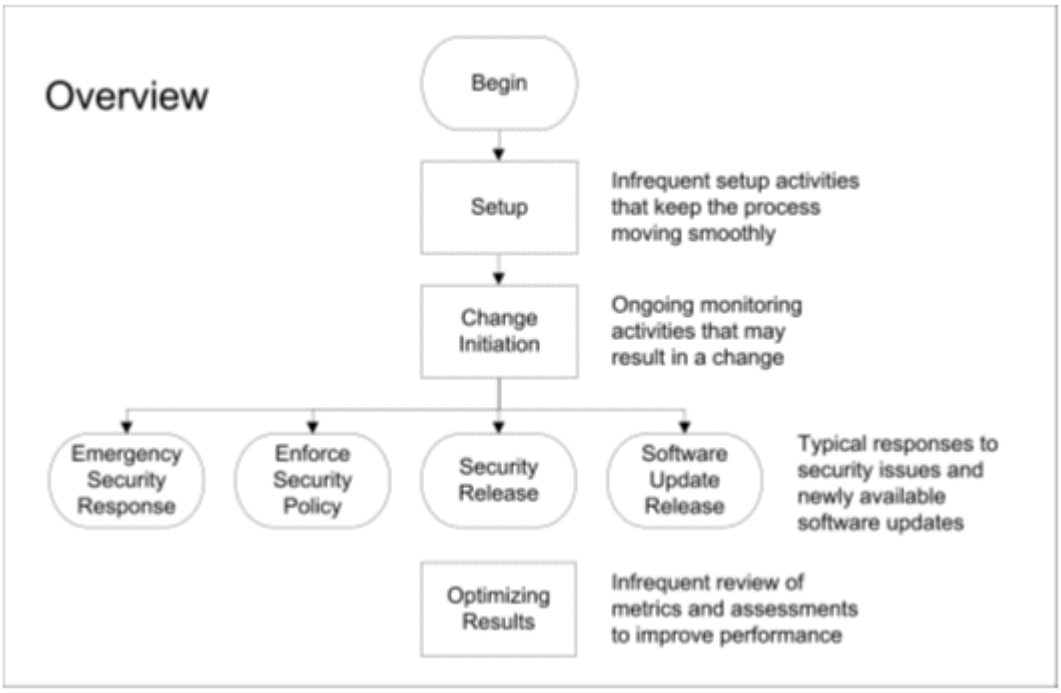


Figure 20. Security Patch Management Procedures (From Microsoft Exchange Server Security Bulletin Summary for October; Version 1.0 Released October 15, 2003)

The Setup stage is for infrequent activities that are required to support effective security patch management, such as taking inventory and base lining the environment, subscribing to security alerts, establishing security reporting to assist with issue identification, and configuring and maintaining the patch management infrastructure.

Change initiation is an ongoing monitoring process that is used to identify any security issues that should be resolved by changing the production environment. This includes reviewing several sources of information and reports to identify new software updates and security issues, determining their relevance, quarantining new software updates for use in subsequent steps, and initiating a response to address the security issue. Table 5 shows when Microsoft acknowledged a known vulnerability and how long it took for an attacker to exploit that vulnerability:

Attack Name	**Date Publicly Discovered**	**MSRC Severity**	**MSRC Bulletin**	**MSRC Bulletin Date**	**Days Available Before Attack**
Trojan.Kaht	5-May-03	Critical	MS03-007	17-Mar-03	49
SQL Slammer	24-Jan-03	Critical	MS02-039	24-Jul-02	184

Klez-E	17-Jan-02	*	MS01-020	29-Mar-01	294
Nimda	18-Sept-01	*	MS00-078	17-Oct-00	336
Code Red	16-Jul-01	*	MS01-033	18-Jun-01	28

Table 5. Exploitation of Vulnerabilities (From Microsoft Exchange Server Security Bulletin Summary for October; Version 1.0 Released October 15, 2003)

Security release entails releasing a software update or related countermeasures response to a newly identified vulnerability. Performing a security release includes change management, release management (including testing), and review (including rollback, if necessary).

Enforcing security policy is a necessary response when previously addressed vulnerabilities recur in the environment. Recurring vulnerabilities are at increased risk of exploitation by viruses, worms, and attack tools that remotely scan computers for security weaknesses and published vulnerabilities.

Emergency security response prepares for and responds to attacks that exploit security vulnerabilities. The majority of successful attacks will come from the exploitation of only a few software vulnerabilities. This trend can be attributed to opportunistic attackers who take the easiest and most convenient routes, and exploit the best-known flaws by using the most effective and widely available attack tools. Attackers would count on Networld not fixing known problems and attack indiscriminately by scanning the Internet for vulnerable computers. Attackers do not generally find the original vulnerability, but instead find the code to exploit it.

The implementation of security patch management is best achieved when it is a consistent and integral part of an organization's standard operational processes. Networld does not currently have a dedicated managed system. Without operational consistency, a separate process for security patch management can increase the overall cost of ownership for OMC.

2. Operating System and Application Hardening

Bulletproof network operating systems do not exist, but there are some common-sense steps that Networld could take to make their operating system a less-attractive target:

- Identify and remove unused applications and services. The fewer components intruders can get their hands on, the better off Networld will be.
- Implement and enforce strong password policies. Remove or disable all unnecessary accounts. This includes immediately removing accounts when workers leave Networld.
- Limit the number of administrator accounts available, and make sure users and IT staff have only the privileges they need to do their jobs.
- Set account lockout policies to discourage password cracking.
- Remove unused file shares.
- Keep an eye out for new security patches and hot fixes.
- Log all user account and administrative task transactions. This is an extremely important step for forensics if Networld's operating system network does get hacked.
- Beware of espionage tactics. Make sure that no one gives out important security information such as administrator passwords without getting approval from managers.
- Keep a secure backup solution handy to restore all systems in case of emergency.

Networld will find applications are the most difficult parts of an IT infrastructure to secure because of their complexity and because they often need to accept input from a variety of users. Here are guidelines to lowering the risk of a system intrusion because of an application flaw:

- Assume all installed applications are flawed—do not rely on the security programmed into them.
- Physically remove from the system all applications not being used.

- Use firewalls, content filters and operating system (OS) user authentication features to restrict access to the application, and provide access only to those who absolutely must have it.
- Update all applications to the latest patches when security bulletins are released.
- Networld should internally develop applications that need to be reviewed for security weaknesses. Consider an external security review for critical applications. Networld has not used external security sources on the development of OMC (see Appendices A-C).

Externally facing Web applications are high-risk applications because they are a bridge between the outside world and OMC customer databases. Networld needs to code that can block or otherwise safely deal with all of the following hostile inputs: missing page parameters, parameters that are unusually long, parameters will nulls or hexadecimal encoding, parameters with Web browser script blocks (which are used to create server-side scripting attacks), and parameters with quotes and semicolons (likely attempts to send hostile SQL commands through to the database).

Networld has written applications in languages that run in virtual machines--such as Java, Visual Basic .Net or C# to provide an extra layer of security protection. Networld has not avoided C and C++, which make them susceptible to applications that allow buffer overflow attacks. (E-week, Mar 2002)

3. Proactive Virus Detection

There have been several widely publicized attacks and vulnerabilities related to Microsoft software. Networld has a proactive security patch management in place and has not been impacted by these attacks, because of information that Microsoft makes available in advance of an attack. The Nimda virus was the only attack that successfully penetrated Networld's email system.

To prepare for virus detection, it is essential to fully understand the importance of patch management for Networld systems and the technologies and skills to perform proactive virus detection management. Networld should assign teams and responsibilities to ensure patch management is carried out as part of normal operations.

There is no documentation that Networld is doing this. Successful virus detection and patch management is achieved through a combination of people, processes, and technology.

Networld could save money and time by utilizing DoD sponsored activities to do the groundwork for intrusion detection. The Information Assurance Technology Analysis Center (IATAC) is a DoD sponsored Information Analysis Center (IAC) that provides a central point of access for scientific and technical information (STINFO) regarding information assurance (IA) technologies, system vulnerabilities, research and development, and models and analyses. The overarching goal of the IAC is to aid in developing and implementing effective defenses against information warfare attacks. IATAC basic services include support for user inquiries, analysis, maintenance, and growth of the IA library; IA database operations; development of technical and state-of-the-art reports; and promotional awareness activities, such as newsletters, conferences, and symposia. Currently the IATAC Information Assurance Tools Database contains descriptions of many tools that Networld could use to detect non-physical intrusions into digital electronic components. It hosts information on intrusion detection, vulnerability analysis, and firewall software applications. Information is obtained from open sources, including direct communication with various agencies, organizations, and vendors (see Appendix B). The database currently provides information about forty-six intrusion detection tools. It includes commercial products, government-owned systems, and research products. The database is built by gathering as much "open source" data as possible, analyzing the data, and summarizing information to give a basic description and contact information for each intrusion detection tool included. The tools in this database are available for Networld to provide information regarding existing approaches to intrusion detection. These tools fall into one or more of the following five classes:

1. Anomaly Detection — anomaly detection techniques assume that all intrusive activities deviate from the norm. These tools typically establish a normal activity profile and then maintain a current activity profile of a system. When the two profiles vary by statistically significant amounts, an intrusion attempt is assumed.

2. Attack Detection — attack detection systems are based on the concept that attacks can be represented as a pattern or a "signature" so that even variations of the same attack can be detected. These systems maintain records or profiles of actions that resemble known bad behavior and identify actions on the system(s) that match the known bad behavior.

3. File Integrity Checking — these systems use a cryptographic mechanism to create a unique identifier for each file to be monitored. The identifiers are then stored for future use. The file integrity program is subsequently executed, either automatically or manually, and new unique identifiers are calculated. The integrity checker compares the new identifiers with the saved versions, and when a mismatch occurs, it notifies the operator or administrator that the file has been modified or deleted. The operator or administrator then determines whether the differences indicate intrusive activity.

4. Misuse Detection — these systems attempt to identify authorized users' misuse of computing resources. Such activity may include visiting unauthorized Internet sites, navigating around a system to areas that have been explicitly identified as "off-limits," or using an application for activity unrelated to work. Misuse detection systems typically rely on an administrator defining activity that is considered "misuse" through the use of configuration files. The information in the configuration files can then be compared with activity that occurs on the system; misuse is assumed when there is a match between the two. Misuse detection differs from attack detection in that the latter focuses on identifying active attacks against a system, whereas the former attempts to identify benign or intentional unauthorized system use.

5. System Monitoring Detection — this technique either uses available system statistics or generates its own statistical information. Statistics may be derived from various sources, such as central processing unit (CPU) usage, disk input/output (I/O), memory usage, user activity, and number of log-ins attempted. The statistics are sampled to determine a normal system usage profile and are continually updated to reflect the current system state. The current state is compared with the normal usage state, and

the intrusion detection system determines whether the actions that have changed the profile or state, constitute a potential intrusion. This classifies the differences among the tools. The methods listed below describe the data sources and activities used to detect intrusions. Methods used by one or more of the tools include the following (IAC, 2002):

a. Audit-Based Detection — an audit based detection system has two major components. One is a catalog of audited events that are considered "bad" behavior. The catalog could include attack profiles, suspicious activity profiles, and activities defined as unacceptable. The second component is an audit trail analysis module. Audit trails come from a chronological record of activities on a system. The analysis module examines the monitored system's audit trail for activity that matches activity in the catalog; when a match occurs, intrusive activity is assumed. Audit-based systems may also provide the ability to identify and track additional activity performed by an individual suspected of intrusive activity.

b. Expert Systems Detection — these systems are designed to act when a given situation occurs. The system often chains such activities so that when one situation occurs, it causes an action that may result in another situation that may cause another action. This pattern could occur many times before the sequence is complete. Expert systems differ from methods that match activity to entries in catalogs of information because the latter compare only discrete activity to discrete information and then perform an action. Expert systems can group activities and events together to make comparisons.

c. Keystroke Monitoring Detection — like audit-based detection, keystroke-monitoring techniques consists of two components. In this case, however, the catalog of bad behavior consists of specific keystrokes that indicate attacks. The second component is a module that captures keystrokes as the user enters them and then compares them with the catalog. When entered keystrokes match a catalog entry, an intrusion is assumed.

d. State Transition Analysis — this technique represents the monitored system as a state transition diagram. As incoming data is analyzed, the system transitions from one state to another. A transition depends on a particular Boolean condition becoming true (e.g., the user's opening a file). Intrusions are assumed when the system transitions from a safe to an unsafe state, based on known attack patterns contained in the intrusion detection tool.

4. Intrusion Detection

Networld has several tools form the IATAC Information Assurance Tools Database to utilize for intrusion detection. These tools fall into one or more of the following five classes (IATFF, Section 6.5):

a. Simple Vulnerability Identification and Analysis—a number of tools have been developed by Microsoft E-business systems to perform limited security checks. These tools may automate the process of scanning Transmission Control Protocol/Internet Protocol (TCP/IP) ports on target hosts. This is done by connecting to ports running services with well-known vulnerabilities and recording the responses. They also may perform secure configuration checks for Networld network files and discretionary access control settings. The user interface of these tools is likely to be command-line based, and the reporting may include limited analysis and recommendations. Networld should avoid using freeware.

b. Comprehensive Vulnerability Identification and Analysis More—this sophisticated vulnerability analysis tool is utilized by Networld to address new threats that require the scope of vulnerabilities to be addressed, the degree of analysis to be performed, and the extent of recommendations made to mitigate potential security risks.

c. Password Crackers—Password cracker tools attempt to match encrypted forms of a dictionary list of possible passwords with encrypted passwords in a password file. This is possible because the algorithm used to encrypt an operating system's passwords is public knowledge. An attacker or insider would run these tools after successfully gaining access to the system in order to acquire a higher privilege level,

such as root. These tools allow operators to verify compliance with password selection policies.

d. Risk Analysis Tools—Risk analysis tools typically provide a framework for conducting a risk analysis but do not actually automate the vulnerability identification process. These tools may include large databases of potential threats and vulnerabilities along with a mechanism to determine, based on user input, cost-effective solutions to mitigate risks. The vulnerabilities identified using a vulnerability analysis tool may be fed into a risk analysis tool to assist in determining the overall risk to the system.

Networld uses a network based ID system to monitor the traffic on its network segments as a data source. Placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment allows monitoring. Network-based ID involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment to which it's attached. Packets are considered to be of interest if they match a signature. Three primary types of signatures are string signatures, port signatures, and header condition signatures (Sans, July 2003).

1. String signatures look for a text string that indicates a possible attack. An string signature for UNIX might be "cat "+ +" > /.rhosts", which if successful, might cause a UNIX system to become extremely vulnerable to network attack. To refine the string signature to reduce the number of false positives, it may be necessary to use a compound string signature. A compound string signature for a common Web server attack might be "cgi-bin" AND "aglimpse" AND "IFS.

2. Port signatures simply watch for connection attempts to well known, frequently attacked ports. Examples of these ports include telnet (TCP port 23), FTP (TCP port 21/20), SUNRPC (TCP/UDP port 111), and IMAP (TCP port 143). If the site does not use any of these ports, then incoming packets to these ports are suspicious.

3. Header signatures watch for dangerous or illogical combinations in packet headers. The most famous example is Winnuke, where a packet is destined for a NetBIOS port

and the Urgent pointer, or Out Of Band pointer is set. This resulted in the "blue screen of death" for Windows systems. Another well-known header signature is a TCP packet with both the SYN and FIN flags set, signifying that the requestor wishes to start and stop a connection at the same time.

Well-known, network-based intrusion detection systems include AXENT (www.axent.com), Cisco (www.cisco.com), CyberSafe (www.cybersafe.com), ISS (www.iss.net), and Shadow (www.nswc.navy.mil/ISSEC/CID). A good ID capability uses both host- and network-based systems.

Due to the inability of Network based ID systems to see all the traffic on a switched Ethernet, Networld should use both Network based and Host based combined systems. A combination system can use fare more efficient intrusion detection techniques such as heuristic rules and analysis. Depending on the sophistication of the sensor, it may also learn and establish user profiles as part of its behavioral database. Charting what is normal behavior on the network is accomplished over a period of time. The following is a list of strengths and limitations of a combination system (RAID, Oct 2000):

Strengths

- A strong IDS Security Policy is a crucial part of commercial IDS.
- Provides worthwhile information about malicious network traffic.
- Can be programmed to minimize damage.
- A useful tool for Networld's Network Security Armory.
- Helps identify the source of the incoming probes or attacks.
- Can collect forensic evidence to identify intruders.
- Similar to a security camera or a burglar alarm.
- Alerts security personnel that a network invasion maybe in progress.
- When well configured, provides a certain "peace" of mind

Limitations

- Not a cure-all for most security ills
- Produces false positive (false alarms)
- Produces false negative (failed to alarm)
- Large-scale attacks could overwhelm a sensor
- NIDS cannot properly protect high-speed networks
- All products have weaknesses
- Not a replacement for:
    - A well managed firewall
    - A regular security audit
    - A strong security policy

Adding a host based ID system to Networld's existing network based system involves loading pieces of software on the network to be monitored. The loaded software uses log files and/or the system's auditing agents as sources of data. Networld would assign a person to be responsible for monitoring the IDS, and alert the System Administrator. The System Administrator who has noticed something "different" about their machines or who has noticed a user logged on at a time not typical for that user contains break-ins. (Sans, Aug 2003)

Host-based ID involves not only looking at the communications traffic in and out of a single computer, but also checking the integrity of the system files and watching for suspicious processes. To get complete coverage at the site with host-based ID, ID software must be on every computer. There are two primary classes of host-based intrusion detection software: host wrappers/personal firewalls and agent-based software. Either approach is much more effective in detecting trusted-insider attacks (so-called anomalous activity) than is network-based ID, and both are relatively effective for detecting attacks from the outside.

Networld also uses a knowledge-based approach to ID. Knowledge based ID techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. Networld's ID system contains information about these vulnerabilities and looks for attempts to exploit these vulnerabilities. When such an attempt is detected, an alarm is triggered. (Sans, Sept 2003)

Advantages of the knowledge-based approaches are that they have the potential for very low false alarm rates, and the contextual analysis proposed by the intrusion detection system is detailed, making it easier for Networld's security manager to take preventive or corrective action.

The main disadvantage to this method is the constant maintenance of gathering the required information on the known attacks and keeping it up to date with new vulnerabilities. Maintenance of the knowledge base of the intrusion detection system requires careful analysis of vulnerabilities and is a very time-consuming task. Detection of insider attacks involving an abuse of privileges is deemed more difficult because no vulnerability is actually exploited by the attacker. This is what contributed to Networld being infiltrated in the spring of 2001.

A former high level IT department person infiltrated the system through infrastructure owned by the University of Phoenix. As a student, this former employee broke into a Linux DNS server in Networld's non-production environment. The server was used to store personal files on Networld's network.

Although this hacked Linux file server was in the corporate environment, it could have been very serious if the network, equipment, or operation of the production environment had been compromised. Network administrators took the compromised machine offline without known losses of revenue and costs of less than $1,000 (man-hours) to counter this situation. The network administrator reviewed and deleted all accounts of personnel who left Networld. All forms of access to areas that contain information systems equipment needed to be re-screened for surrender and removal.

The network administrator also re-evaluated the need to leave the Linux server online and implemented behavior based ID techniques that detect an intrusion by

observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. Therefore, the intrusion detection system might be complete (i.e. all attacks should be caught), but its accuracy is a difficult issue (i.e. a lot of false alarms).

The advantage of this behavior-based ID system is that it can detect attempts to exploit new and unforeseen vulnerabilities. To compliment the knowledge-based portion of the Networld system, it detects an abuse of privilege type of attacks that do not actually involve exploiting any security vulnerability. In short: everything that has not been seen previously is considered dangerous.

The downside to the behavior-based system is its high false alarm rate, because the entire scope of the behavior of an information system may not be covered during the initial input and learning phase. Also, behavior can change over time, introducing the need for periodic online retraining of the behavior profile and resulting in the unavailability of the intrusion detection system or additional false alarms.

C. INTERNAL AND EXTERNAL SECURITY PROCEDURES

This section is broken down into four areas:

1. DoD Compliance & Certification
2. Network Security Incidents
    a. Type of Incidents
    b. Techniques and tools to exploit Networld vulnerabilities
3. Public Key Infrastructure (PKI)
4. Security Policies & Practices

These areas help Networld focus on areas of their information systems that may not have received the areas of attention that OMC would warrant.

1. DoD Compliance & Certification

Networld has implemented the following procedures to comply with requirements for DoD Certification and Accreditation by establishing teams to review current security status and to oversee completion of the DoD IT Certification process. Networld has incorporated government policies and standards from DoD 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and DoD 8510.1-M DITSCAP Application Manual to ensure a checklist of goals is being met. (CSRD, 2002) The recommendations contained in the previously mentioned publications govern IT security awareness, training, education, and implementation. Networld is currently completing DITSCAP Phase I, which validates the following areas:

- System mission
- Environment and architecture
- Identifies threats
- Defines levels of effort
- Identifies and documents the Designated Approving And Certification Authority (DACA)
- Application of firewall security on the network
- Two factor authentication
- Record level access controls on each database
- Audit logging
- 128 bit SSL encryption outside the firewall
- Anti-virus software
- Security patch management

Networld corporate offices are secured by an internal magnetic card-reader governing the front door and the servers are behind a secondary door, also locked. The

production environment is co-located in a secure off-site facility. The data center is specifically designed for e-commerce systems and offers these security features:

- Staffing 24 hours a day, 7 days a week.
- Facility access only after identity verification, accomplished through use of proximity card readers.
- Equipment cage within the facility locked with keys.
- Facility equipped with a centralized security station.
- The data center is designed to ensure uninterrupted continuous service.
- The UPS system is deployed in a parallel redundant configuration with N+ 1 module.
- Generator backup is provided for up to 100 percent of customer peak load with a fuel supply of 24 hours.
- Refueling contracts exist for cases where there is an extended utility failure.

Environmental systems are engineered to provide the functionality and redundancy required for optimum equipment operability. The following specifications are kept at all times:

- Data-grade HVAC system with N+1 redundancy.
- Constant ambient air temperature of 72 F, +/- 2 degrees
- Humidity controlled to a constant 45%, +/- 5%.

The facility offers the added reliability of 24-hour critical-systems monitoring to solve potential problems prior to escalation, including the following:

- All systems (including uninterruptible power supply, DC power, power; distribution unit, HVAC, temperature, humidity, security and fire threat) are constantly checked by a web-based monitoring system.
- Fire detection is managed with a VESDA air-sampling system.
- Dry-pipe pre-action systems complement the front-line fire-detection system.

- Networld maintains redundant links for OMC Internet Service Providers (ISP). These systems include backup plans and disaster recovery plans. Backups are conducted several times a day 365 days a year.

2. Network Security Incidents

A network security incident is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy (see the section on security policy). Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. An intrusion may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised. A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in as little as 45 seconds; with automation, the time decreases further. (CERT, July 2002) Networld has taken steps to prevent each type of incident that could affect transactions on OMC. Each incident is described in the "type of incidents" section of this document.

a. Type of Incident

Incidents can be broadly classified into several kinds: the probe, scan, account compromise, root compromise, packet sniffer, denial of service, exploitation of trust, and malicious code attacks. Networld has eliminated these threats through their DITSCAP checklist requirements.

- **Probe** -A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example given earlier is an attempt by the former employee to log in to an unused server account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry.

- **Scan** -A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a

prelude to a more directed attack on systems that the intruder has found to be vulnerable.

- **Account Compromise** -An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services. The lack of root-level access means Networld can contain any damage, but a user-level account is often an entry point for greater access to the system.

- **Root Compromise** -A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or "super user", privileges. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs, change how the system works, and hide traces of their intrusion.

- **Packet Sniffer** -A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems.

- **Denial of Service** -The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data. This is still the greatest area of concern for OMC's traffic on the Internet.

- **Exploitation of Trust** -Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a

set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers. Public Key Infrastructure (PKI) has been implemented to solve this problem.

- **Malicious Code** -Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents. Networld has overcome these problems with sound security patch management procedures.

b. Techniques and Tools to Exploit Networld Vulnerabilities

As intruders become more sophisticated, they identify new and increasingly complex methods of attack. For example, intruders are developing sophisticated techniques to monitor the Internet for new connections. Newly connected systems are often not fully configured from a security perspective and are, therefore, vulnerable to attacks. The most widely publicized of the newer types of intrusion is the use of the packet sniffers described in the section above. Other tools are used to construct packets with forged addresses; one use of these tools is to mount a denial-or-service attack in a way that obscures the source of the attack. Intruders also "spoof' computer addresses, masking their real identity and successfully making connections that would not otherwise be permitted. In this way, they exploit trust relationships between computers. Networld networks have undergone vulnerability checks using the Microsoft Baseline Security Analyzer (MBSA) to counter these threats. Networld reviews the results of takes MBSA vulnerability checks and takes appropriate countermeasures after analyzing the vulnerabilities, risks, and threats to exploit found vulnerabilities.

With their sophisticated technical knowledge and understanding of the network, intruders are increasingly exploiting network interconnections. They move through the Internet infrastructure, attacking areas on which many people and systems depend. Infrastructure attacks are even more threatening to Networld because network managers and administrators typically think about protecting systems and parts of the infrastructure rather than the infrastructure as a whole.

The tools available to launch an attack have become more effective, easier to use, and more accessible to people without an in-depth knowledge of computer systems. Often a sophisticated intruder embeds an attack procedure in a program and widely distributes it to the intruder community. Thus, people who have the desire but not the technical skill are able to break into systems. Indeed, there have been instances of intruders breaking into a UNIX system using a relatively sophisticated attack and then attempting to run DOS commands (commands that apply to an entirely different operating system). The same tools that Networld uses to examine programs for vulnerabilities are the same tools that intruders use to find new ways to break into Networld systems.

As in many areas of computing, the tools used by intruders have become more automated, allowing intruders to gather information about thousands of Internet hosts quickly and with minimum effort. These tools can scan entire networks from a remote location and identify individual hosts with specific weaknesses. Intruders may catalog the information for later exploitation, share or trade with other intruders, or attack immediately. The increased availability and usability of scanning tools means that even technically naive, would-be intruders can find new sites and particular vulnerabilities.

Some tools automate multiphase attacks in which several small components are combined to achieve a particular end. For example, intruders can use a tool to mount a denial-or-service attack on a machine and spoof that machine's address to subvert the intended victim's machine. A second example is using a packet sniffer to get router or firewall passwords, logging in to the firewall to disable filters, then using a network file service to read data on an otherwise secure server. These challenges have been solved by MBSA recommendations.

The trend toward automation can be seen in the distribution of software packages containing a variety of tools to exploit vulnerabilities. These packages are often maintained by competent programmers and are distributed complete with version numbers and documentation. A typical tool package might include the following:

- Network scanners.
- Password cracking tool and large dictionaries.
- Packet sniffer.
- A variety of Trojan horse programs and libraries tools for selectively modifying system log files.
- Tools to conceal current activity
- Tools for automatically modifying system configuration files

3. Public Key Infrastructure (PKI)

Networld uses VeriSign Managed PKI Services for its implementation of Public Key Infrastructure (PKI). VeriSign is a world leader in the development of PKI practices, with audited business processes that meet the most stringent industry standards. Networld outsourced PKIs to VeriSign because they offer a greater number of services, is a lower cost of ownership option, can be rapidly deployed, and reduces Networld's risk.

VeriSign locates critical PKI functions in a secure data center operated by VeriSign or an affiliate on a continual twenty-four hour basis, 365 days a year. To ensure the highest levels of security and availability, all PKIs implemented through VeriSign Managed PKI (VeriSign, Oct 2003) services employ hardware-based cryptography, highly screened and trained personnel, a military-grade secure facility, and a rigidly audited system of procedural controls. Round-the-clock service levels are supported.

VeriSign's Certification Practices Statement (CPS), which delineates the practices underlying the VeriSign Trust Network (VTN) public Certification Authority (CA) services, is recognized as the most comprehensive document of its type and is used internationally as a foundation for enterprise PKI practices. VeriSign's practices include

witnessed and audited processes for CA key establishment and management, and rigid multi-party controls over all key materials. VeriSign undergoes an annual, independent security audit against established Web Trust for CA (SAS 70) security guidelines, and has been approved to issue certificates consistent with the polices and procedures defined by the Department of Defense. KPMG (AICPA) in accordance with AICPA SAS- 70 certifies VeriSign's processes. (Lloyd)

4. Security Policies & Practices

Networld could not provide a copy of their internal IT security procedures, because they are not comprehensive and are being rewritten to reflect increased involvement with OMC and Federal procedures.

Networld should develop a documented high-level plan for organization-wide computer and information security. It should provide a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for Networld users and system administrators to follow. Because a security policy is a long-term document, the contents should avoid technology-specific issues. A basic security policy covers the following:

- High-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy
- Risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of assets in case of loss.
- Guidelines for system administrators on how to manage systems
- Definition of acceptable use for users.
- Guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system)

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Networld management should assign responsibility for security, provide training for security personnel, and allocate funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology, but this needs to be monitored. The result is an automatic and consistent enforcement of policies, such as those for access and authentication. Technical options that support policy should include:

- Challenge/response systems for authentication
- Auditing systems for accountability and event reconstruction
- Encryption systems for the confidential storage and transmission of data
- Network tools such as firewalls and proxy servers

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of recommended practices for Networld systems:

- Ensure all accounts have passwords that are difficult to guess. A one- time password system is preferable.
- Use tools such as MD5 checksums (8) with a strong cryptographic technique, to ensure the integrity of the system software on a continual basis.
- Use secure programming techniques when writing software found on the Microsoft Operations Manager website. (Microsoft, Oct 2003)
- Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- Regularly check with Microsoft Operations Manager for the latest available fixes and keep systems current with upgrades and patches.
- Record and implement daily on line updates from Microsoft Security Bulletins for training of incident response teams and technical advice.

- ❖ Document audit system results on each occurrence. Networld could suffer computer security incidents by not recording sufficient audit data when collected. This will make detection and tracing an intrusion more difficult.

D. CONCLUSION

Networld information protection decisions could be hampered by incomplete or lack of documented procedures of current practices. Lessons learned from managing Internet security risks could be repeated without a company internal procedures guide. External consultants who have knowledge of the organization can be utilized to thoroughly document company internal policies and procedures. In order to address the widening gap between current risk management practices and the need for administrative documentation of information protection, Networld needs a Systems Assessment Program (SAP) by developing a comprehensive, repeatable technique for identifying vulnerabilities in:

1. Security Patch Management
2. Operating System and Application Hardening
3. Proactive Virus Detection
4. Intrusion Detection
5. DoD Compliance & Certification
6. Network Security Incidents
7. Public Key Infrastructure (PKI)
8. Security Policies & Practices

SAP enables Networld to develop and document appropriate protection strategies by considering policy, management, administration, and other organizational issues, as well as technologies, to form a comprehensive view of the information security state of that organization. This allows employees to have a company manual for an overarching security and information protection framework that allows them to readily identify and pursue an appropriate security posture.

Networld does have an effective risk management strategy that assesses more than the existing information infrastructure. Networld guidelines are summarized as:

- The value of the assets that must be protected.
- Consequences of loss of confidentiality or operational capability.
- Vulnerabilities that could be exploited to bring about the losses.
- Existing threats that could exploit the vulnerabilities.
- Likelihood that a threat might occur.
- Availability and appropriateness of options and resources to address risks and concerns.

Networld must continue toward certification in three phases to provide a systematic, context-driven approach to managing information security risks, and enables an organization to assemble a comprehensive picture of their information security needs.

Phase 1 identifies information assets and their values, as well as threats to those assets and the security requirements to protect them. This is accomplished as Networld uses its staff knowledge at multiple levels within the organization along with standard internal documentation procedures. The information collected can then be used to achieve Phase 1 goals, which are to establish the security requirements of Networld.

Phase 2 examines the security assets of Networld in relation to the security infrastructure to identify high priority vulnerabilities. Networld staff evaluates the vulnerabilities within the infrastructure and concludes Phase 2 by identifying the high-priority security infrastructure components, missing policies and practices, and vulnerabilities.

Phase 3 builds on the information captured during Phases 1 and 2. Analyzing the assets, threats, and vulnerabilities identifies risks. Estimates of impact and probability of the risks are made, and the risks are then prioritized, ultimately resulting in the development of a protection strategy and a comprehensive, enterprise-wide plan for managing information and security risks.

E. RECOMMENDATIONS

Networld should establish a SAP to provide an organizing framework as well as a method of capitalizing on their abilities, practices, and mission through self-assessments. This will help Networld understand which strategies and practices are working effectively. It also reveals needed improvements and existing gaps in strategy, technology, staff knowledge, and in the ability of Networld to protect key OMC assets in a constantly changing environment.

Networld's good internal communication among all levels of staff and management will help provide a clear picture of gaps in internal capabilities, thus enabling a strategy to be built that can include appropriate use of specialized, external experts. Ultimately the goal of SAP is to improve how well OMC assets are protected, thus putting Networld in a better position to achieve their missions.

Inherent in a SAP is the assumption that Networld is already working to meet its mission objectives by using Microsoft Security Policies and Procedures to augment internal protection strategies. A generic plan of duties and responsibilities for members of Networld's Internal Security Team has been provided in Appendix E as a guide to be contained within the SAP. A good internal policy will continue to define technology and management practices that provide practical guidance, which will help Networld counter problems in network security and protect OMC assets.

V. WIRELESS COMMUNICATION

A. HISTORY OF THE INTERNET "TIMELINE"

1. Introduction

The advent of the computer has brought about the Internet, which has in turn revolutionized the world. The stage for this revolutionary means of communication was started over a century ago with the development of the telegraph, followed by the telephone, then the radio, and finally the computer. Together, these technologies set the stage for an unprecedented integration of capabilities.

The Internet is capable of world wide dissemination of information and a means for collaboration between individuals and their computers via email, web-based pictures, video-conferencing, instant messaging, and much more, all without regard for geographic location (Leiner, 2000). It is this worldwide capability that makes the Internet the perfect tool for government electronic commerce and procurement. A contracting officer with access to the Internet can order almost anything he/she needs from anywhere in the world via the DoD EMALL, if the hurdles of delivery are satisfied. A contracting officer with the Electronic Procurement Palette Setup (EPPS, a simplified visionary idea explained later) can be up and running with the DoD EMALL within just an hour of arriving in a mature or even immature environment regardless of the circumstances.

2. Telegraph

Even before the telegraph, there were other forms of communication over what was then considered great distances. Most were semaphore systems incorporating flags or lights (The Invention of the Telegraph). Similar to how the Chinese communicated from tower to tower using smoke signals on the Great Wall of China, the eighteenth century American used an observer who would decipher a signal from a high tower station on a hill then send it to the next tower and so forth.

Instead of using smoke, flags, or lights, wire transmission forever changed the way information was to be sent. On May 24, 1844, Samuel F. B. Morse, using the magnetic telegraph, electrically transmitted his famous message "What hath God wrought?" from Washington to Baltimore, a distance of 37 miles, a mere inch compared

to today's transcontinental distances. However, this was just the beginning of what was yet to come. Morse Code, used to make the telegraph function, used a series of dots and dashes to communicate. This technology is not far from today's computer technology of communicating via a binary system of 0's and 1's. Even in the 1800's the telegraph revolutionized human tele-communication (History of the Internet).

3. Transatlantic Cable

The magnetic telegraph brought about the rapid deployment of telegraph lines all over Europe and North America, allowing near instantaneous messaging within those theaters. However, the desire to communicate across the Atlantic required laying a telegraph line across the ocean, a task that would be accomplished only due to sheer determination.

The idea of a transatlantic cable was first conceived just one year after Samuel Morse sent his famous message from Washington to Baltimore. However, because of the formidable problem a transatlantic cable posed, it was 1856 before the Atlantic Telegraph Company registered to take on the task.

The first cable was manufactured in 1857. However, it was not until 1858, after a couple of unsuccessful attempts, that the two continents were finally joined. Unfortunately, because of an engineer's mistake, the cable was damaged. It was not until July 1866, when the final successful cable was laid 1,686 nautical miles across the Atlantic Ocean, permanently connecting the two continents. This accomplishment allowed direct instantaneous communication across the Atlantic for many decades. The next technological leap occurred in the 1960's when the first communication satellites offered an alternative to the magnetic telegraph. Although there have been huge advances in satellite technology, inter-continental cable is still the main hub of telecommunications (The Transatlantic Cable).

4. Telephone

In March 1876, Alexander Graham Bell invented the telephone. The invention brought about a new level of communication that exceeded the capabilities of the telegraph. However, it would still be a century before the telephone's true calling would be to provide the backbone of today's Internet connections. Although computers use digital technology, modems still provide digital to audio conversations to allow computers to connect via a telephone network (Farley, 2003).

5. Sputnik

On October 4, 1957 the former Soviet Union launched the world's first artificial satellite - the Sputnik Satellite. Its mission to determine the density of the Earth's upper atmosphere and ionosphere were important, but more relevant was how the information was sent back to Earth.

Although the Sputnik Satellite only returned signals to Earth for 21 days, it was the use of its two radio transmitters that paved the way for telecommunications. This marked the start of global telecommunications. The United States responded by forming the Advanced Research Project Agency (ARPA) within the DoD. Today, satellites play an important role in transmitting voice and data signals, as explained later (Nauts, 2000).

6. Networks "Packet Switching"

The Cold War led to research by three inventors to overcome the communications challenges of the 1960's. Paul Baran, a Rand Corporation, engineer began work on a project to develop a survivable communication system in the event of a nuclear war. In addition to the Soviet Union and the United States achieving mutually assured destruction by matching quantities of nuclear weapons, Baran hoped that he could increase deterrence by developing a communication system that would survive a nuclear attack.

Baran's first thought was to incorporate a redundant nationwide system of several hundred switching nodes, with as many as eight links at each node. Later, Baran proposed transmitting uniform blocks of data or bits. These multiple blocks of data would be coined "packets", but his formal term was "distributive adaptive message block switching." The packets would take independent routes through the network and get

reassembled at the final destination once they all arrived. Donald Davies, another inventor continued the work in this area and called it "packet switching." (Williams, 2001)

Initially, it was thought that packet switching introduced two design flaws: (a) Discontinuity, where it gives up the advantage of always being on or continuous connection like a telephone; and (b) Conversions, where analog communications like voice have to undergo analog-to-digital encoding to get on the network just to get decoded at the destination, creating extra work and time. However, packet switching created four practical advantages:

- Digital – Communications were made digital, which proved to be error free.
- Processing – It allowed the computer to be a part of the network by placing software systems at each node, which can be continually upgraded and improved.
- Redundancy – It eliminates the dependency of any one-communication link like that of a telephone, which conceivably allowed the network to survive considerable damage.
- Efficiency – Unlike a telephone linking one conversation on one line, a network enabled more than one communication to share a given link at the same time (Living Internet).

7. ARPANET

The third packet switching inventor, Leonard Kleinrock had a great deal of influence in the development of the ARPANET (Williams, 2001). With his development of packet switching theory and focus on design and measurement, his Network Measurement Center at UCLA was the site for the first node on the ARPANET. Other nodes at the Stanford Research Institute, University of California Santa Barbara and University of Utah soon followed. Soon after, in 1969, these nodes and their host computers were connected together into the ARPANET, where the birth of the Internet was formed and the first host-to-host message was sent.

In the years following, more computers were added to the ARPANET and work proceeded on a functionally complete Host-to-Host protocol, the first being the Network Control Protocol (NCP). In October 1972, an exhibit of the ARPANET at the International Computer Communication Conference successfully demonstrated a fundamental version of today's e-mail utility or people-to-people traffic. What was originally the ARPANET, eventually grew into the Internet. The ARPANET began as the pioneering packet switching network, but soon incorporated packet satellite networks, ground-based packet radio networks and other open architecture networks (Leiner, 2000).

8. TCP/IP

Defense Communications Agency (DCA) and ARPA establish the Transmission Control Protocol (TCP) and Internet Protocol (IP) as the protocol suite for ARPANET. This led to one of the first definitions of the Internet being a series of connected networks (History of the Internet).

9. Global Networking

It was 1973 when the University College of London and Royal Radar Establishment in Norway connected to the ARPANET, making global networking a reality. Once the barrier of the vast ocean was overcome, email, audio mail, instant messaging, newsgroups, e-commerce, and more soon followed (History of the Internet).

10. World Wide Web

Although reference to the Internet and World Wide Web are used interchangeably, they are different. As referenced above, the Internet is a global network of computers used to support a variety of applications: like e-mail, chat rooms, and many other applications. Ironically, the World Wide Web is merely another application accessed through the Internet. The World Wide Web or "Web" allows us the opportunity to view information such as graphics, audio, video, and text in Web pages (Long, 31). In other words, the Internet is the vehicle that allows access to the World Wide Web.

B. VARIOUS USES OF THE INTERNET

1. E-Mail

Electronic mail is just one way for people to interact with each other through the computer. Unlike the traditional mail system taking days to reach the recipient at a real street or post office box address, e-mail allows people to instantaneously send and receive information to an electronic address through computers that are linked to each other via a connection like the Internet. In addition to just sending simple messages, a person can transmit an actual file, program, digital image, or almost anything needed. Even with the advent of electronic mail, the future of electronic procurement was being shaped (Long, 20, 279).

2. Internet Café's

Also known as Cyber Café's, people that desired to catch up on emails or surf the web could do so at places like coffee shops that were set-up with computers and Internet connectivity. Although a big craze in the early 1990's, cyber cafes closed almost as quickly as they opened. One major reason for this was the reduction in home computer prices. Cyber café's fulfilled a need in the early 1990's, however, in 1999 about 40 percent of Americans owned a home computer thereby reducing the need for cyber café's. Further decline of cyber café's occurred because of the advent of laptop computers, handheld devices, and recently, the use of cell phones and other mobile technologies to gain Internet access (Johnson, 1999).

3. News Groups

News Group doesn't mean that any real news is found on the Internet. In fact, it is an electronic version of a bulletin board or electronic discussion group. The newsgroups are organized by topics and subtopics, where a person posts opinions or a discussion topic in the news group area of their interests and awaits a response from someone on a different computer. Some of the major topics include science, recreation, computers, and more (Long, 282).

4. News

News of local, national, and international current events can be found throughout the day on various television channels like your primary networks or CNN, FoxNews,

and MSNBC. However, a person interested in a specific event might have to wait for a particular news clip to air on the hour. Internet news is a convenient way for Internet users to search specific news events with just a click of a mouse. Well-known newspapers like USA Today, The Washington Post, and the Los Angeles Times host Internet web sites with up to the minute news. They allow users to categorically search most types of current or old news whether local or international, as well as a variety of other information-based services (Long, 287).

5. On-Line Stores

The commercialization of stores began hitting the Internet in 1994. People were able to do shopping for items at on-line stores that they used to only be able to purchase at malls or able to complete simple banking transactions. To complete transactions via the computer and Internet as opposed to physical transactions in person was the start of a new way of life (History of the Internet). This internet based sales concept or e-business saved time and money for many companies like Wal-Mart, Circuit City, Best Buy, eBay, and Amazon.com to name a few.

6. EBAY

The online auction began in late 1995 with a simple conversation between Pierre Omidyar, an engineer and his fiancé. Her desire to trade Pez dispensers over the Internet generated the online auction idea. Initially called Auction Web, the company changed its name to eBay in 1996 when it completed nearly 800,000 transactions a day.

EBay started as an Internet-based garage sale where people can buy, sell, or trade collectables. However, it soon blossomed to include retail merchant's surplus inventories. The online garage sale eventually included competitors like Yahoo, FairMarket.com, and Amazon.com (Afuah, 361-367).

7. AMAZON.COM

In July 1995, Amazon.com began selling books on the Internet. It was not long before the brick and mortar (storefront) businesses like Barnes & Noble and Borders took notice. Within the next few years Amazon added compact disks, videos, gift stores, toys and electronics to its online sales. However, in September 1999 Amazon announced the

introduction of its zShops, a marketplace of online retailers like that of a mall, only this was more of an online mall.

Amazon did not wish to just be in book sales, they wanted to sell everything possible with the ease of just clicking a mouse. In fact, "Amazon.com defined e-commerce as we know it today." (Afuah, 224-230) With just about any one able to sell merchandise on the internet, comparison shopping put pressure on the size of store markups which forced retailers to give their best prices. This competition may have been a problem for many companies. However, competition is good for the buyer and this e-commerce model would soon find its way into government procurement (Afuah, 109).

8. GSA Advantage

In 1995, the government launched its own online version of Amazon.com, called GSA Advantage. This source of online procurement is available for Federal Government employees and sells everything from office supplies to specialized capital equipment. In fact, GSA Advantage receives more than 35,000 hits a day and provides access to over 2.3 million products and services from Supply System depots, Federal Supply Schedule (FSS) products, and commercial items directly from contractors. All this is available with just a click of the mouse and the assurance of meeting Federal Acquisition Regulation guidelines. (GSA Advantage, 2001)

9. DoD EMALL

DoD EMALL is operated by the Defense Logistics Information Service (DLIS) and, like GSA Advantage, is an Internet electronic mall that is available for authorized government users. DoD EMALL customers can securely shop for and order supplies from a variety of government and commercial source catalogs. The site has over 150 commercial catalogs with over 12 million items available. DoD EMALL allows its customers to compare prices and order items from more than one source at a time. Customers can order items using their Government Purchase Card or MILSTRIP/FEDSTRIP. Finally, DoD EMALL has the ability to generate various levels of reports to Commands, Purchasing Offices, or any user requesting information about their purchasing activities. (DoD EMALL, 2003)

C. TRANSMISSION MEDIA

1. Introduction

Computer networks allow us to transmit and receive data. The way that computers are connected, or connectivity, determines the speed that data is transmitted. Companies are increasingly more dependent on the Internet to conduct business-to-business e-commerce. The communication channel is the transmission media used to get the information from one computer to another. There are a variety of communication channels made up of wired and/or wireless media. The data carrying capacity of that media is known as the bandwidth (Long, 243). The following chart shows the relative download speeds of various broadband technologies to include the 56k modem on a regular phone line. Some of the bars show varying solidity. The more solid areas indicate the average speeds that are generally available to users (I buy broadband, 2001).

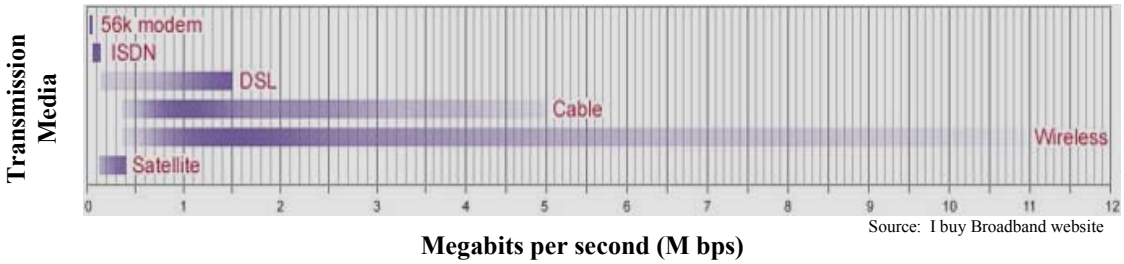


Figure 21. Internet Speed Comparison Chart

2. Wired Communication

Before the advent of high-speed broadband access, computer users, with the aid of a modem to convert analog signals to digital signals, used telephone services to access the Internet. Telephone lines use copper twisted pair wire to transmit voice and digital data. Twisted pair wire also provides two other services: Integrated Services Digital Network (ISDN) and Digital Subscriber Line (DSL). The ISDN line allows a digital data transmission speed of 128Kbps, which is twice the speed of a typical analog modem (Long, 222).

Digital Subscriber Line is the fastest of the three copper twisted wire transmission methods. It allows download speeds of 1.5 to 9 M bps and upstream speeds of 512 K bps

to 1.5 M bps. The increased speed over that of the typical telephone method supports applications like full motion videos and other real-time applications involving a group of online participants. Even with speeds as fast as DSL, there is still another wired form of transmission media that is almost ten times faster than DSL (Long, 223).

The same media that sends the cable company's television signal, coaxial cable, is capable of sending and receiving digital signals as well. It has data transfer rates of 1 to 10 M bps, which permits high-speed data transmission with minimal signal distortion. Just like a telephone line, coaxial cable connects computers and terminals in a local area or even across the vast ocean. In fact, coaxial cable is laid across the ocean floor to connect the continents (Long, 223).

Another form of wired transmission media comes in the form of Fiber optic cable. This technology carries digital data as laser-generated pulses of light. Fiber optic cable delivers data cheaper and faster than copper twisted wire as is used in telephone lines, DSL, ISDN, and regular copper wire as is used in coaxial cable. Another major advantage to using fiber optic cable is the difficulty intercepting a light signal as compared to intercepting an electric current signal (Long, 225).

Interestingly, two optical fibers can handle the equivalent of over 600,000 Internet dial-up connections at one time. Specifically, optical fiber can exchange data at an astonishing rate of 44-155 Mbps (Moore, 2001). High-speed communication channels do not have to consist of land-based wires though. They can and often do consist of wireless technology (Long, 225). Unlike a wired network in which an entire market must be wired before initiating service, the capital expenditures of a wireless network can be incrementally incurred as more customers are added.

3. Wireless Communication

In addition to transmitting data on wires or fibers, data can be transmitted wirelessly. With use of wireless transceivers, wireless communication is a good alternative to using telephone lines, coaxial cable, or fiber optic cable. About the size of a credit card, wireless transceivers permit data communication between any source and destination such as a personal computer and a local area network (LAN) (Long, 226).

Transceivers transmit wireless signals via microwave or radio signals. When used locally within a building, radio waves travel in all directions at once or omni-directional and have a limited range of about 50 feet. In this case, a transceiver transmits the signal to other transceivers in a network. The major disadvantages to this technology are its limited channel capacity of about 115 Kbps and the number of computers that can be linked because of limited frequencies allowed on a network (Long, 226).

As previously implied, one of the major advantages to using wireless technology is the cost savings when installing a network system in a new building. Related to the cost savings is the convenience of not having to rearrange wall outlets when moving furniture in an office or moving from office to office. The savings are estimated to be $150-200 per move. In the event that a wireless access point needs to be moved, it can be done with minimal effort, cost, and time.

One last key issue surrounding wireless technology is its vulnerability to hackers. Unlike a building network using a hard-wired line, a hacker does not need to gain physical access to the building to infiltrate the system in a wireless network. Because the radio signals penetrate building walls, it's conceivable that a hacker could access a wireless network from a car parked outside the building (Bluesocket bluePaper, 1-4). Regardless of its security and bandwidth issues, the seamless mobility of wireless technology far outweighs its disadvantages.

Similar to radio waves traveling through the air, microwave signals travel in a straight line from the source to the destination, known as line-of-sight. Because these signals cannot bend with the curvature of the Earth, the signals need to be repeated from point to point until they reach their final destination. This is done via repeater stations that are placed on towers about 30 miles apart (Long, 223).

Recently, Intel launched its new Centrino mobile technology. Intel Centrino integrates wireless technology capabilities with the power of mobile computers. Specifically, it includes a new mobile processor and wireless network functions to give people the freedom to connect to the Internet at thousands of "Hotspots." These Hotspots

are locations that users will be able to use 802.11 wireless technologies at places like airports, hotels, and retail and restaurant chains worldwide ("Intel Launches", 2003).

People can access the Internet with specially configured cell phones or pocket computers attached to those phones. However, surfing the Internet on the small screen of a cell phone or pocket computer can be quite inconvenient and frustrating. A majority of the United States' wireless carriers like AT&T Wireless, Sprint PCS, T-Mobile, and Verizon Wireless sell PC cards that allow users to connect to the Internet even when out of range of a Hotspot. As long as a signal is received, data can be transmitted wirelessly. Cingular Wireless sells a cell phone that connects to a laptop to provide Internet access virtually anywhere. The data rates for the data card or phone are roughly 144 Kbps, slightly better than a typical 56K modem (Brown, 26).

Roughly between 100,000 and 150,000 visitors a day attend festivities at Walt Disney World in Florida. Most of them are unaware that the 47-square mile theme park is almost completely serviced by a wireless system. The park's 55,000 employees rely on its 802.11b wireless LAN to complete functions like authorize credit cards at snack bars and merchandise centers, and track visitors while they wander through the park. This wireless technology is especially convenient for allowing the park's employees the mobility to bring merchandise and food to people waiting in lines for rides.

Disney has also incorporated this wireless technology on its cruise ships. On these cruises, guests are given a card that allows the ship to track these guests as they disembark for island walks (Mingis, 2001). Although wireless technology is fairly new, its potential seems endless. Using wireless technology as thus far mentioned is quite handy for the typical businessman while traveling or for generating revenue for businesses. However, if a Federal employee wants to order supplies through the open market corridor, these wireless technologies do not guarantee that vital connection to accomplish the order. Therefore, other forms of wireless connectivity might be needed to ensure wireless technology anywhere on this planet.

4. Satellite Communication

Satellites are spacecraft that enable voice and data communications virtually anywhere on Earth. As previously mentioned in the microwave wireless community, repeater stations carry signals from point-to-point until they arrive at their final destination. Satellites are flown into space and act as a repeater station. Therefore, instead of being placed on towers, buildings, or mountains, these expensive repeater stations are placed in various fixed positions around the Earth's orbit (Long, 224). In fact, satellites are classified into one of three orbits.

a. Geostationary Spacecraft

At first, communication satellites were placed in a Geostationary Earth Orbit (GEO), which is an altitude of 35,786 km above the Earth's equator, or the so-called "Clarke Belt." Here the gravitational pull matches the centrifugal force out thus maintaining the satellite's stationary orbit in relation to the Earth. (Hogle, 2002) Satellites in Geostationary orbits circle the Earth every 24 hours. As a result, the satellite always remains in proximity to a fixed observer on the Earth's surface. This feature ensures that the satellite's coverage area remains stationary. (Akyildiz, 301-301)

A GEO satellite has an enormous footprint that covers about 1/3 of the Earth's surface with exception to the polar caps. Therefore, it only takes three satellites to cover just about the whole Earth's surface. Placing a satellite at a high or geostationary orbit ensures almost total coverage for data and voice communications. The GEO satellite's large footprint is suitable for broadcast delivery of information over large areas of the Earth's surface, but does have its disadvantages (Akyildiz, 301-302).

A signal traveling to a 35,786 km altitude will cause latency, the time delay (approximately 250 ms each way) for a signal to travel to and from the satellite. This latency problem between users is too noticeable for effective, real-time communications (Hogle, 2002). Second, the user terminals and the satellites consume a lot of power. Additionally, for high altitude satellites to achieve high bandwidth, they have to use a large antenna, which limits the mobility of the terminals (Shek, 273). Third, this altitude results in an inefficient use of available frequencies.

b. Non-geostationary Spacecraft

An alternative to using GEO satellites is to use a lower orbit spacecraft, specifically in a Middle Earth Orbit (MEO) or Low Earth Orbit (LEO). MEO satellites are placed about 9,800 – 20,500 km from the Earth's surface and have a lower latency problem than that of the GEO satellites. Because these satellites are closer to the Earth, it requires more of them to cover the same footprint as the GEO satellites. The same is true for LEO satellites, which are the closest spacecraft to the Earth's surface. (Refer to Figure 22)

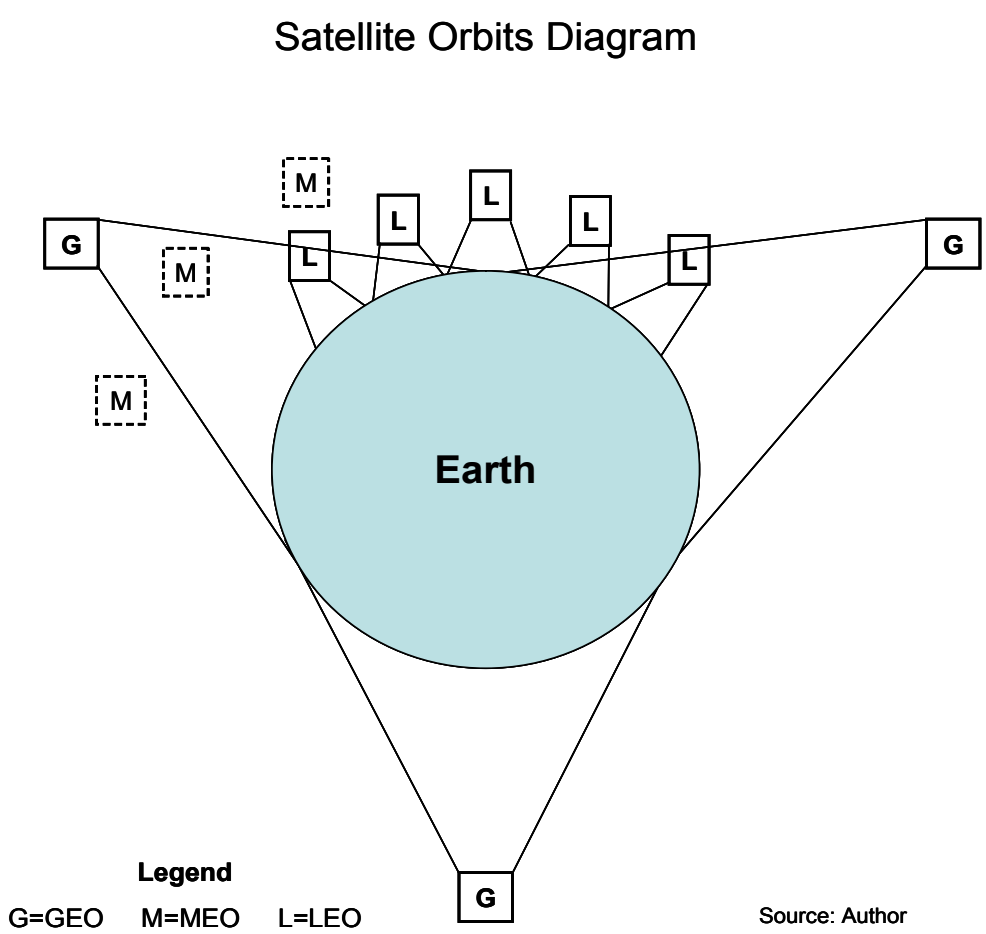


Figure 22. Satellite Orbits Diagram

LEO satellites are placed about 800 – 2400 km from the Earth's surface and seem to be the preference of many satellite global communication networks (Hogle, 2002). Because of the closer altitude to the Earth, MEO and LEO satellites circle the Earth faster than the GEO satellites. Therefore, unlike a geostationary satellite always

staying in position with a fixed observer on the ground, MEO and LEO satellites have non-geostationary orbits and do not stay in proximity of a specific fixed observer. As a result, global communication networks using non-geostationary satellites must deal with mobility management, such as tracking and locating a user terminal as the satellite passes overhead, while handover management hands over a signal to a subsequent observer ensuring a call isn't dropped in the transfer (Akyildiz, 301) Therefore, the technology to handle this mobility problem is newer and more complex than geostationary satellites, but its advantages outweigh the alternatives (Hogle, 2002).

LEO satellites provide the fastest data and voice transmission with only less than a .03ms latency factor. Being the closest to the Earth, many more of these satellites are needed to cover the same surface footprint as the MEO and GEO satellites. However, these satellites might be the best choice for accessing the OMC through the Internet via satellite communication. Unlike GEO satellites' long signal delays and high power requirements in the user terminals and satellites, LEO spacecraft are preferred because of their lower user terminal and satellite power requirements (Akyildiz, 302).

c. Network Connectivity and Connection Routing

In a wired or wireless based communication system, the ability to send and receive communication signals is dependent upon the available infrastructure. However, a satellite based communication system incorporates various routing techniques to get a signal from origin to destination. Because of the LEO satellites' smaller footprint, it's likely that a call might need routing through different satellites as opposed to just one in a geostationary orbit. Therefore, communications involves links between user terminals and their respective serving satellites and a backbone network. The voice or data link from a user terminal to a satellite is called the uplink. Conversely, the link from a satellite to a user terminal is the downlink. User signals can be transmitted through a terrestrial or space-based network. (Akyildiz, 303-304)

A terrestrial network uses a wired system to transfer voice and data. In a terrestrial network the user's uplink signal travels to the satellite and then to a gateway that sends the information to the receiver's gateway via the wired network and finally to the recipient (Figure 23).

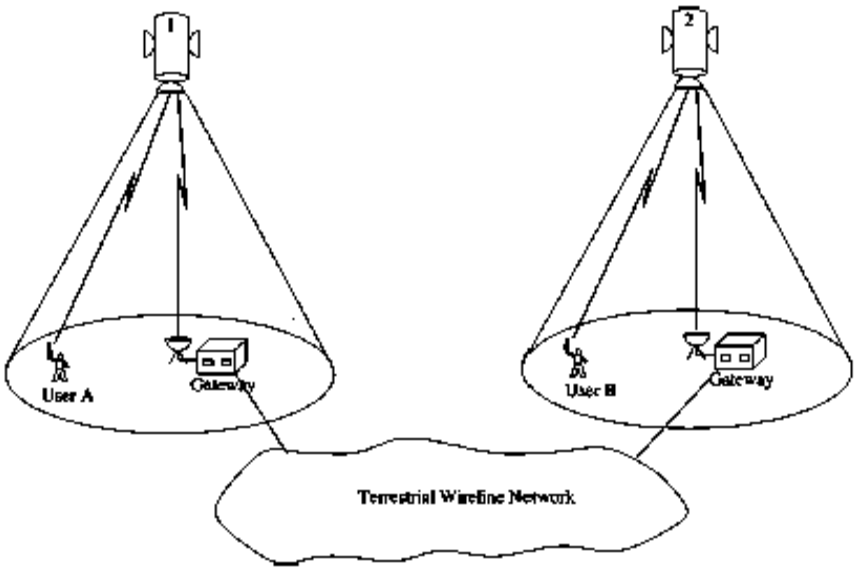


Figure 23. Terrestrial Network **Source: Handover Management**

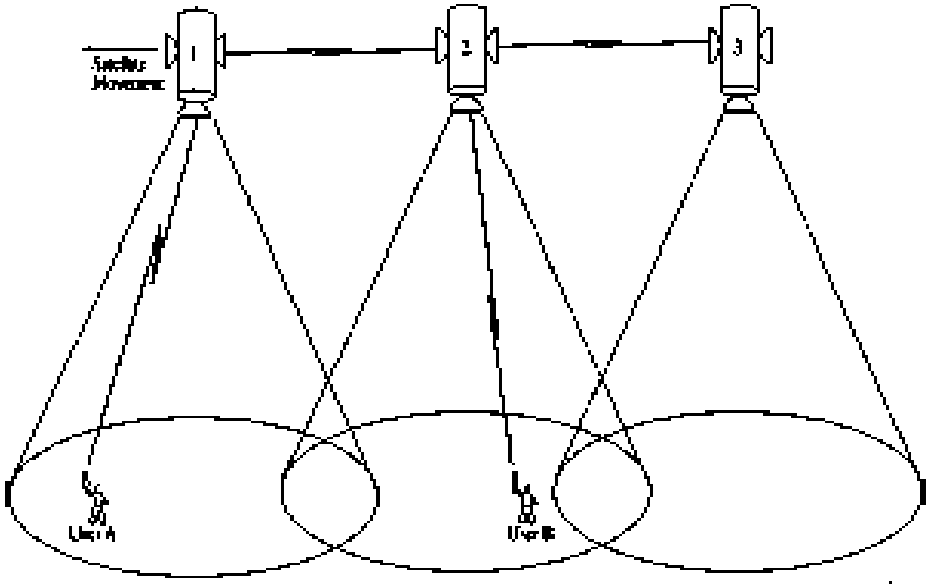


Figure 24. Space Based Network **Source: Handover Management**

A space-based network is an alternative to a terrestrial wired network. A space-based network routes calls through links between satellites known as Inter-satellite links (ISL) (Figure 24). There are multiple global communications network companies available, but some, such as Globalstar and Ellipso route their calls in a terrestrial based network while others like Iridium and Teledesic (which recently suspended service) use

space-based networks as their backbone network (Akyildiz, 304). Neither satellite routing system is the perfect setup for every situation or emergency response, but when appropriately combined, they provide a complete networking solution. Specifically, the ISL can be used for rapidly deployable network needs while the terrestrial network can be used when sufficient infrastructure is available (Shek, 273). Choosing the correct company requires market research and is dependent on user needs and available infrastructure. This topic is briefly addressed in the Electronic Procurement Palette Setup (EPPS) section.

Satellite dishes vary in sizes, but over the years have been getting smaller. Very small aperture (VAST) and Ultra small aperture (USAT) satellite dishes make data communications possible. Newer versions of USATs are about a foot in diameter and make satellite mobility easier, while providing data networks for companies and voice networks for commercial carriers. (Hogle, 2002) Satellites provide many other services like video and audio broadcasting, teleconferencing, facsimile, and most importantly high-speed Internet access. (Ananasso, 155)

As previously mentioned, satellites use some form of radio system and have the ability to cover vast areas of the Earth's surface at any time. These properties lead to some unique and important characteristics (Golding, 102):

- Ability to provide service and cumulative traffic over large areas
- Ability to allocate bandwidth and power to various users
- Ability to provide coverage just about anywhere on the planet surface to include rural and water areas and air space
- Ability to provide broadcasting, data collection, and point-to-point communications
- Ability to have direct access to users regardless of their location

Whether using a satellite phone or a satellite dish, satellite communications are used in more ways than ever before and have opened the door for data and voice communication for servicemen abroad.

As explained above, GEO, MEO, and LEO satellites provide communications links in addition to tasks as meteorology, navigation, and remote sensing. A fourth type, Highly Elliptical Orbit (HEO) satellites, also provides communications, but provides it primarily for the Polar Regions. As mentioned, many companies are investing heavily on the research and development of satellite technology, while other companies are aggressively incorporating its uses to increase market share (Buddie, 1).

d. Today's Satellite Communication Uses

In January 2001, Air Canada announced its in-flight e-mail and Internet surfing capabilities. Similar to how a person connects to the Internet at home, a passenger simply plugs into a connector on the airplane, but instead of dialing into an Internet service provider (ISP), the passenger dials into a Tensing Corporation ISP that is on the aircraft (Walton, 2001). Anyone who has traveled on Jet Blue knows that they also provide a satellite service. Specifically, Jet Blue provides DirecTV access to 24 television network channels. Although Jet Blue has not yet offered Internet service on its airplanes, the technology clearly exists.

Boeing Co. was about to launch its sky-high Internet service, but the project got delayed due to the New York and Washington DC attacks of September 11, 2001. *Connexion* by Boeing provides passengers Internet and Intranet access, television, and email services over U.S. territory and waters via a direct connection of an onboard transmitter and receiver antennae to geostationary satellites. (Technology) Although Boeing lost its original three primary partners due to the attacks, Germany's Lufthansa AG is an active partner in Boeing's Connexion broadband satellite services. Scott Carson, president of Connexion by Boeing, said, "This marks a new era for in-flight connectivity." (Mearian, 2002) In fact, corporate and government aircraft also use satellite communications technology with Inmarsat Swift64 (Inmarsat).

Passengers at sea can also access their e-mails, get ship-to-shore video feeds and radio broadcasts, and Internet access. Maritime Telecommunications Network, Inc. provides voice, data, Internet access, and Inmarsat services, not only to commercial cruise lines like Norwegian Cruise Lines, but also to the United States Navy (Wireless

Internet Access at Sea, 2002). Using satellite technology to send and receive data signals on aircraft and at sea marks its strengths in mobility applications such as are needed in war and natural disasters.

D. VISION FOR FUTURE ELECTRONIC COMMERCE OR ELECTRONIC PROCUREMENT

1. Various Environments

Contracting officers may find themselves supporting operations in a variety of working environments from mature environments with heavy communications infrastructure to austere or immature environments with little to no communications infrastructure. Regardless of the available infrastructure, a contracting officer must be prepared to order supplies and services from anywhere on Earth at anytime.

a. Mature Environment

A mature contracting environment offers an intact, well-developed communication and sophisticated distribution system that can rapidly respond to changing requirements. In many cases, mature contracting environments already have existing contracting offices in place with outlets, phone lines, fax machines, computers and many other technological tools to make contracting easy. Examples of these types of offices can be found in locations like Korea or Western Europe where they have been in place for many years.

A contracting officer in a mature environment can simply walk over to a computer already connected to the Internet in order to access DoD EMALL and the OMC. These types of situations don't usually present challenges for the typical contracting officer. In fact, contracting officers perform their daily contracting activities without worries of technological adolescence. However, a simple or even catastrophic change in the local environment could render the mature environment into an immature environment.

b. Immature Environment

An immature environment is usually located in an austere area that offers little or no established infrastructure with few experienced vendors. It is these types of environments that are a source of frustration for contracting officers. These contingency contracting environment can be found all over the world to include Somalia, Haiti, Kosovo, and Rwanda.

In fact, in April 1999, a contracting team sent to Kosovo faced just such an immature environment. A contracting team set up the JCC. The environment was so new that the team was provided a tent out of which they lived and worked. Unfortunately, it took the JCC a few days before they were provided with a generator. Also, it took several weeks to establish JCC communications because of Camp Bondsteel's wire shortage. Although a Mobile Subscriber Equipment (MSE) line was eventually run to the JCC, it kept getting cut, repeatedly knocking out communications. It took six months before Camp Bondsteel deployed telephone poles, providing Internet access across the camp.

These austere conditions presented extreme contracting challenges for the JCC. It took an additional six months before the JCC was given satellite phones to aide in their communications needs. In fact, the Iridium satellite phones allowed the JCC to communicate with vendors in the United States and Europe, and made credit card purchases easier to complete. Because Kosovo had an unreliable cellular network, the satellite system proved to be a reliable source of voice and data communications, not only in Kosovo, but potentially in future contingent, immature environments (Phillips, 2001). Therefore, if incorporated in the planning stage, a deployed contracting officer can conceivably be up and running in as little as a few hours, as opposed to the months that it took the JCC at Camp Bondsteel.

c. Natural Disaster Environments

Natural disasters like tornadoes, hurricanes, earthquakes, and floods can damage established infrastructure and often turn a mature environment into an immature environment. Natural disasters often pose communication challenges for rescuers and

people ordering supplies. Depending on the level of infrastructure damage, people can communicate using landlines, wireless technology, or even satellite technology.

If existing landlines are still operational after a natural disaster, it makes economical sense to use those lines for data and voice communications. However, if landlines are damaged, using wireless technology makes sense because it's less expensive than satellite technology. Determining which technology to use depends not only on existing infrastructure, but also convenience and expenses involved with each mode of communication.

When Tropical Storm Allison hit Texas in 2001, the Federal Emergency Management Agency (FEMA) setup their temporary headquarters in a Houston mall using hundreds of laptops, wireless phones and wireless modems to maintain communications. FEMA claimed that instead of taking the typical three to five days to setup a field office, that using wireless technology took less than one day to setup and was less expensive to incorporate in the long term (Dean, 2001). Using wireless technology in this case requires using repeater stations on towers. Therefore, if the natural disaster damaged the local area repeater stations, another communication source would be necessary.

While wireless technology helped FEMA complete their tasks, Arizona Fire Fighters used Iridium Satellite phones to stay in touch with each other and base units. The fire fighters knew that constant communication was necessary to help coordinate their efforts to fight the fires, but needed the reliability of satellite phones in the forests as opposed to the spotty unreliable coverage of cellular service or non-existent terrestrial service ("Fire Fighters Use", 2002).

d. Miscellaneous Environments

Iridium's Satellite phones provide easy to use voice and data communications in many markets to include emergency services, Government, Maritime (Commercial and Leisure), Mining, Forestry, Oil & Gas, Humanitarian relief, and many more ("Corporate", 2002). In fact, military personnel have used satellite phones to make

morale calls while on maneuvers, and news stations have used satellite technology to broadcast live news reports from remote areas like Iraq ("Iridium Outlook", 2003).

In an Iridium customer testimonial, the Himalayan Rescue Association uses satellite phones at their Everest base camp in Nepal to communicate with doctors and call in swift air evacuations. In a similar use of satellite phones in austere locations, the Defense Information Systems Agency (DISA) noted that satellite phones were used in a coordinated effort between various agencies to include the National Science Foundation and the United States Air Force in rescuing Dr. Ronald S. Shemenski from the South Pole. Due to the lack of cellular service in Antarctica, satellite phones were a critical link in the communications efforts between the South Pole station and rescue agencies involved in flying the doctor out ("Iridium Provides Vital", 2001).

2. Contingency Contracting Support Plan (CCSP)

Under the deliberate and crisis action planning, the process of planning a joint operation is planned for contingent military operations. One of the topics discussed is the Contingency Contracting Support Plan (CCSP), which ensures that contracting procedures are carried out under different circumstances to include:

- Disaster relief efforts,
- Rapid deployment logistics support, and
- Support of deployed U. S. troops overseas.

The CCSP ensures that contracting officers incorporate the proper logistics plans as part of their preparation before deployment. Following is a list of some topics addressed in the CSSP:

- Location and structure of the contracting offices,
- Manpower, equipment and supplies required for contracting support,
- Types of supplies, services, and construction customers can expect to receive,

The Service Federal Acquisition Regulations address that each Contingency Contracting Office (CCO) must maintain a Contingency Contracting Support Kit (a detailed list is provided in Appendix F). These kits contain items like forms, a laptop

computer, fax and copier machines, communications equipment, and other pertinent office supplies; however, they do not specify satellite equipment (Defense Acquisition Deskbook, 2002). In fact, the Army Federal Acquisition Regulation Supplement (AFARS) states that contracting officers should make arrangements for some type of mobile communication network devices to ensure that they can be reached by Army units and organizations, however it doesn't specify satellite capable devices (AFARS, 4-3.a.3).

3. EPPS – Electronic Procurement Palette Setup

The facts are unclear as to how the Contingency Contracting Support Kits are transferred abroad. But it is likely that for the kit to move into the contingency environment, the kit must be included in the TPFDL in order to be deployed on a palette aboard an Air Force or civilian aircraft. The deployment kit should specify in addition to the above items, those tools needed to access the Internet so that the Contracting Personnel have quick access to the OMC. As a minimum to support the OMC, the Contingency Contracting Support Kit should include:

- Laptop computers,
- Cellular and satellite voice and data capable phones with activated service agreement (civilian or military satellites),
- Data kit to link the laptop to the phone, (Voice and Data Services)
- Printer, fax, copier, and scanner (all in one), and
- Power generator with local and United States type outlets

These items as part of a so-called Electronic Procurement Palette Setup (EPPS) would ensure that contracting personnel are up and running within hours of arriving at their contingency operating site. Granted, the EPPS items do not include everything for every possible scenario, but could have prevented some of the problems experienced by the contracting personnel at Camp Bondsteel, specifically the huge delay in establishing communication networks. The objective of the joint action planning ensures that all contingency operations, to include the contracting functions, take into consideration all the logistics support necessary to complete those functions.

Satellite voice and data technology is being used in almost every imaginable situation from government and military uses to everyday business uses. Satellite technology is definitely the missing link for users that cannot receive a cellular signal because of austere, damaged, and immature environments. The company Iridium, for example, offers their Smart Connect ^{TM} direct Internet service that features an always-on mode that allows users to have 24 hour, continuous Internet connection without being charged for continuous airtime charges ("Iridium Launches Global", 2001). This feature alone makes satellite connectivity the answer to accessing the OMC while deployed overseas or in any variety of immature environment situations.

Furthermore, Iridium is only one satellite Communications Company amongst many. Granted, satellite service might be costly today, however, as competition increases, the price for satellite service will decrease just as the cellular service has over the past ten or so years. Eventually, the military should incorporate satellite technology into all contingency plans to ensure one hundred percent satellite voice and data communication from anywhere in the world.

APPENDIX A. FEDERAL AGENCY SITES

- FAA Chief Information Officer (AIO)
- FAA Office of Information Technology (AIT)
- DOE Computer Incident Advisory Capability (CIAC)
- Computer Security Technology Center (CSTC)
- Federal Computer Incident Response Capability (FedCIRC)
- Information Design Assurance Red Team (IDART)
- Information Operations Red Team and Assessments (IORTA)
- Information Infrastructure Task Force (IITF)
- NASA Automated Systems Incident Response Capability (NASIRC)
- National Institute of Standards and Technology (NIST) Computer Security Division
- NIST Computer Security Resource Clearinghouse
- National Telecommunications and Information Administration (NTIA)
- Plans, Customer Service, and Information Assurance Division (N5)
- Security Proof of Concept Keystone (SPOCK)
- ICAT Metabase
  ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DOD/MILITARY SERVICE SITES

- Information Assurance Support Environment
- Office of Technology Transition
- Dual Use S&T
- Defense Production Act Title III
- Department of Defense Computer Emergency Response Team (DoD CERT)
- DISA Information Assurance Support Environment
- OSD C3I Home Page
- Defense Advanced Research Projects Agency (DARPA)
- Rainbow Series Library
  Performs trusted product evaluations. The program focuses initially on products with features and assurances characterized by the Trusted Computer System Evaluation Criteria (TCSEC) C2 level of trust
- School of Information Warfare and Strategy
- Naval Postgraduate School Information Warfare Academic Group (IWAG)
- National Security Study Group (NSSG)
  The National Security Study Group or Hart-Rudman Commission is a Federal Advisory Commission charged with thinking comprehensively and creatively about how the United States should provide for its national security in the first quarter of the 21st century.
- NPS Joint C4I Systems
- SPAWAR Information Warfare-Protect Systems Engineering Division
- The Joint C4ISR Battle Center
  The Joint C4ISR Battle Center (JBC) has an assessment team that conducts assessments on IA and CND technological solutions that enhance interoperability and NETOPS for the deployed JTF.
- Current Focus
  DTIC's vision for a new Web resource, titled Current Focus, is designed to provide authoritative, publicly releasable information focused on topic areas within the general realm of homeland security. As the site development progresses unclassified/limited information will be added. This information will be gathered

from numerous sources both within and external to the Government, and will be validated by appropriate experts. DTIC is uniquely positioned to provide expertise and commitment in a manner that will offer material support to the leaders and decision makers of homeland security. DTIC's information specialists and Government, private sector, and academic partners will add value to existing information resources by selecting relevant content from authoritative sources, validating it as necessary, and presenting it in an inclusive, yet protected Web environment. The site will be on a secure Web server, with encrypted information transmission. To provide further security, a registration process will assure that only authorized users are able to obtain access. At the present time, only individuals with e-mail addresses ending in .mil or .gov or those listed in the Defense Manpower Data Center (DMDC) database are able to access the site. Please go to the following URL to register: https://focus.dtic.mil/help/help_account.html

APPENDIX C. COMMERCIAL SITES

- Internet Traffic Report
  The Internet Traffic Report monitors the flow of data around the world. It then displays a value between zero and 100 and is updated ever 15 minutes. Higher values indicate faster and more reliable connections.

- CERT Coordination Center
  Studies Internet security vulnerabilities, provides incident response services to sites that have been the victims of attack, publishes a variety of security alerts, researches security and survivability in a wide-area-networked computing environment.

- Electronic Privacy Information Center Home Page
  Public interest research center in Washington, D.C.

- Information Security Portal
  This site provides information concerning the topic of Information Warfare including security tools, the law and legal issues, espionage, terrorism, and information operations.

- Internet Privacy Coalition

- International Computer Security Association (ICSA)
  ICSA is known worldwide as an objective source for security assurance services.

- The Terrorism Research Center

- Cybersoft White Papers
  White Papers written on the subjects of viruses, antivirus, Unix, computer security and CyberSoft products.

- Glossary of Information Warfare Terms

- Cyberwar - Information warfare and psychological operations
  Provides information on the topics of propaganda analysis, online journals, index and metapages, general resources, intelligence agencies, and articles and documents.

- Reliable Software Technologies (RST): Information Warfare

- RAND National Security Research Division
  This division conducts research for RAND's national security research sponsors other than the U.S. Army and Air Force. It contains the National Defense Research Institute (NDRI), RAND's federally funded research and development center for the Secretary of Defense, the Joint Staff, and the defense agencies.

- Forum of Incident Response and Security Teams (FIRST)
  FIRST brings together a variety of computer security incident response teams from

Government, commercial, and academic organizations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

- International Association for Cryptologic Research (IACR)
  The International Association for Cryptologic Research (IACR) is a non-profit scientific organization whose primary purpose is to further research in cryptology and related fields.

- International Biometrics Industry Association (IBIA)

- Military Information Services, Inc.
  Military Information Services (MIS) is a Washington DC based consulting and sales group. Provides open source intelligence data retrieval, collection and analysis products in addition to a full range of editorial support services for defense and intelligence organizations, research centers, libraries, trade publications and information groups worldwide.

- Common Vulnerabilities and Exposures
  A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

APPENDIX D. GOVERNMENT AND PROFESSIONAL AGENCIES AND RESEARCH CENTERS

1. Air Force Computer Emergency Response Team (AFCERT)
2. Air Force Information Warfare Center (AFIWC)
3. Army Computer Emergency Response Team (ACERT)
4. Association for Computing Machinery (ACM) Special Interest Group on Security, Audit, and Control (SIGSAC)
5. Australian Computer Emergency Response Team (AU. S.CERT)
6. Center for Secure Information Systems (CSIS) at George Mason University
7. Central Intelligence Agency (CIA)
8. Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University
9. Computer Emergency Response Team for the German Research
10. Network (DFN-CERT), German Federal Networks CERT, Germany
11. Computer Operations, Audit, and Security Technology (COAST)
12. Project at Purdue University
13. Computer Security Research Laboratory at the University of
14. California, Davis
15. Computer Security Technology Center at the Lawrence Livermore
16. National Laboratory
17. Computing Professionals for Social Responsibility (CPSR)
18. Defense Advanced Research Projects Agency (DARPA)
19. Department of Defense Computer Emergency Response Team (DoD CERT), Defense Information Systems Agency (DISA)
20. Department of Energy, Computer Incident Advisory Capability (CIAC)
21. Forum of Incident Response and Security Teams (FIRST)
22. IEEE-CS Technical Committee on Security and Privacy
23. IFIP Technical Committee 6 on Communication Systems
24. IFIP Technical Committee 11 on Security and Protection in Information Processing
25. IFIP Working Group 11.3 on Database Security
26. IFIP Working Group 11.4 on Network Security
27. Information Sciences Institute, University of Southern California School of Engineering
28. Information Security Research Centre at Queensland University of Technology, Australia
29. Information Systems Audit and Control Research at CalPoly Pomona
30. Institute for Computer & Telecommunications Systems Policy at George Washington University
31. International Association for Cryptologic Research
32. International Computer Security Association (ICSA)
33. Joint Task Force for Computer Network Defense (JTF-CND)

34. Lawrence Berkeley National Laboratory
35. Los Alamos National Laboratory
36. Marine Forces Computer Network Defense (MARFOR-CND)
37. Marine Corps Intrusion Detection Analysis Section (MIDAS)
38. National Aeronautics and Space Administration (NASA) Automated Systems Incident Response Capability (NASIRC)
39. National Institute of Standards and Technology (NIST) Computer Systems Laboratory
40. National Security Agency (NSA)
41. Naval Computer Incident Response Team (NAVCIRT)
42. Navy Research Laboratory Center for High Assurance Computer Systems (Naval Research Laboratory [NRL])
43. Navy Space and Naval Warfare Systems Command (SPAWAR)
44. Purdue University Computer Emergency Response Team (PCERT)
45. SIRENE: Slcherheit in RechnerNEtzen (Security in Computer Networks) at the University of Hildesheim/IBM Zurich
46. SURFnet Computer Emergency Response Team (CERT- N L), Netherlands
47. Swiss Academic and Research Network CERT, Switzerland (SWITCH-CERT)
48. Texas A&M University

APPENDIX E. IT SECURITY RESPONSIBILITIES

A. CHIEF INFORMATION OFFICER (CIO)

Evaluates overall IT security requirements and provides specific direction to Division Administrators, IT Managers, system developers, and users relative to the risk evident in the IT security platform. The CIO is responsible for all aspects of security compliance for IT systems. Specific duties include:

1. Provides direction for IT security policy.
2. Ensures compliance with IT security policy.
3. Ensuring information ownership is established for each IT system to include: accountability, access rights, and special handling requirements for systems containing sensitive or confidential information.
4. Approving alternative safeguards.
5. Ensuring employees are properly trained or provided training.

B. IT MANAGERS

Responsible for the secure operation of all systems, ensuring they are accessed, used, maintained, and when appropriate, disposed of according to approved security practices. Responsible for implementing internal system safeguards to ensure users are held accountable for their actions. General duties include:

1. Ensure all users and vendors have appropriate clearances, authorizations, and security training prior to being given access to an IT system.
2. Ensure safeguards are appropriate for system security and are addressed in system documentation.
3. Reviewing all proposed changes to system software and hardware to determine if security safeguards have been addressed.
4. Maintaining a current version of system documentation.

5. Assisting with the maintenance of agency-wide security policy.
6. Ensuring that protective measures are initiated if a security incident occurs.
7. Reporting significant security incidents to the CIO and IT Security Personnel.
8. Conducting regular evaluations of known system vulnerabilities to ascertain if additional safeguards are necessary.
9. When available, ensuring audit trail and intrusion detection reports are reviewed on a regular basis.
10. Directing the development and review of IT contingency/disaster recovery plans.

C. IT SECURITY PERSONNEL OR DESIGNEE

Appointed by the CIO and responsible for the secure operation of all systems, ensuring they are accessed, used, maintained, and disposed of according to approved security practices. General duties include:

1. Verifying IT users and vendors have appropriate clearances, authorization, and security training prior to being given access to an IT system.
2. Ensuring IT safeguards are appropriate for the system and are addressed in system documentation.
3. Reviewing all proposed changes to system software and hardware to determine if security safeguards are affected, reporting any discrepancies to IT Management and the CIO.
4. Reviewing and assisting with the maintenance of system documentation.
5. Maintaining an agency-wide IT security policy.
6. Initiating protective or corrective measures if an IT security incident occurs, and reporting significant incidents to the CIO, Internal Audit, and appropriate IT Management.

7. Evaluating known system vulnerabilities to ascertain if additional safeguards are needed.
8. Reviewing audit trails and intrusion detection reports, when available.
9. Assisting in the development of IT contingency/disaster recovery plans.
10. Initiating risk analysis at least every two years.
11. Providing assistance to other state agencies in the areas of risk analysis, IT security policy development, incident response and investigation, and user awareness.
12. Conducting annual compliance reviews to sustain optimal security levels.

D. SYSTEM ADMINISTRATORS

Systems Administrator is responsible for the administration of a computer system. They manage access to the system and observe the system for any signs of unusual activity. General duties include:

1. Assigning agency users appropriate access to IT systems.
2. Verifying users and vendors have appropriate clearances, authorization, and security awareness prior to being given access to a system.
3. Utilizing whatever safeguards are appropriate for, and approved by, IT Management for systems security.
4. Maintaining a working knowledge of any system under System Administrator authority and direct control, and a general knowledge of all other DAS systems.
5. Assisting in the review of proposed changes to system software or hardware when required in determining if security safeguards are affected. Report any discrepancies to IT Management and IT Security Personnel.
6. Assisting with the maintenance of systems documentation.
7. Assisting with the maintenance of agency-wide IT policy.

8. Initiating protective or corrective measures if a security incident occurs, and reporting all such incidents to IT Management and IT Security Personnel.
9. Evaluating known system vulnerabilities to ascertain if additional safeguards are needed.
10. Reviewing audit trail and intrusion reports daily.
11. Assisting in the development of IT contingency plans.
12. Ensuring that, whenever the system allows, the IT system screen displays a warning message before logon (minimum of one sentence) that lets the user know that unauthorized access to the IT system and software is prohibited. Example: "UNAUTHORIZED U. S.E OF THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE COLLECTED DURING MONITORING MAY BE U. S.ED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. U. S.E OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."

E. USERS

Individuals who have access to, or use of, any state computing resource are expected to:

1. Protect their passwords and not share them with others, unless directed by the Division Administrators or the CIO.
2. Protect their network and system IDs.
3. Assess their information for level of sensitivity and protect it.
4. Protect their unattended terminal or workstation, and log-off when not in use.
5. Protect against viruses by virus checking all disks and software from external sources.
6. Protect their equipment from abuse.
7. Protect their area by putting away sensitive materials when they are absent.

8. Protect their files by appropriately saving and storing them.
9. Protect their media through safe storage and destruction.
10. Protect against disaster by following disaster emergency procedures.
11. Report all security violations immediately to their supervisor.
12. Comply with all applicable laws and organizational policies.

F. SYSTEM ACCESS

1. All Networld systems will have an access control policy (facilities, systems, and information) that defines the intention and strategy of the organization to prevent unauthorized system access.
2. Employees, consultants, and contractors, who design, develop, operate, or maintain IT systems shall undergo appropriate background investigations and authorizations for access to system components, output, or documentation.
3. No Networld employee or vendor personnel shall allow or assist in the unauthorized access of any individual to a restricted area within Networld offices.
4. All visitors to restricted premises, not previously cleared or identified by badge, shall be escorted.

G. USE OF THE IT SYSTEM

1. All users of IT systems must receive appropriate clearances to use a system from IT Management, System Administrators, application administrators, or the IT Security Personnel or Designee. This permission must be written, which will include the assignment of a user account (User ID and Password) or issuance of a microcomputer. Users must immediately, following assignment, change their password.
2. All users of an IT system must receive security awareness training, either in a formal classroom setting or by other means such as user awareness brochures,

on-line or electronic mail training, or individual instruction from the IT personnel who installs or sets up the workstation.

3. All IT system use is for official business only as specified in Networld policy.
4. All users must report suspicious activity to their supervisor or IT Security Personnel. Suspicious activity includes suspected misuse of government resources; use of the system by an unauthorized party; illegal copying of software; or strange activity on a computer system which may be caused by a computer virus or other malicious logic.

H. MANAGEMENT OF USER IDS AND PASSWORDS

User IDs

1. Each User ID is to be assigned to only one person at a time.
2. User IDs are not to be shared with another person.
3. User IDs shall be a minimum of six characters.
4. A record of user assignment must be kept for a minimum of three years after a user leaves the organization.
5. Before reuse of a User ID, all previous access authorizations and their associated directories and files must be removed from the system.
6. A user shall have only three attempts to log into the system. After the maximum number of incorrect attempts, the system will lock the user out. Action from the System Administrator is to be required to reactivate the account.
7. Each user must acknowledge receipt of a User ID and Password by signing a statement that details his or her responsibility for protecting this information prior to being issued a password.
8. A User ID must be suspended by the System Administrator for any of the following reasons:
    a. Termination of employment or contract (within 24 hours).

b. Nonuse of account for six consecutive months.

c. Notification of security violation (by management direction).

d. As directed by the CIO.

Passwords

1. System password files should be protected as confidential information.
2. Passwords must never be stored in clear text.
3. The maximum lifetime for all passwords should be no longer than 90 days.
4. Passwords must be at least seven alpha and numeric characters in length and should contain both upper and lower case letters.
5. Passwords must not spell a common word or name.
6. Passwords must not be repeated within a 12-month period.
7. Users must not use personal information for their passwords (e.g., birth dates, home address, etc.).
8. Users are not to share passwords with anyone, unless directed by their manager or the CIO. Users will keep passwords safe and confidential at all times. Requisite protection consists of a combination of controls designed to ensure integrity, availability, and confidentiality.

I. HANDLING OF CONFIDENTIAL, SENSITIVE, OR GENERAL INFORMATION

1. All sensitive output, media, and media containers should be marked to accurately reflect the information classification: confidential, sensitive, or general. Confidential or sensitive information includes, but is not limited to passwords, encryption keys, program source code, financial transactions, and personnel records.

2. Confidential information is not to be sent via the Internet or transmitted by modem unless security controls, such as the appropriate level of encryption, are in place.
3. Recipients of confidential information shall be made aware of the classification of the information.
4. Transmission of confidential information shall be by means that preclude unauthorized disclosure.
5. Transmittal documents shall call attention to the presence of confidential attachments.
6. Records containing confidential information shall be transported in a manner that precludes disclosure of the contents.

J. MINIMUM SECURITY REQUIREMENTS

1. Access – System Administrators shall implement an access control policy that will positively identify each user who is authorized to access a system prior to granting access.
2. Accountability – Networld IT Management shall implement internal system safeguards to ensure users are held accountable for their actions. Individual application access authority is the responsibility of the application administrator. Where available, an automated audit trail shall be implemented that documents violations as follows:
    a. The identity of each person and device having access.
    b. The time of access.
    c. The user's activities.
    d. All activities that might modify, bypass, or negate safeguards.
    e. All relevant actions associated with period processing.
    f. Any changes to security level or categories of information.

3. Audit and Reporting – Where available, System Administrators shall maintain an audit trail so all actions affecting system security can be traced.
4. Electronic Mail – Electronic mail is primarily for business use. It is not to be used for the distribution of confidential information. It is not private and may be accessed by the state at any time. Networld email policy governs the acceptable use of the state's electronic mail systems.
5. Identification and Authentication – System Administrators shall identify each individual user of the system prior to allowing activity on that system, and establish passwords to authenticate the user's identity.
6. Internet Use – Use of the Internet is for state business. Networld's Policy governs the appropriate use of the Internet.
7. Labeling – Users shall label all information media and media containers with identifying information that accurately reflects what the information is, its level of sensitivity, and the current date.
8. Least Privilege – System Administrators and application administrators shall ensure IT systems and applications function in a manner that allows each user to have access only to information to which the user is entitled and no more. Open-access applications, such as time sheets, etc., may be accepted. Specifically, least privilege means that access is to be provided at the minimum level required for the user to perform their regular job duties.
9. Objects Reuse – System Administrators shall eliminate all residual information from a medium (page frame, disk sector, and magnetic tape) before reassignment of that medium from one subject to another.
10. Users – All users shall exercise good judgment, keeping in mind the particular sensitivity of the data, when sharing or reassigning media for reuse.
11. Physical Controls – Users shall protect hardware, software, documentation, and information from unauthorized disclosure, destruction, or modification.

12. Remote Access –The appropriate Division Administrator and the CIO, prior to gaining access, must approve remote access to Networld owned computers. Division Administrators shall assess each request and determine the risk, prior to requesting approval by the CIO. The IT Security Personnel or Designee must maintain documentation logs for all remote access. All access to Networld systems must conform to Networld's internal security policy.

13. Security Training and Awareness – At the direction of the CIO, the Networld IT Security Designee shall establish a security training and awareness program that will ensure all users responsible for IT systems or information are aware of proper operational and security-related procedures. IT security specific training may be delivered formally (individual or classroom) or through written communications.

K. COMPUTER SECURITY USER DECLARATION

I declare that I have read the Department of Administrative Services Information Technology Security Policy. Furthermore, I understand that I shall:

- Protect sensitive data/information by following applicable policies and procedures. Use passwords and keep them secret.
- Create passwords that are at least seven characters long, have both letters and numbers, which do not spell a word or a name, and do not contain personal data.
- Protect my computer by logging off when I am gone for the day or for extended periods of time and keep assigned equipment safe from harm.
- Protect equipment assigned to me by keeping it safe from harm.
- Scan all computer disks from home and external sources for viruses before I use them on my computer.
- Do not install any software or use hardware & software unless authorized.
- Protect my work area, media, and files, against all threats and report any incidents that occur to the CIO and IT Security Personnel or Designee.
- Not download software from the Internet unless specifically authorized to do so by the CIO or designee.
- Comply with all applicable laws and organizational policies and procedures.

I agree that by signing this document I am declaring that I have read and understand the Information Technology Security Policy, and that if I fail to follow mandatory requirements outlined in the Policy that I may be subject to personnel action or dismissal.

_____

Employee Sign and Date **Department Head Sign and Date**

_____

Employee (Please Print) **Department Head (Please Print)**

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. CONTINGENCY CONTRACTING SUPPORT KIT (AFARS, APPENDIX F)

F1. Planning. Each Contracting Officer and deployable contracting element must prepare a Contingency Contracting Support Kit. From previous experience, gathering procurement regulations, equipment, and forms upon deployment notification is too late. Units are already deploying to the site and procuring locally to respond to immediate needs. As a result, there may be many unauthorized purchases, which will create a workload upon the arrival of procurement personnel. Individual kits should be developed to specific scenarios or anticipated deployment areas, but all should include samples of a Price Negotiation Memorandum (PRM), a Buyer's Worksheet, and a Justification and Approval (J&A).

F2. The Contingency Contracting Support Kit:

a. Each kit should include a 90-day supply of the following forms and materials:

FOR INITIALLY DEPLOYING CONTRACTING ELEMENT:

- ✓ DA Form 3953, Purchase Request and Commitment (or service equivalent)
- ✓ DD Form 250, Material Inspection and Receiving Report
- ✓ DD Form 350, Individual Contracting Action Report (Over $25,000)
- ✓ DD Form 1592, Contract Cross Reference Data
- ✓ Standard Form 18, Request for Quotation
- ✓ Standard Form 26, Award/Contract
- ✓ Standard Form 30, Amendment of Solicitation/Modification of Contract
- ✓ Standard Form 33, Solicitation, Offer, and Award
- ✓ Standard Form 44, Purchase Order/Invoice/Voucher
- ✓ Standard Form 129, Solicitation Mailing List Application

- ✓ Standard Form 252, Architecture/Engineer Contract
- ✓ Standard Form 254, Architecture/Engineer and Related Services Questionnaire
- ✓ Standard Form 255, Architecture/Engineer and Related Services Questionnaire for Specific Project
- ✓ Standard Form 1165, Receipt for Cash/Sub-voucher
- ✓ Standard Form 1409, Abstract of Offers
- ✓ Standard Form 1442, Solicitation, Offer, and Award (Construction, Alteration or Repair)
- ✓ Standard Form 1449, Solicitation/Contract/Order for Commercial Items

FOR MAIN ELEMENT CONTRACTING OFFICE:

- ✓ DA Form 3953, Purchase Request and Commitment
- ✓ DD Form 250, Material Inspection and Receiving Report
- ✓ DD Form 350. Individual Contracting Action Report (Over $25,000)
- ✓ DD Form 448, Military Interdepartmental Purchase Request (MIPR)
- ✓ DD Form 448-2, Acceptance of MIPR
- ✓ DD Form 1057, Monthly Contracting Summary of Actions $25,000 or less
- ✓ DD Form 1155, Order for Supplies or Services
- ✓ DD Form 1593, Contract Administration Completion Record
- ✓ DD Form 1594, Contract Completion Statement
- ✓ DD Form 1597, Contract Close-out Checklist
- ✓ DD Form 1598, Contract Termination Status Report
- ✓ DD Form 1784, Small Purchase Pricing Memorandum
- ✓ NAVCOMP Form 2276, Purchase Request and Commitment

- ✓ Standard Form 18, Request for Quotation
- ✓ Standard Form 26, Award/Contract
- ✓ Standard Form 30, Amendment of Solicitation/Modification of Contract
- ✓ Standard Form 33, Solicitation, Offer and Award
- ✓ Standard Form 36, Continuation Sheet
- ✓ Standard Form 44, Purchase Order/Invoice Voucher
- ✓ Standard Form 1129, Solicitation Mailing List Application
- ✓ Standard Form 1165, Receipt for Cash Sub-voucher
- ✓ Standard Form 1402, Certificate of Appointment
- ✓ Standard Form 1403, Pre-award Survey of Prospective Contractor General
- ✓ Standard Form 1409, Abstract of Offers
- ✓ Standard Form 1410, Abstract of Offers Continuation
- ✓ Optional Form 1419, Abstract of Offers Construction
- ✓ Standard Form 1449, Solicitation/Contract/Order for Commercial Items

b. Because of probable language barriers, catalogs with pictures of supplies would be very helpful. Catalogs of hardware, construction supplies, automotive parts, among others, would be useful.

c. Administrative and other supplies, such as:

(1) Office supplies.

(2) Contract file folders.

(3) Handheld calculators and batteries.

(4) Field safe and/or security container.

(5) Flashlights and batteries.

(6) Sample contract formats.

(7) Authority to carry a sidearm (DA Form 2818, Firearms Authorization).

(8) SF 1402, Certificate of Appointment, issued by the Head of Contracting Activity (HCA) or the Principal Assistant Responsible for Contracting (PARC).

(9) A personal computer with CD-ROM (loaded with Defense Acquisition Deskbook AT&L Knowledge Sharing System), printer, power converter, extension cords, batteries, diskettes, paper, telephone line adapters, AC/DC adapter of the type used to connect to an automobile cigarette lighters, modem and other peripherals as required

(10) A manual typewriter with ribbons.

(11) A small photocopier.

(12) Facsimile machine.

(13) Polaroid camera, batteries, flash and film.

(14) Paper copies of the FAR, DFARS and appropriate service supplement.

d. Currency. The need for cash and U.S. Treasury checks should be determined in conjunction with the finance and accounting office. FAR 25.501 (a) requires that contracting officers make a determination if offshore contracts with local firms are to be paid in local currency. The use of U.S. currency requires a status of forces agreement with the Host Nation. Cash or U.S. Treasury checks will remain in the possession of finance and accounting office personnel. Authorized finance personnel or finance officer's representative will normally accompany the ordering officer to pay on the spot for goods received. A list of banking facilities available in the host country where U.S. cash and checks may be converted to local currencies would be helpful to both finance and supply personnel.

e. An EPPS as described in Chapter 5.

F3. Personal Protective and Communication Equipment.

(1) Mask, Protective CBR.

(2) Pistol, 9mm and/or Rifle, 5.56mm M16A2.

(3) Portable Phone, Cellular (preferable satellite capable).

F4. Logistical Support Data Bases: U.S. Army, Pacific is developing a database designed to identify potential sources of goods and services throughout the Pacific theater. The database is exportable and can be tailored to meet the needs of deployed units. Such databases may already be available at your site and should be used to supplement operations whenever possible.

F5. Voltage Requirements: Equipment may need to be adapted to use the local power sources so include these adapters in your kit. Also, bring along extra batteries/power packs in support of your equipment.

F6. Standard Specifications: When acquiring logistics and life support through contractual means, writing adequate specifications is one of the most difficult tasks the requiring activity will encounter. In order to simplify the process and provide assistance to requiring units, the following specifications are samples of standard requirements, which should be prepared in advance of any deployment. Standard specifications under contingency conditions only require the DA Form 3953, Purchase Request and Commitment (or service equivalent), attached with certified funds and authorized signatures.

Preparing standard specifications before deployment, with the coordination of requiring activities, expedites the process for the unit, clarifies and simplifies the work for the contracting office, and eliminates gold plating or excessive specifications that are beyond the government's minimum needs.

Note: AFARS Appendix F and The Naval Contingency Contracting Handbook recommend deploying with Procurement Instrument Identification Numbers (PIIN) from the sponsoring support contracting activity. This publication recommends that the PIINs be assigned within OMC for continuity in the contingency area of operation.

HOST NATION (HN) COMMODITY DESCRIPTIONS (SAMPLE)

These general guidelines are not detailed specifications as used for commercial contracting. It is understood that reasonable variations to conform to HN capabilities and the needs of the U.S. Army will be made so long as the safety and the health of U.S. personnel are not endangered.

PERMANENT FACILITIES

Office Space:

Will be heated to ____ C (+/□ 3 degrees C), lighted to a minimum of _____ lux at desk level, and have as a minimum.

a. Sufficient number of desks and chairs to accommodate _____ personnel.

b. Use of normal office provisions such as paper, pencils, typewriters, calculators, etc.

c. Access to telephones, copy machines, etc. as listed in the schedule.

d. Access to sanitary facilities.

Dining/Mess Facilities:

Will be heated to _____C (+/□ 3 degrees C), lighted to a minimum of _____ lux at table level and have as a minimum:

a. Sufficient number of wares (plates, bowls, glassware, spoons, knives, forks) and tables and chairs to accommodate the total number of personnel indicated.

b. Condiments such as, but not limited to, salt, pepper, sugar, and sauces.

c. Access to sanitary facilities.

Wash Rack:

Will have as a minimum:

a. Roof and sufficient space to accommodate the following vehicles:

b. Access to steam cleaners, water and electricity as follows:

c. Access to portable or fixed ramps.

CONTRACTED SUPPLIES AND SERVICES (SAMPLE)

UCC Specification F 0001 Forklifts:

1. Forklifts provided by the contractor for the stated rental period will be of commercial type that is equipped for outdoor use. The lifts must have the capability of lifting _____ kilos, to a minimum of 2.5 meters in height. In addition the equipment will be capable of maintaining stability on a 6 percent incline, while handling a load of the specified amount.

2. At the time of delivery the forklifts shall be in sound mechanical condition free of all known defects and ready immediate use. The equipment must meet all the applicable standards (i.e., government and trade unions) for safe operation.

3. The forklifts will be equipped with the following:

a. Gas/diesel powered engine.

b. Self sustained electrical system to include an electric starter.

c. Pneumatic tires (snow chains to be provided during winter if applicable).

d. Spark proof exhaust system.

e. Front and rear lights that will facilitate on road operations during hours of darkness.

f. Driver protection roll bar.

g. Adjustable forks.

h. Warning device (automatically activated when the lift is placed in reverse gear).

4. The contractor shall furnish all the transportation, labor, material, and supervision required for the delivery, operational test, repair and maintenance, and removal of the equipment through the end of the rental period. In addition, the contractor shall furnish all POL products, (with the exception of fuel). This is to include distilled water for batteries.

5. The contractor shall provide a point of contact for on call maintenance and/or replacement of equipment. The point of contact must be available from 0800 to 2100 to include Saturdays, Sundays and all local and American holidays (understand that some local customs may preclude the coverage desired). The contractor will provide all labor, material, and supervision required to keep the equipment in a serviceable and safe operating condition. Repair and maintenance may be performed on site, subject to coordination with the COR. If a forklift becomes inoperable due to the need for repair and/or maintenance, the contractor will be notified immediately. The contractor must respond, within six (6) hours after notification, to perform the repair and maintenance services. If repair and maintenance services cannot be performed within the same day, the contractor shall furnish a replacement unit. Equipment that remains inoperable for more than a 12-hour period will be considered not available for use and rental fees will cease until the equipment is repaired to a fully operational condition or replaced with a serviceable unit. The pickup and removal of inoperable equipment will be accomplished at contractor expense.

6. Acceptance of forklifts by the government. At the time forklifts are delivered to the Government, the contractor shall issue a form, written in English, for each forklift, which provides the user a means to annotate the conditions of the equipment. In addition, the contractor will provide general operating instructions, to include refueling procedures, how to check and add oil, proper operating techniques, and preventative maintenance procedures. The contractor and the COR will jointly inspect the equipment for completeness and will list all damage (to include scratches and dents, etc.) on the inspection form. The inspection form must be signed and dated by both the COR and the contractor as acknowledgment that the forklift was received by the government in the

condition described/annotated. A copy of the inspection form will be retained by the contractor and the COR for use during the joint inspection at the end of the rental period.

7. Return of forklifts to contractor. Upon expiration of the rental period, forklifts will be returned to the contractor, clean, and complete with all accessories. Utilizing the inspection form, a joint inspection will be conducted and all discrepancies will be noted. Both the COR and the contractor, or his authorized representative, will sign the inspection form to acknowledge the return of the equipment in the described condition. Reasonable wear and tear, as well as damages which are not annotated on the turn in inspection form, will not be considered as valid if the contractor later submits a claim against the government.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Army Federal Acquisition Regulation Supplement (AFARS) Manual No. 2, *Contingency Contracting*, Nov 1997

Air Mobility Command, *Air Mobility Command Global Reach for America 1999 Stakeholders Report*, Headquarters Air Mobility Command Public Affairs Office, 1999

AMC Website. www.public.amc.af.mil (October 2003)

Adams, Carlisle and Steve Lloyd, Understanding the Public-Key Infrastructure, Que Publishing, November 19, 1999 http://www.counterpane.com/pki-risks.htrni

Armstrong, Thomas, LCDR SC, USN, CJTF-HOA, Djibouti, September 2003

Bureau of National Statistics U. S. DOT, *National Transportation Statistics 2002,* Bureau of Transportation Statistics, (Washington, DC, 2002), table 1-44, 2002

Camm, Frank. New Challenges New Tools for Defense Decisionmaking, "Adapting Best Commercial Practices to Defense". RAND, Santa Monica, CA. September 2003

CJCS, Joint Doctrine for the Defense Transportation System (Joint Publication 4-01), 19 March 2003, p. vii

Conneen, Kevin, DLA Purchase Card Manager, Interview, 11 September 2003

Contingency Contracting Student Handbook (CCSH), CON 234, November 1999

Csorba, Rob, Submarine Logistics Supply Center Detachment, Pearl Harbor, Hawaii, e-mail, 12 September 2002

Davis, Aaron and Kristi Helm, "Worm targets Windows flaw" The Mercury News, August 11, 2003
http://www.siliconvalley.com/mld/siliconvalley/business/special_packages/6511962.htm

Debar, Herve, 3rd Annual International Workshop on Recent Advances in Intrusion Detection (RAID) October 2-5, 2000
http://www.raid-symposium.org/raid2000/

Debar, Herve, "Frequently Asked Questions on Intrusion Detection", IBM Zurich Research Laboratory, September 2003
http://www.sans.org/resources/idfaq/knowledge_based.php

Defense Science Board Task Force on Logistics Transformation. Office Of The Under Secretary Of Defense For Acquisition, Technology & Logistics (OUSD, AT/L) Washington, D.C., January 2001 (http://www.acq.osd.mil/dsb/log2.pdf)

Department of Defense, "Charge Card Task Force Final Report", Washington, DC, 27 June 2002

Department of Defense, *Defense Total Asset Visibility Implementation Plan*, November 1995

Department of Defense, "Government Purchase Card Concept of Operations", Washington, DC, 31 July 2002

Department of Defense Information Analysis Center Report on Intrusion Detection 2002 http://iac.dtic.mil/iatac/pdf/reports/intrusion_detection.pdf

Department of Defense, "Joint Report of the Purchase Card Financial Management Team and the Purchase Card Integrated Product Team to the Undersecretary of Defense (Acquisition and Technology) and the Under Secretary of Defense (Comptroller)", Washington, DC, 26 February 1997

Department of Defense, Office of the Inspector General, "Acquisition, Controls Over the DoD Purchase Card Program", Arlington, VA, 29 March 2002

Department of Defense, Purchase Card Website

DHL Express. http://www.dhl.com/us/about/ (October 2003)

DoD EMALL website. www.emall.dla.mil (October 2003)

DTS Website. http://www.dtic.mil/doctrine/jel/new_pubs/jp4_01.pdf (October 2003)

Ebright, Sonya, FISC Puget Sound Washington Credit Card Branch Manager, e-mail 12 September 2002

e-Week Enterprise News and Reviews, *Application Hardening Checklist*, E-week.com magazine; Article 2, March 25, 2002 http://www.eweek.com/article2/0,4149,35208,00.asp

Federal Register, Volume 68, Number 190, *Federal Acquisition Regulation; Electronic Commerce in Federal Procurement*, 01 October 2003

FedEx Express webpage, http://www.fedex.com/us/about/express/history.html/ (September 2003)

Field Manual Number 100-7, ***Decisive Force:*** *The Army in Theater Operations*, 31 May 1995

Flournoy, Michele A., *"Quadrennial Defense Review 2001 Working Group"*. Institute for National Strategic Studies National Defense University. November 2000

Gansler, Jacques S., *"A Vision of the Government as a World-Class Buyer: Major Procurement Issues for the Coming Decade",* The PricewaterhouseCoopers Endowment for The Business of Government. January 2002

Gansler, Jacques S. "A Vision of the Government as a World-Class Buyer: Major Procurement Issues for the Coming Decade". New Ways to Manage Series. PricewaterhouseCoopers Endowment for the Business of Government. Arlington, VA. January 2002

Graham, Thomas, Networld Exchange COO, e-mail, 27 October 2003

Graham, Thomas, Networld Exchange COO, interview, 2 October 2003

Graham, Thomas, Networld Exchange COO, e-mail, 3 November 2003

Grandjean, Philippe J., "An Assessment of the World Wide Express (WWX) Program and its Effects on Customer Wait Time and Readiness", pages 37-59, June 200.

GTN Website. www.gtn.transcom.mil (October 2003)

Harris, Joe, European Purchase Card Manager, e-mail, 16 September 2003

Headquarters Air Mobility Command, World Wide Express Small Package Service Contract, F11626-98-D-0030-31, 30 June 1998

Hodges, Cody, LCDR SC, USN, COMFISCS, San Diego, CA, October 2003

http://purchasecard.saalt.army.mil/Fraud/summaries.htm

http://naples.navy.mil/nrcc/purchase card/htm

Information Assurance Technical Framework Forum (IATFF), Chapter 6 Section 5 Ver 3.1. http://www.iatf.net/framework_docs/version-3_1/docfile.cfm?chapter=ch06s5

International Chamber of Commerce (ICC) http://www.iccwbo.org (2002)

Joint Publication 4-0, *Doctrine For Logistics Support of Joint Operations*, 06 April 2000

Joint Publication 4-08, *Joint Doctrine for Logistics Support of Multinational Operations*, 25 September 2002

JTAV Website, October 2003, www.defenselink.mil/acq/jtav/appendxe.pdf

Kelman, Steven. "Contracting at the Core". Federal Focus, 30 July 2001

Kinney, Michael, LCDR CEC, U. S.N, Transportation Officer, USNAVCENT, Bahrain, October 2003

Kirk, Pierre. World Wide Express (WWX) 2: More About This New Tool for the Transporter's Toolbox, The Navy Supply Corps Newsletter, June/July/August 2002

Leard, Thomas E., "Competing Goals of the Governmentwide Purchase Card Program: Customer Satisfaction, Vendor Rotation, Fair and Reasonable Pricing, Master's Thesis", Naval Postgraduate School, Monterey, CA, June 1998

MARAD Website, October 2003, www.marad.dot.gov

McGowan, Major B. D., USMC, "After Action Report for Operation Iraqi Freedom", 18 AUG 2003, page 7

McMahon, Neal P., The Impact of the Purchase Card Program of Increasing the Micro-Purchase Threshold and Simplified Acquisition Threshold within the Federal Acquisition Streamlining Act of 1994, Master's Thesis, Naval Postgraduate School, Monterey, CA, December 1995

Microsoft Exchange Server Security Bulletin Summary for October; Version 1.0 Released October 15, 2003
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/exc oct03.asp

Microsoft Operations Manager (MOM) for IT Professionals, October 2003
http://www.microsoft.com/mom/

MSC Website, October 2003 www.msc.navy.mil

NAVSUP Instruction 3230.37B, *Naval Contingency Contracting Program*, Naval Supply Systems Command, 11 July 2003

NAVSUP Instruction 4200.85C, *DoN Simplified Acquisition Procedures*, Naval Supply Systems Command, September 1995

NAVSUP Publication 713, *The Naval Contingency Contracting Handbook* (NCCH), May 1997

Networld Exchange, “Purchase Card Initiative Submission Information”, Networld Exchange, San Diego, CA, 2002

Networld Exchange, “Purchase Card Statement of Work”, Networld Exchange, San Diego, CA 2002

NFAF Website, October 2003, www.nvr.navy.mil.

Northcutt, Stephen, *Frequently Asked Questions on Intrusion Detection*, System Administration, Audit, Network, Security Institute (SANS), July 2003 http://www.sans.org/resources/idfaq/network_based.php

Office of the Inspector General, DoD, “Controls Over Government Bills of Lading”, Report Number 98-016, 03 November 1997

Office of the Inspector General, DoD, “DoD Workforce Reduction Trends and Impact”, Report Number D-2000-088, 29 February 2000

Office of the Inspector General, DoD, “Standard Procurement System—Use and User Satisfaction”, Report Number D-2001-075, 13 March 2001

Paquette, Richard, LCDR, SC, USN, NAVAIR, October 2003

Procurement Policy, Committee on Government Reform, House of Representatives, 22 May 2001

Richardson, Robert, Editorial Director; “2003 CSI/FBI Computer Crime and Security Survey” Computer Security Institute May 29, 2003 http://www.gocsi.com/db_area/pdfs/fbi/FBI2003.pdf

Robert D. Paulus, “’A Full Partner’-Logistics and the Joint Force” Army Logistician. July-August 2003. Army Logistics Management College, Fort Lee VA

Smith, James, Outline of Financial Alternatives, Networld Exchange, San Diego, CA, 2002

TRANSCOM Public Website, October 2003, http://www.transcom.mil/,

The Cyber Security Research and Development Act of 2002, Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST) http://csrc.ncsl.nist.gov/pcig/cig.html

United States, Department of Defense. Joint Vision 2002. U. S. Government Printing Office, Washington D.C., June 2000

United States Transportation Command Handbook 24-2, "Understanding the Defense Transportation System", Third Edition, September 2000, page 2

Untermann, Maria, Transportation Dept, DLA, September 2003

UPS website, October 2003, http://www.ups.com/

U.S. General Accounting Office, Report to Congressional Requestors, "Purchase Cards, Control Weaknesses Leave Two Navy Units Vulnerable to Fraud and Abuse", Washington, DC, November 2001

U.S. General Accounting Office, Report to Subcommittee on Readiness and Management Support, Committees on Armed Service, U.S. Senate, "Military Operations: Contractors Provide Vital Service to Deployed Forces But Are Not Adequately Addressed in DoD Plans", Washington, DC, June 2003

U.S. General Services Administration, "Blueprint for Success: Purchase Card Oversight", Washington, DC

U.S. Government Printing Office, "Oversight and Management of the Government Purchase Card Program: Reviewing Its Weaknesses and Identifying Solutions", Hearing Before the Subcommittee on Oversight and Investigations, One Hundred Seventh Congress, Second Session, Washington, DC, 1 May 2002

Valentine, Harold, Office of Humanitarian Relief Assistance, Interview, 11 September 2003

VeriSign, Inc. Whitepapers on Public Key Infrastructure (PKI) October 2003 http://www.verisign.com.au/whitepapers/enterprise/pki/diffl.shtml

West-Brown, Moira J, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, 'Handbook for Computer Security Incident Response Teams (CSIRTs)" 2nd Edition, April 2003, http://www.cert.org/archive/pdf/csirt-handbook.pdf

Womack, John S. "Contingency Contracting – A Commander's Logistics Force Multiplier". http://call.army.mil/products/trngqtr/tq4-00/womack.pdf

World Wide Express webpage, October 2003, http://amcpublic.scott.af.mil/wwx/wwx.htm/

Zirkle, Laurie, "Frequently Asked Questions on Computer Network Security (CNS)", Computational Science & Engineering (CSE) Department of Virginia Tech University August 2003 http://www.sans.org/resources/idfaq/host_based.php

LIST OF REFERENCES

Afuah, Allan. Internet: Business Models and Strategies. Illinois: McGraw Hill, 2003

Akyildiz, Ian F. "Handover Management in Low Earth Orbit (LEO) Satellite networks." Mobile Networks and Applications (1999): pages 301-310. Online. PDF. 10 Oct. 2003. Available: http://delivery.acm.org/10.1145/340000/337887/p301-akyildiz.pdf?key1=337887&key2=7035867601&coll=GUIDE&dl=ACM&CFID=13600901&CFTOKEN=24822703

Ananasso, Fulvio. "Satellite Systems for Personal Communication Networks." Wireless Networks (1998): pages 155-165. Online. PDF. 8 Oct. 2003. Available: http://www.ee.surrey.ac.uk/Personal/K.Narenthiran/documents/sat_sys/ananasso_paper.pdf

Army Federal Acquisition Regulation Supplement (AFARS) Manual No. 2 (Contingency Contracting) Paragraph 4-3.a.3

"Bluesocket BluePaper: Overview of Wireless Local Area Networking." Bluesocket: pages 1-6. Online. PDF. 8 Oct. 2003. Available: http://solutions.addictivity.com/files/bluesocket/Overview%20of%20Wireless%20Local%20Area%20Networking.pdf

Buddie, Paul. "Wireless Technology – Mobile Communications – Sat Data, and fleet." Verizon: pages 1-4. Online. Internet. 4 Sep. 2003. Available: http://www22.verizon.com/about/community/learningcenter/articles/displayarticle1/0,4065,1158z3,00.html

Brown, Bruce & Marge. "Wireless Cards Give your PC Access Anywhere." PC Magazine Fall 2003: 26-28

"Corporate Fact Sheet." Iridium Our Story (2002): n. pag. Online. Internet. 10 Oct. 2003. Available: http://www.iridium.com/corp/iri_corp-story.asp?storyid=2

Defense Acquisition Deskbook: DAU Contingency Contracting Course (CON234) Supplemental Materials, Mar 2002

"DoD Emall." Defense Logistics Information Service (2003): n. pag. Online. Internet. 19 Sep. 2003. Available: www.dlis.dla.mil/emall.asp

Dean, Joshua. "Wireless Technology Helps FEMA Handle Disaster Relief." GovExec.com (Jun. 2001): n. pag. Online. Internet. 1 Nov. 2003. Available: http://www.govexec.com/dailyfed/0601/062001j1.htm

Farley, Tom. "TelecomWriting.com's Telephone History Series." Telecom Writing (2003): page 1. Online. Internet. 7 Sep. 2003. Available: www.privateline.com/TelephoneHistory/History1.htm

"Fire Fighters Use Iridium to Communicate While Fighting Wildfires in Arizona." Iridium Customer Testimonials (2002): n. pag. Online. Internet. 30 Oct. 2003. Available: http://www.iridium.com/corp/iri_corp-testimonial-detail.asp?testimonialid=55

"FlyNet – Internet on Board." Lufthansa: n. pag. Online. Internet. 24 Oct. 2003. Available: http://cms.lufthansa.com/fly/de/en/inf/0,4976,0-0-781134,00.html

Golding, Leonard S. "Satellite Communications Systems Move Into the Twenty-first Century." Wireless Networks (1998): pages 101-107. Online. PDF. 10 Oct. 2003. Available: http://delivery.acm.org/10.1145/280000/274731/p101-golding.pdf?key1=274731&key2=8016867601&coll=GUIDE&dl=GUIDE&CFID=13601125&CFTOKEN=28295007

Gromov, Gregory R. "History of the Internet and WWW: The Roads and Crossroads of Internet History." Netvalley (2002): n. pag. Online. Internet. 9 Sep. 2003. Avalailable: www.netvalley.com/intval1.html

GSA Advantage. "Welcome to the New Advantage." GSA Advantage: n. pag. Online. Internet. 8 Oct. 2003. Available: www.gsaadvantage.gov/advgsa/information/page.jsp?BV_SessionID=@@@@@1666917489.1067682379@@@@&BV_EngineID=ccckadcjkjefgdhcflgcefmdgfhdfgl.0&keyName=ADV_TIPS&prevPage=/main_pages/start_page.jsp

"GSA Advantage." Verity (2001): n. pag. Online. PDF. 6 Sep. 2003. Available: http://wendolene.verity.com/customers/verticals/government/pdf/MK0412_VIA_GSA_Advantage.pdf

"Himalayan Rescue Association." Iridium Customer Testimonials (2003): n. pag. Online. Internet. 30 Oct. 2003. Available: http://www.iridium.com/corp/iri_corp-testimonial-detail.asp?testimonialid=63

"History of the Internet." n. pag. Online. Internet. 3 Sep. 2003. Available: www.netvalley.com/archives/mirrors/davemarsh-timeline-1.htm

Hogle, Lee. "Satellite Data Communications." Interlinx (May 2002): n. pag. Online. Internet. 4 Sep. 2003. Available: http://www.interlinx.qc.ca/leehogle/satellite.html

I Buy Broadband (2001): n. pag. Online. Internet. 10 Oct. 2003. Available: https://www.ibuybroadband.com/ibb2/consumer.asp

"Inmarsat." Swift64: n. pag. Online. Internet. 24 Oct. 2003. Available: http://www.inmarsat.org/swift64/pr_Swift64_Farnborough02.htm.

"Intel Launches Intel Centrino Mobile Technology." Intel (2003): n. pag. Online. Internet Press Release. 7 Oct. 2003. Available: www.intel.com/pressroom/archive/releases/20030312comp.htm

"Iridium Launches Global Satellite Data and Internet Services." Iridium Press (Jun. 2001): n. pag. Online. Internet. 10 Oct. 2003. Available: http://www.iridium.com/corp/iri_corp-news.asp?newsid=17

"Iridium Outlook Government and Military Edition." Iridium Press (Jun. 2003): n. pag. Online. Internet. 10 Oct. 2003. Available: http://www.iridium.com/corp/iri_corp-news.asp?newsid=64

"Iridium Provides Vital Communications for South Pole Rescue." Iridium Press (May 2001): n. pag. Online. Internet. 10 Oct. 2003. Available: http://www.iridium.com/corp/iri_corp-news.asp?newsid=20

Johnson, Robert. "Cyber Cafes Fail to Deliver Profits." ZDnet (Jun. 1999): n. pag. Online. Internet. 2 Oct. 2003. Available: http://zdnet.com.com/2100-11-514840.html

Leiner, Barry M. "A Brief History of the Internet." Internet Society (Aug. 2000): n. pag. Online. Internet. 4 Sep. 2003. Available: www.isoc.org/internet/history/brief.shtml

Living Internet. "Packet Switching History." n. pag. Online. Internet. 9 Sep. 2003. Available: www.livinginternet.com/i/iw_packet_inv.htm

Long, Larry & Nancy. Computers: Information Technology in Perspective. New Jersey: Prentice Hall, 2002

Mearian, Lucas. "Boeing Granted License for In-flight Web Access." CNN.com Sci-Tech (Jan. 2002): n. pag. Online. Internet. 11 Oct. 2003. Available: http://edition.cnn.com/2002/TECH/internet/01/01/boeing.license.idg/index.htmlM iller, Michael J. "Your Unwired World." PC Magazine Fall 2003: 58-62

Mingis, Ken. "Mickey Mouse Goes Wireless." CNN.com/Sci-Tech (Nov. 2001): n. pag. Online. Internet. 10 Oct. 2003. Available: http://solutions.addictivity.com/files/bluesocket/Overview%20of%20Wireless%20Local%20Area%20Networking.pdf

Moore, Alan. "Internet Connection Speed Comparison Chart." Summersault (2001): n. pag. Online. Internet. 12 Oct. 2003. Available: http://support.summersault.com/bandwidth_chart.html

Nauts. "Sputnik Satellites and Launch Vehicles." Nauts (2000): n. pag. Online. Internet. 7 Sep. 2003. Available: www.nauts.com/vehicles/50s/sputnik.html

Phillips, Mark E. "Contingency Contracting in Kosovo: Starting From Scratch." Army AL&T (2001): 22-24

Rohde, Laura. "In-flight Satellite Internet Service Coming Soon." CNN.com Sci-Tech (Apr. 2002): n. pag. Online. Internet. 11 Oct. 2003. Available: http://edition.cnn.com/2002/TECH/internet/04/11/in.flight.service.idg/

Shek, Eddie C. "Intelligent Information Dissemination Services in Hybrid Satellite-Wireless Networks." Mobile Networks and Applications (2000): pages 273-284. Online. PDF. 10 Oct. 2003. Available: http://www.cs.uml.edu/~kajal/courses/91.580-S03/papers/Shek.pdf

"Technology." Lufthansa: n. pag. Online. Internet. 24 Oct. 2003. Available: http://cms.lufthansa.com/fly/de/en/inf/0,4976,0-0-1067464,00.html

"The Basics of Wireless." pages 1-16. Online. PDF. 10 Oct. 2003. Available: http://www.formulasys.com/assets/Whitepapers/Basics-of-Wireless_Formulasys.pdf

"The Invention of the Telegraph." n. pag. Online. Internet. 6 Sep. 2003. Available: www.upgradedays.ro/lucrari/Stasisin_Loredana_Elena/Libera/invention.htm

"The Transatlantic Cable." History Magazine: n. pag. Online. Internet. 6 Sep. 2003. Available: www.history-magazine.com/cable.html

Varney, Alan L. "Telegraph." Netvalley: n. pag. Online. Internet. 5 Sep. 2003. Available: www.netvalley.com/archives/mirrors/telegraph__radio_timeline-3.htm

"Voice and Data Services." Globalstar U. S.A: n. pag. Online. Internet. 10 Oct. 2003. Available: http://www.globalstarusa.com/services/data/

Walton, Marsha. "Airline Travelers to go Online While En Route." CNN.com Technology (Jan. 2001): n. pag. Online. Internet. 11 Oct. 2003. Available: http://edition.cnn.com/2001/TECH/computing/01/23/inflight.internet/index.html

Williams, Bernard. "The Roots of Packet Switching Networks." Unix Review (Jun. 2001): n. pag. Online. Internet. 9 Sep. 2003. Available: www.upgradedays.ro/lucrari/Stasisin_Loredana_Elena/Libera/invention.htm

"Wireless Internet Access At Sea." Norwegian Cruise Line (Dec. 2002): n. pag. Online. Internet. 11 Oct. 2003. Available: http://www.groupcruise.com/News/wireless_internet_access_at_sea.htm

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3PL	Third Party Logistics
ACSA	Acquisition and Cross-Servicing Agreements
AFARS	Army Federal Acquisition Regulation Supplement
AICPA	American Institute of Certified Public Accountants
AIS	Automated Information Systems
AIT	Automated Information Technology
AMC	Air Mobility Command
AO	Approving Official
APC	Agency Program Coordinator
ARPA	Advanced Research Project Agency
ASC	Administrative Service Charge
BOA	Basic Ordering Agreement
BPA	Blanket Purchase Agreement
CA	Certification Authority
CACB	Combatant Commander Acquisition And Contracting Board
CCO	Contingency Contracting Officer
CCSP	Contingency Contracting Support Plan
CER	Currency Exchange Rate
CERT	Computer Emergency Response Team
CHE	Container Handling Equipment
CNS	Computer Network Security
COCOM	Combatant Command (Command Authority)
COMLOGFORNVCENT	Commander, Logistics Forces, Naval Forces Central Command
CONUS	Continental United States
CRAF	Civil Reserve Aircraft Fleet

CRC	Cost Reimbursable Contractor
CS	Combat Support
CSE	Computational Science & Engineering
CSI	Computer Security Institute
CSRC	Computer Security Resource Center
CSRD	Cyber Security Research and Development Act
CSS	Combat Service Support
CUL	Common-User Logistics
DACA	Designated Approving and Certification Authority
DCA	Defense Communications Agency
DDP	Director, Defense Procurement
DEBX	Defense Electronic Business Exchange
DHL	Dalsey, Hillblom and Lynn
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DLIS	Defense Logistics Information Service
DoD	Department of Defense
DODIG	Department of Defense Inspector General
DSL	Digital Subscriber Line
DTR	Defense Transportation Regulation
DTRACS	Defense Transportation Reporting and Control System
DTS	Defense Transportation System
EDI	Electronic Data Interchange
EEC	European Economic Community
EECT	Early Entry Contracting Team
ELSF	Expeditionary Logistics Support Force
EO	Executive Order

EPPS	Electronic Procurement Palette Setup
FAST	Forward Area Support Teams
FAR	Federal Acquisition Regulation
FASA	Federal Acquisition and Streamlining Act
FBI	Federal Bureau of Investigation
FedBizOpps	Federal Business Opportunities
FedEx	Federal Express
FEMA	Federal Emergency Management Agency
FSS	Fast Sealift Ships
GAO	General Accounting Office
GATES	Global Air Transportation Execution System
GCSS	Global Control Support System
GDP	Gross Domestic Product
GEO	Geostationary Earth Orbit
GFM	Global Freight Management
GPE	Government Wide Point of Entry
GPS	Global Positioning System
GSA	General Services Administration
GTN	Global Transit Network
GWAC	Government-wide acquisition contracts
HCA	Head of Contracting Activity
HAZMAT	Hazardous Materials
HEO	Highly Elliptical Orbit
HNS	Host Nation Support
HVAC	High Voltage Alternating Current
IATAC	Information Assurance Technology Analysis Center
IATFF	Information Assurance Technical Framework Forum
IBCC	International Bureau of Chambers of Commerce
IC	Interchange Convention

ICC	International Chamber of Commerce
IDIQ	Indefinite Delivery, Indefinite Quantity
I.M.P.A.C.	International Merchant Purchase Authorization Card
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Providers
ISL	Intersatellite Links
IT	Information Technology
ITS	Intelligent Transportation System
ITV	In-Transit Visibility
JAB	Joint Acquisition Board
JACB	Joint Acquisition and Contracts Board
JARB	Joint Acquisition Review Board
JCC	Joint Contracting Center
JIT	Just-In-Time
JLCC	Joint Logistics Coordination Center
JOA	Joint Operations Area
JTAV	Joint Total Asset Visibility
JTF	Joint Task Force
JTLM	Joint Theater Logistics Management
JV	Joint Vision 2020
KBR	Kellogg Brown and Root
LAN	Local Area Network
LEO	Low Earth Orbit
LIPS	Logistics Information Processing System
LMSR	Large, Medium Speed Roll-on/Roll-off
MAC	Multiple Award Task Order Contract
MACB	Multinational Acquisition and Contracting Board
MACOM	Major Command

MACTS	Maintenance Activity and Cost Tracking System
MARAD	Maritime Administration
MBSA	Microsoft Baseline Security Analyzer
MEO	Middle Earth Orbit
MHE	Material Handling Equipment
MJLC	Multinational Joint Logistic Center
MNF	Multinational Force
MNFC	Multinational Force Commander
MNL	Multinational Logistics
MNLC	Multinational Logistic Center
MOM	Microsoft Operations Manager
MOOTW	Military Operations Other Than War
MSE	Mobile Subscriber Equipment
MTW	Major Theater War
NAF	Non-Appropriated Funds
NFAF	Naval Fleet Auxiliary Force
NASA	National Aeronautics and Space Administration
NAVAIRTERM	Naval Air Terminal
NIST	National Institute of Standards and Technology
NPR	National Performance Review
NPS	Naval Postgraduate School
OCONUS	Outside the Continental United States
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OMC	Open Market Corridor
OO	Ordering Officer
OPC	Organization Program Coordinator
OPLAN	Operation Plan
ORHA	Office of Reconstruction and Humanitarian Assistance

OS	Operating System
PACOM	U.S. Pacific Command
PALT	Procurement Administrative Lead Time
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POD	Points Of Debarkation
POTS	Plain Old Telephone Services
QDR	Quadrennial Defense Review
RAID	Recent Advances in Intrusion Detection
RFID	Radio Frequency Identification
RMBCS	Rocky Mountain Bank Card System
SANS	System Administration, Audit, Network, Security Institute
SAP	Systems Assessment Program
SAS 70	Statement of Accounting Standard No 70
SAT	Simplified Acquisition Threshold
SECDEF	Secretary of Defense
SOFA	Status of Forces Agreement
SPS	Standard Procurement System
SSC	Small-Scale Contingencies
SSL	Secure Socket Logic
TA	Technical Arrangement
TACO	Theater Allied Contracting Office
TAV	Total Asset Visibility
TDC	Theater Distribution Center
TCN	Tracking Control Number
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TPFDL	Time Phased Force and Deployment List
USG	United States Government

UPS	United Parcel Service
UPS	Uninterrupted Power Supply
USACCE	U. S. Army Contracting Command Europe
USACOM	U. S. Atlantic Command
USAREUR	United States Army, Europe
USAT	Ultra Small Aperture
USCENTCOM	United States Central Command
USEUCOM	U.S. European Command
USMC	United States Marine Corps
USTRANSCOM	United States Transportation Command
VAT	Value Added Tax
VSAT	Very Small Aperture
VTN	VeriSign Trust Network
WCO	World Customs Organization
WWX	World Wide Express

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Ron Tudor
   Naval Postgraduate School
   Monterey, California

4. LTCOL Rodney E. Tudor
   Naval Postgraduate School
   Monterey, California

5. LCDR James T. Chavis
   Seaside, CA

6. LCDR (sel) James Cheatham
   Monterey, CA

7. 2nd LT Vaughn Gonzalez
   Monterey, CA

8. LT Rolando Ibanez
   Monterey, CA

9. LCDR Richard Nalwasky
   Monterey, CA

10. LCDR Martin Rios
    Monterey, CA

11. LCDR (sel) Marco A. Turner
    Monterey, CA