23 March 1992 Final Student Research Report

The Communications Security Material System

Captain J. T. Dillon, USMC; Captain K. M. Fox, USMC; Captain J. J. Jefferson, USA; Captain M. A. Pratt, USMC

Command and Control Systems Course
Communication Officer's School
2085 Morrell Avenue
Quantico, Virginia 22134-5058

Marine Corps University
Marine Corps Combat Development Command
2076 South Street
Quantico, Virginia 22134-5068

Thesis: During Desert Shield and Desert Storm, the differences in policies, procedures, and attitudes concerning the Communications Security Material System (CMS) caused many problems for the Marine Corps and fewer for the Army. The Navy and Marine Corps CMS program must be changed to provide a more usable, flexible, and effective system. This paper provides an overview of CMS programs within the Army and Marine Corps.

USMC; Command and Control; C2; C3; C4I; Joint Command and Control; CMS; COMSEC; MCMO; OTAR; CCEO, DCMS, Education; Crypto; ADP Support; ICP 38

Unclassified Unclassified Unclassified

THE COMMUNICATIONS SECURITY MATERIAL SYSTEM

Submitted to
Major Snyder
at the Communication Officers School
Quantico, Virginia

Captain J. T. Dillon, USMC
Captain K. M. Fox, USMC
Captain J. J. Jefferson, USA
Captain M. A. Pratt, USMC

23 March 1992

THE COMMUNICATIONS SECURITY MATERIAL SYSTEM

Research Paper Topic Outline

Thesis: During Desert Shield and Desert Storm, the differences in policies, procedures, and attitudes concerning the Communications Security Material System (CMS) caused many problems for the Marine Corps and fewer for the Army. The Navy and Marine Corps CMS program must be changed to provide a more usable, flexible, and effective system.

Introduction: Overview of the research paper

I. Background: Genesis of COMSEC

II. U.S. Navy/Marine Corps COMSEC
    - A. CMS administrative structure
    - B. CMS account management
    - C. CMS distribution structure

III. U.S. Army COMSEC
    - A. CMS policies and procedures
    - B. CMS in a deployed environment
    - C. CMS in Southwest Asia
        1. Problems
        2. Solutions

IV. Existing CMS problems
    - A. Inadequate and inflexible rules for tactical forces
    - B. Incompatibility of software in contingency operations

C. Slow and labor intensive distribution of key

D. Insufficient education on policy and procedures

E. Poor attitude toward CMS

F. Proliferation of data communication devices

G. Excessive amount of software held by each account

V. Possible solutions

A. Establishment of the MCMO

1. MCMO organization and responsibilities

2. Pros and cons

B. Use of OTAR

1. Description

2. Pros and cons

C. Establishment of the CCEO

1. Description and responsibilities

2. Pros and cons

D. Establishment of new training and assignment policies

1. Description of new policies

2. Pros and cons

E. Marine Corps contingency key material

1. Description

2. Pros and cons

VI. Recommendations

A. MCMO

B. OTAR

C. CCEO

D. Education policies

E. DCMS assignments

Conclusion: A long term solution to our CMS problems can be implemented by integrating all of the above recommendations.

THE COMMUNICATIONS SECURITY MATERIAL SYSTEM

During Desert Shield and Desert Storm, the differences in policies, procedures, and attitudes concerning the Communications Security Material System (CMS) caused many problems for the Marine Corps and fewer for the Army. The Navy and Marine Corps CMS program must be changed to provide a more usable, flexible, and effective system.

The present Marine Corps system for employing CMS is inadequate for tactical forces and must be changed to accommodate their particular needs. Operating under the Department of the Navy for CMS policies and procedures, the Marine Corps has been tied to an inflexible system designed for Navy shipboard requirements. In Desert Shield and Desert Storm, both Marine Corps and Army tactical units were faced with similar problems in the Communications Security (COMSEC) arena; however, due to their flexibility, Army units developed and employed corrections in theater. This flexibility minimized the impact of such problems as key distribution from CONUS and to tactical units throughout the theater. Marine Corps units were not able to solve problems as quickly; as a result, COMSEC problems were common. Marine Corps problems in the CMS arena include inadequate and inflexible rules for tactical forces, incompatibility of software in contingency operations, slow and labor intensive

distribution of key, insufficient education on policy and procedures, poor attitude toward CMS, proliferation of data communications devices, and the excessive amount of software held by each account. After examining these problems, we will present possible solutions, and recommend changes to Marine Corps' CMS policies and procedures.

Our recent actions in Southwest Asia revealed that our current CMS system is not adequate to support modern Marine Corps operations.

BACKGROUND

To understand our CMS problems, we need to be familiar with the basics of the COMSEC system and the organizations tasked with managing it. There has been some form of COMSEC since the first time a sensitive message was sent from one commander to another. As electronic communications means, such as the telegraph, became more abundant, governments and military organizations began to rely more heavily on these means, and as a result, it became easier for these same institutions to intercept an adversary's transmissions. With the advent of the radio, it was recognized that these new kinds of transmissions were even more susceptible to unauthorized eavesdropping. Thus, our present day COMSEC system has evolved from the continuous actions of individuals over time attempting to protect their communications from unauthorized parties.

U.S. NAVY/MARINE CORPS COMSEC

So what is the system we have today? The system we have in place is quite extensive. However, it cannot meet the needs of a modern force that projects power around the world. To gain an understanding of this system, it is necessary to look at the COMSEC chain of command. At the very top is the National Telecommunications and Information Systems Security Committee (NTISSC), the national authority for promulgation of policy and guidance on COMSEC. The National Security Agency (NSA), in collaboration with other departments and agencies of the government, under NTISSC policy, develops and issues guidance on control of COMSEC material. NSA also produces most of the COMSEC material used to secure our communications. (7:1) Within the Department of the Navy (DON), the Chief of Naval Operations (CNO) is the COMSEC authority. The Director, Communications Security Material System (DCMS), as the primary agent for CNO, is the overseer of the implementation of national and Navy plans, policies, procedures, and directives in the Navy, Marine Corps, Coast Guard, and Military Sealift Command. DCMS is the organization that publishes procedures for managing the CMS system. (14:1) These publications are the CSP 1A and CMS 4L.

To manage the system, CMS accounts were created. These accounts are assigned down to the lowest units that hold and use COMSEC material on a regular basis. In the Marine

Corps, the lowest level is the battalion or squadron. (Most commands above that have one also.) Each account, by policy, must have at least four custodians who are grade E-6 or above, US citizens, and capable of having a security clearance equal to the highest classification of material held. Marine Corps policy prohibits the unit communications officer (COMMO) from being assigned as a custodian or alternate custodian. (5:2) The Navy Education and Training Command (NETC) offers a 1 week CMS Custodian Course that all custodians must attend within 90 days of appointment. This course is offered at Fleet Training Centers and is exported to USMC installations, when required. The course teaches custodians basic account management and CMS book keeping.

Distribution of COMSEC material within DON is for the most part strictly controlled. NSA produces virtually all COMSEC material used by the Navy and Marine Corps. NSA ships the material to DCMS where it is entered into the Navy system. It is then shipped to the COMSEC Material Issuing Office (CMIO). There are two CMIOs: one in Norfolk, Virginia, and one in San Diego, California. The CMIOs issue the material to each CMS account.

As we have shown, the Marine Corps COMSEC system is based on CMS policies and procedures dictated through the Navy chain of command. As a result, we are operating under policies designed for shipboard requirements. In comparison, the Army's COMSEC system is designed and

maintained for tactical ground forces This approach provides an effective system that proved more flexible than the Marine Corps' system in solving problems encountered in Southwest Asia.

U.S. ARMY COMSEC

The Army's COMSEC system is governed by Technical Bulletin (TB) 380-41. The TB 380-41 describes procedures for the safeguarding and accounting of COMSEC material. These technical bulletins define minimum safeguards, standard criteria, and procedures for protecting COMSEC information. The technical bulletins also assign responsibilities and define the procedures for requesting, receiving, stocking, and reporting COMSEC key material and publications. TB-380-41 establishes procedures to implement the Department of the Army (DA) COMSEC policy defined in Army Regulation (AR) 380-41. All commanders, warrant officers, and COMSEC custodians within the active Army, Army National Guard and Army reserve must be familiar with the policies and procedures set forth by AR 380-41 and TB-380-41.

Soldiers identified as COMSEC custodians attend the COMSEC Material Handlers Course at Fort Gordon, Georgia. This course teaches the future COMSEC custodian how to properly maintain, safeguard, account for, distribute, and destroy COMSEC material. The course also teaches them how to load keying material into cryptographic devices The

COMSEC custodian learns what keying material is used with specific items of cryptographic equipment.

Distribution of COMSEC material within the Army is a little different from the Navy. NSA also produces virtually all Army COMSEC material. However, NSA ships this material directly to individual COMSEC accounts -- located down to the corps level -- where it is accounted for and managed. As covered previously, the Navy distribution is more involved. NSA ships Navy COMSEC material to DCMS where it is entered into the system and sent to one of the CMIOs. The CMIOs then send the material to individual COMSEC accounts.

Before any Army unit is deployed on a field exercise or a real world contingency, cryptonets are established. A cryptonet is defined as a cryptographically secure communications net. Establishing cryptonets involves identifying those individuals or operating elements that must intercommunicate in a secure mode. In order to intercommunicate, all cryptonet members must possess identical key and associated communications equipment.

There are three types of key material associated with cryptonets. The first is known as the Current-Operation Key. This key is used for routine day-to-day operations. The second type of key material is known as the Contingency Key. This key is used for operations that occur infrequently. The Army does not use current-operational key

to secure infrequent operations because it results in the costly destruction of unused key. The third type of key material is a Combined Contingency and Current-Operational Key. This key is used when there is a huge difference between the number of cryptonet users participating in day-to-day communications and those involved in real world contingency. Both a current operational cryptonet and contingency cryptonet will be established to meet the two requirements.

When the Army deployed to Southwest Asia, ARCENT decided that the Contingency Key would be used. Each unit deployed with the amount of key necessary to satisfy the immediate operational requirement. Key material normally held by COMSEC accounts or subaccounts is limited to a 4 month supply. This is similar to the amount of software Marine Corps' accounts hold -- 1 month effective and 3 months reserve. As the buildup of Army forces continued, it became increasingly difficult for units to receive new keymat. All keying material was being sent to the deployed unit's account. That account was still located in CONUS.

NSA and Intelligence and Security Command (INSCOM) decided to implement a Theater COMSEC Management Office (TCMO). The TCMO was responsible for distributing and accounting for all cryptographic material in theater. The TCMO's mission was to manage theater COMSEC assets for the Commander-in-Chief (CINC); order, store and distribute codes

and keys; manage theater bulk key sustainment and resupply; validate theater cryptonets; and provide 'one stop' cryptonet shopping. This is similar to what the Navy's CMIO does except the TCMO deploys. The TCMO also provided 12 to 24 hour compromise recovery, warfighting system upgrades, and service for multiservice/joint operations. In short, the TCMO became a deployed version of NSA and INSCOM. NSA sent all keying material to the TCMO. The TCMO would then distribute the keying material to the Major Subordinate Commands (MSC). The MSC's would then issue the COMSEC material to the appropriate account/subaccount holder.

This was an efficient system except for one major problem: many ARMY units deployed to Southwest Asia without the appropriate COMSEC. This problem was further magnified because elements of these units were attached to other units. The receiving units only had enough COMSEC material to fill their systems. The TCMO solved this problem by implementing a facet of cryptonet expansion called Planned Rapid Cryptonet Expansion. Planned Rapid Cryptonet Expansion is used when there is a real possibility that rapid cryptonet expansion will take place and it is known that timely reproduction of the entire key (either by NSA or the stateside controlling authority) is not possible at that time. In this situation extra copies of the key would be distributed by the TCMO (who would be the controlling authority). The TCMO would request a change in copy count for numerous keying material and submit a message to

INSCOM. Even though this material was sent out continuously through Operation Desert Shield/Storm, NSA and INSCOM could not meet the demand. The solution to this problem was to have like cryptographic systems share keying material until each system could be provided its own keying material.

The TCMO proved to be a success in Southwest Asia. Its timely and responsive service filled a void in the current COMSEC system in a joint environment. Also, Over-the-Air-Rekeying (OTAR) was used to transmit the key to selected systems electronically. This helped to reduce the amount of 'hard copy' keying material as well as simplifying the key changing process. Currently, the Army is beginning to implement OTAR over more systems, with the ultimate goal of creating an almost paperless COMSEC environment. OTAR will be covered in detail later, as we present proposed solutions to our CMS problems.

Although no present COMSEC system is flawless, the Army system, which incorporated a TCMO, can limit the size and scope of potential COMSEC problems for the ground forces in a joint theater of operations. The TCMO provides a theater level organization that is responsive to user needs, unlike the Navy's CMIO which is administrative in nature and does not deploy.

EXISTING CMS PROBLEMS

Under the current Navy/Marine Corps' system, some major problems exist. We will cover those problems in depth.

The Marine Corps has been tied to an inflexible system designed for Navy shipboard requirements. There are many examples of this, however, TPI requirements are the most obvious. TPI is the security measure implemented by the DON for all CMS accounts to prevent single-person access to classified CMS keying material and cryptographic maintenance manuals. TPI was implemented by DON after the Walker-Whitworth spy case surfaced. Previous to this, CMS rules allowed single-person access to COMSEC material. This was how Walker was able to steal COMSEC material and sell it to the USSR. To prevent this from happening again, TPI was established. TPI measures must be used by all Marine Corps CMS accounts beginning with the initial pick-up or delivery of material through the final disposition or destruction of the material. TPI is required not only at the CMS account level but also at the user level. Some of the tasks that require TPI are listed below:

(1) Material must be receipted for and destroyed by two people.

(2) Material must be stored under double lock protection, and when not stored, it must be under constant surveillance of two appropriately cleared individuals.

(3) COMSEC equipment that requires the physical

insertion and/or removal of the actual keying material must be filled and operated under TPI.

(4) Mechanical fill devices which allow the viewing of key settings must be provided TPI at all times when filled. While the logistics requirements of TPI may be easily satisfied on board a ship, logistics requirements for qualified personnel, safes, and lockups are more difficult for ground forces.

The above examples indicate how TPI can be a costly procedure in both personnel and equipment, especially in an operational environment. DCMS has granted waivers for tactical units; therefore, TPI now impacts only garrison units. However, TPI is an example of how Navy policy impacts Marine units.

Compatibility of software (key material) in contingency operations became an issue as a result of lessons learned from the Grenada operation. Although these problems were solved, the large scale deployment of Marine units in operations Desert Shield and Desert Storm uncovered others.

The Intertheater COMSEC Package (ICP) software system was developed by the Joint Chiefs of Staff to facilitate secure communications for joint forces. The value of ICP was truly recognized as a result of joint operations in Grenada. At the time, the lack of a common cryptographic keying material system severely hampered secure communications between service components. The component

commanders could maintain secure internal C3, but they could not maintain secure external C3 with adjacent components and higher headquarters. (8)

A serious weakness had been discovered in the conduct of joint operations. Forces deployed on short notice had not planned for external secure communications systems. If they had prepared ahead of time, they would have been forced to specify one services' cryptographic software short title for use by all of the Joint Task Force (JTF) components on any particular circuit. The CMS system was not prepared to provide such quantities of individual short titles on short notice. (17) Additionally, no common CMS short titles were held by all of the services for such joint or combined operations.

The ICP addressed this shortfall. A common package of CMS software was distributed which enabled the JTF commander and his component commanders to maintain effective, secure communication links on short notice. During operations in Southwest Asia, ICP was also used successfully by component commands to communicate to all aircraft in theater. (15)

During operation Desert Shield, the initial Marine forces deployed to Saudi Arabia were from I Marine Expeditionary Force (MEF). On the MEF level and above, ICP was used to initiate secure voice and data communications between the different service components. When II MEF forces were introduced within the I MEF area of

responsibility (AOR), CMS problems became readily apparent. The two MEF's maintained different short titles of CMS material for similar communication circuits, and too few I MEF CMS short titles existed within the system to allow for common software usage by the forces combined under I MEF.

The solution seemed simple: the forces under I MEF would utilize ICP CMS material to ensure interoperability of their communication circuits. This worked well until ICP software losses began to occur. These compromises of ICP material meant that all forces within the theater using the ICP had to change editions of CMS software, as the compromised editions were replaced by emergency releases.

This problem required immediate resolution because the CMS system does not maintain enough ICP material to supply every MSC. The ICP was only meant to be used at the component level. After several such compromises, the Marine Corps was forced to revert to their own CMS short title software for internal communication circuits. The ICP was rendered safe from excessive danger of compromise, but C3 interoperability between the I MEF and II MEF forces under I MEF was hampered because there wasn't enough common CMS software within the MEF. (12)

Recent world events have underscored the absolute requirement for interoperability among the forces, agencies, and nationalities operating in concert on the modern battlefield. During operations Desert Shield and Desert

Storm, CMS distribution to account holders was highly ineffective.

Distribution of CMS material was slow and labor intensive. This was due to the vast distances covered by maneuvering units and the large volume of paper CMS material required at the account level. Distribution of materials from the MSC parent account to the unit account required CMS custodians to drive many miles across open desert to receipt for CMS shipments from the parent account. This was slow, at best, during defensive operations. With the shift to offensive operations, this method of distribution could not keep pace with the tempo of maneuvering units. During sustained operations, secure and effective resupply of unit accounts was virtually impossible. (3)

Inadequate education of Marine commanders, CMS users, and custodians concerning CMS policies and procedures is another area that must be considered.

After-action reports and interviews with Marine commanders reveal that our leaders appreciate the need to maintain reliable secure communications, both in combat and in training. However, few understand how the system is designed, how it is used to support secure C3 among different units on the battlefield, what the CMS custodian must do to maintain the proper levels of CMS hardware and software within the unit account, and how this impacts their command both internally and externally. (10) NAVMC 2900,

"The Commanding Officer's Handbook for CMS Account Management," explains how to manage CMS accounts, but no standardized training is available to commanders. The handbook alone cannot fully prepare them to effectively use and maintain this capability.

CMS user training is conducted at the unit level. As a result, many units have highly proficient CMS users, but many more units do not have proper training in CMS use. Our MOS schools conduct little, if any, CMS user training for enlisted personnel or officers. Furthermore, the training that is provided is not coordinated throughout the service. (10) The quality of training at the unit level reflects experience of the individuals in the unit. Lack of standardized user training weakens an already complex, burdensome, and unresponsive system.

The CMS custodians, though formally trained for their duties at the Navy's CMS Custodian Course, usually are not familiar with their unit's communication circuits or equipment that requires CMS material. They rely upon the COMMO for oversight of CMS holdings. Unfortunately, as a result of being prohibited from custodial duties, many COMMOs do not exercise staff cognizance over this area resulting in a poorly planned, coordinated, and utilized CMS account. (4)

Marine Corps Order (MCO) 2201.1 prohibits communication officers from assignment to duty as unit CMS custodians.

Typically, CMS duties are assigned to personnel from the S-1 or S-3 sections. This was done to enhance system security and avoid the possible conflict of interest between the users of CMS material and its accountability chain. The net effect is to alienate CMS users, primarily the COMMOs, from one of the most important aspects of the system, its day-to-day management and oversight. We seem to be breeding an attitude among our COMMOs that CMS is a bad thing to take an interest in, and that it's not their responsibility.

Existing CMS problems are compounded by the proliferation of data communication devices. The Marine Corps deployed over 30 local area networks in Southwest Asia, more than any other service. This demand was driven by users who had experienced the value of networks in garrison. The local area networks were the engines that drove electronic sitreps, air tasking orders, naval messages, class I data, class II data, logistics reports, weather, and mail. One statistic coming out of Desert Storm was that in the 36 hours before, and until noon the day after G-Day, approximately 1.3 million messages were passed, supporting everything from command and control to Combat Service Support (CSS) functions.

The success of the local area networks in Southwest Asia will surely spark more requirements. The Marine Corps now possesses approximately 25,000 personal computers that can potentially be linked together in local area networks

like those in Desert Storm. This proliferation of data communication devices is a concern, because all internetwork connections must be covered by COMSEC devices. To keep these networks running, compatible key material and timely distribution of that material is essential.

One major administrative problem in our CMS system is the excessive amount of CMS material held in any account. At present all keying materials, codes, and authenticators are on paper. Accounts have to maintain enough copies of each of these in order to support the needs of all its users plus the required 90 days of reserve material, operational and exercise material, and contingency material. As can be seen, every custodian has a lot of paper to account for. The more material held by an account, the greater chance there is for a security violation. This is due to the extensive administrative requirements of accounting for COMSEC material. The problem is greatly compounded if an inexperienced or unqualified individual is assigned as the custodian.

PROPOSED SOLUTIONS

Now that we've looked at the problems plaguing our present CMS system, let's look at the possible solutions. Some solutions are already in place, and some are planned. It's important to understand that these solutions are not designed to correct one specific problem; the implementation of each solution will affect many problem areas.

An idea being tested by I MEF at the present time seems to have a lot of merit. This idea is to establish a MEF COMSEC Management Office (MCMO), based mainly on the Army's TCMO concept. The MCMO will improve CMS coordination for deployed forces, decrease the amount of CMS held by accounts on a daily basis, and ensure proper education for CMS personnel.

The MCMO, an organization or section resident within the MEF headquarters, would hold keying material for contingencies so that subordinate units would not have to maintain it. This arrangement will effectively reduce the copy count and management burdens associated with contingency keymat (i.e. ICP material) for subordinate units. Units can be prevalidated -- that is, authorized by a controlling authority to hold certain keying materials, to receive material (again material such as ICP) without having to actually hold it. The MCMO would coordinate and manage contingency keymat so that when a unit needed it, they would draw it from the MCMO. This concept could also be applied to actual operational keymat as well. Subordinate units would hold exercise key on a day-to-day basis, and the MCMO would hold operational key to issue on an as-needed basis.

The MCMO would be the sole point of contact for the MEF in CMS matters both internal and external. The MCMO would be the main point of contact to external organizations such

as distribution agencies (i.e. CCMSEC Material Issuing Office (CMIO)), other services, controlling authorities, etc. The MCMO would also be the main point of effort within the MEF for training and education of CMS.

If the MEF is to deploy, the MCMO would deploy with it and set up in theater and provide the critical coordination, in-theater distribution, and storage functions that were lacking in Southwest Asia. The MCMO would also interface with the Army's TCMO in a joint environment.

This MCMO concept can reduce the amount of CMS software maintained at the subordinate level on a day-to-day garrison basis. As a result, much of the administrative workload would be eliminated at the lower levels. This is particularly desirable where the CMS custodian billet is a collateral duty. It will also facilitate better coordination with other services, controlling authorities, and distribution agencies because these outside organizations will have one command to coordinate with. (16) (19)

Implementation of the MCMO will push most of the work required to manage CMS to the MEF level, but the MEF will have individuals dedicated to dealing with CMS as a full time job.

Some problems with this concept concern manning the MCMO. Where will the staff come from and what rank should

they be? How will operational and contingency key be provided to units? If subordinate units maintain all the key material they could possibly need plus the required 3 months reserve on board (ROB), they can virtually pick up and go without having to worry about drawing CMS material from the MCMO and still receive their required material on a regular basis from the CMIOs.

An initiative is now being implemented to reduce the amount of paper CMS material held and handled at all levels of command. The Navy, through the direction of Vice Admiral Tuttle, CNO Op 094, is moving to a paperless CMS environment. As early as the latter half of 1990 and especially during Desert Shield and Desert Storm, the Navy was electronically sending key material over the fleet broadcast to its deployed battlegroups with much success. After-action reports from these deployed battlegroups greatly acclaimed its use. The Navy has established sound procedures for this technique and actively uses them.

This concept is known as electronic distribution of key or OTAR. Presently it is used tactically, but plans are in the works to abolish most of the paper key and replace it in garrison and in the field with not only the electronic distribution of key but also by electronic management of CMS with personal computers and STU-IIIs. The OTAR concept will replace today's safes, paper keying material, and logbooks with more manageable electronic equipment. This equipment

includes electronic storage devices (such as the KYK-13, KYX-15), a personal computer, and a STU-III. Electronic COMSEC management will greatly reduce administrative burdens.

The security aspects of electronic management are also appealing. When a MEF/Marine Air Ground Task Force (MAGTF) deploys, it can receive all required keys over-the-air, so that it can deploy anywhere and receive any keys necessary within a matter of hours. Additionally, any key material needed for internal requirements can be generated by the sending agency (NCTAMS, MCMO) so that the key material will be completely unique to the MEF/MAGTF. Furthermore, in the event of a compromise, only the MEF/MAGTF is affected, and it can immediately generate a new key.

NSA is working to implement this idea for all the services, so that by the end of the century all keying material, distribution of key, and management of the system will be electronic.

Presently the Marine Corps is still using paper, even though the Navy has proven procedures in place to electronically distribute key material in a tactical environment, and despite the fact that many reports have indicated the severe problems of not having the appropriate version or amount of key material. These problems are easily solved by using over-the-air distribution. The Marine Corps can receive these keys in the electronic form.

As a matter of fact, within the Atlantic Fleet, the Navy has borrowed these electronic storage and key generating devices (KYK-13 and KYX-15) from the Marine Corps to satisfy the needs of its commands. The Marine Corps has practiced electronic distribution of key for years in VINSON (KY-57) operations or Saville Advanced Remote Keying (SARK). Over-the-air-distribution (OTAD) of key uses the same principles as SARK but on a larger scale. The Navy is rapidly moving to a paperless CMS environment, leaving the Marine Corps behind.

OTAD transfers all the key material a unit needs electronically over one secure circuit for use on other cryptographic devices. These cryptographic devices are systems such as the KY-57, KY-65, KG-84, the embedded COMSEC device for SINCGARS, and the new Advanced Narrowband Digital Voice Terminal (ANDVT). We already employ or will employ these systems on virtually all of our circuits now.

Headquarters Marine Corps (HQMC) has proposed an initiative to aid in the management of CMS at the major command level by appointing of a Command COMSEC Employment Officer (CCEO). Although HQMC recognizes that the CCEO responsibilities have been associated with the G-6/CEO section, they state that CMS responsibilities have often been delegated to the CMS custodian, who in many cases does not have the background, experience, or training to perform these duties. Some of the responsibilities that will be

associated with the CCEO are:

1) Keeping the commander abreast of all operational COMSEC matters relating to the command and its subordinate units.

2) Monitoring the command's COMSEC requirements: coordinating with staff sections, internal and external to the command, to ensure that the command's COMSEC plans are integrated into the command's Operations Security (OPSEC) and C3CM planning.

3) Advising subordinate commands of COMSEC keying material requirements for operations and requirements.

4) Advising the CMS custodian of changes in requirements.

5) Acting as the command's item manager for cryptographic hardware by coordinating with the supply officer and CMS custodian to ensure that cryptographic hardware and ancillary devices are on hand.

6) Recommending reallocation of COMSEC assets among subordinate commands to ensure maximum use of available assets.

7) Performing controlling authority duties for keying material for which the command is responsible.

8) Conducting inspections and surveys of subordinate commands COMSEC operational readiness. (20)

HQMC contends that assigning a CCEO in writing, will give each major command a designated focal point for these responsibilities. These functions are the responsibility of

the G-6/CEO and should never be delegated to an individual not directly responsible to the G-6. Proper CMS planning is crucial to the success of any operation.

It is not effective or efficient to assign these responsibilities to someone who must work hand in hand with the CMS custodian. The CMS custodian, in our present system, is usually working for a completely different section head, normally the G-1. Additionally, he has absolutely no experience in the employment of such material. The question therefore is simplicity itself. Why not make the CMS custodian and the CCEO responsible -- administratively and operationally -- to the G-6/CEO for all matters dealing with CMS and COMSEC? The Marine Corps is the only service that does not follow this system. The Navy, Coast Guard, Army, and Air Force all have the CMS custodian and CCEO working for the G-6/CEO.

Defense of our present system raises legitimate concerns. One concern is that the CMS custodian, a full time job, will then have to come from the present G-6 staff. This may be so but, alternate custodians can come from anywhere providing they meet the basic requirements. So theoretically, only the CMS custodian need be from the G-6 shop. Other custodians can be spread evenly throughout the rest of the staff. It only makes good sense to have the CMS custodian from the G-6. He will not only be familiar with the cryptographic material but will know how it is

employed.

HQMC, to reduce the account management problems previously discussed, has proposed more stringent training and assignment requirements. In a nutshell these are:

1) Prohibit assignment of individuals as the CMS custodian or primary alternate until formal training has been completed (1 week course offered by NETC Newport RI). Since each account has four custodians, when the custodian or primary alternate is relieved, simply move the second or third custodian up to take over until training is completed for the incoming custodian.

2) Establish a minimum assignment for the custodian of at least 18 months for a three year tour and nine months for a one-year tour. This tour length will allow the custodian to become familiar with CMS account management. (20)

These sound management proposals can only improve CMS accounts. One more assignment requirement should be added. The responsible assignment of custodians, instead of assigning the billet to the lieutenant or gunny who just can't seem to hold on to a job. Proper COMSEC management is vitally important to everyone, and irresponsible assignment of 'expendable' individuals to be CMS custodians must stop.

ICP material, as discussed earlier, was developed by JCS to improve the interoperability of forces and CINCs during contingency operations. This material has proved to work successfully. After-action reports have highlighted

the need for a Marine-Corps-specific contingency key to be used by Marine forces from different MEFs pulled together. There is a Marine Corps contingency key; however, it was not widely publicized and had a relatively small copy count. (17) Our operations in Southwest Asia revealed the need for more of this Marine Corps contingency keymat with distribution validated to all units down to the battalion/squadron level.

RECOMMENDATIONS

The present CMS system and the way the Marine Corps uses it must change. Short term solutions are being implemented, but we need a comprehensive system to take us into the next century, not a bunch of good ideas being implemented separately. Here's what that system should be.

First and foremost we need full implementation of the MCMO concept. This organization shows a lot of merit. Not only must the MCMO be institutionalized in our MEF headquarters, but it must be supported by the commander and staff. A table of organization (T/O) must be established to adequately meet the requirements, and responsible individuals who have the appropriate experience and training must be assigned to it. Conversations with the MAGTF Integration Team indicate the new proposed MEF structure will have three individuals assigned to a CMS section within the MEF G-6. This could form the nucleus of the MCMO, CMS is a very critical component of successful command and

control and must be treated as such. Furthermore, a MCMO, on a smaller scale, must be sent with a Marine Expeditionary Brigade (MEB) size organization if and when it deploys. This could be just an augmentation from the main MCMO to round out the MEB's G-6 staff.

As electronic distribution of key becomes the standard, the Marine Corps must utilize this procedure in all operations. The MCMO would be the perfect organization to coordinate electronic distribution now and in the future.

To effectively carry out its mission, the MCMO organization must fall under the cognizance of the G-6. The MCMO must also have administrative and operational control of the CMS custodian so that all CMS matters can be properly coordinated. The Command COMSEC Employment Officer can also be integrated into the MCMO. On lower levels of command one individual should be responsible for COMSEC employment and CMS management. If the Command COMSEC Employment Officer and CMS custodian are the same person or if the CMS custodian works both administratively and operationally for the CCEO, then so be it. Separation of these two individuals is unnecessary and causes easily avoidable problems.

Proper education of CMS personnel, users, and command personnel is essential. Through education we can break down misconceptions of the CMS system, so these individuals can understand what COMSEC can do for them. COMSEC is nothing

to be afraid of, in fact when employed properly, it is a combat multiplier. Here again the MCMO can earn money. The MCMO, if staffed properly, can be the focal point of effective CMS training within the MEF. Through the use of mobile training teams, assist visits, and inspections we can really begin to tighten up our CMS programs. Coupled with training is the appropriate assignment policy discussed previously. Again this only makes good managerial sense. It adds stability to a critical job.

The other change that will cement all this together is external to the Marine Corps. It lies with the Navy where policy is developed and implemented, DCMS (Director, COMSEC Material System). The Marine Corps presently only has one Marine Gunnery Sergeant at DCMS and he works in the COMSEC hardware section of DCMS. We need at least two more individuals of appropriate rank, master sergeant to captain, to work in the policy section and the operations section. These individuals, who understand the unique aspects of Marine Corps operations, can help develop policy in conjunction with the Navy. The Navy can benefit from this arrangement as well. Their substantial ground forces operate like the Marine Corps (SEALS, Beachmasters, EOD units, Amphibious CBs, Cargo Handling units). Additionally, as the Secretary of the Navy has directed that certain parts of CNO and HQMC integrate, this area is a good candidate for that integration.

CONCLUSION

We believe, the MCMO concept should be the core of the Marine Corps' CMS program. By localizing the management within each MEF, we can ensure an effective utilization of the system. And within subordinate units of the MEF, the employment and management of COMSEC should rest with one individual, the Communications Officer. Also establishing Marine Corps personnel with the Navy policy makers at DCMS will help tie the whole CMS program into an effective, user-friendly, and responsive system. Only by implementing these basic ideas will the Marine Corps have an effective and responsive COMSEC program at its disposal.

BIBLIOGRAPHY

1. Army Regulation 380-41 (AR 380-41). U.S. Army. Feb 89

2. ADP Support for the Marine Corps. Computer Sciences School, Student Handout, DFO 1000, Dec 91: 1.

3. CMS. MCLLS Long Report, Number 91535-97213 (02252). Submitted by 9thCommBn. 12 May 91

4. Cross, R.N., Chief Warrant Officer-2, USMC. Personal interview. 2d FSSG. 24 Jan 92

5. Commanding Officer's (CO's) Handbook for Communications Security Material (CMS) Account Management. NAVMC 2900, CCT-636, May 89: 4-5.

6. Communications Security Material System (CMS) 4L Manual (CMS 4L). DCMS

7. Cryptographic Security Policy 1A (CSP 1A). COMNAVSECGRU.

8. Dillon, J.T., Captain, USMC. Personal interview, CCSC MCCDC. 3 Feb 92.

9. Fraison, R., CW4, USA. Personal interview, XVIII Airborne Corps. 21 Dec 92

10. Hull, J.E., Lieutenant Colonel, USMC. Personal interview, 2ND FSSG. 24 Jan 92.

11. Ibanez, G., Captain, USMC. Personal interview, FMFLANT. Various Dates.

12. Inter-Theater Communications Security Packages (ICP). MCLLS Long Report, Number 02141-57815 (02281). Submitted by I MEF. 23 Mar 91.

13. Jefferson, J.J., Captain, USMC. Personal interview, CCSC MCCDC. 3 Feb 92.

14. Jensen, L.A. A Description of the Functions of the Office of the Director, COMSEC Materials Systems. Navy Research Laboratory Memorandum Report 6631. 10 May 1990

15. Licari, J., Captain, USMC. Personal interview, MAWTS-1. 6 Dec 92.

16. Malone, Lieutenant, USN. Personal interview, I MEF. 24 Jan 92.

17. Nicosia, Dee. Personal interview, HQMC. 28 Jan 92.

18. Pratt, M.A., Captain, USMC. Personal interview, CCSC MCCDC. 3 Feb 92.

19. Proposal to Establish Marine Corps MEF COMSEC Management Officer (MCMO). CMC Washington DC 191900Z Jun 91

20. Proposed Changes to COMSEC Account Management. CMC Washington DC 081900Z Jan 92

21. Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT) Procedures Manual Promulgation. CNO ltr 2250 Ser 941J/1U556106 dtd 07 Feb 1991.

22. Technical Bulletin 380-41 (TB 380-41). U.S. Army. Volumes 1 thru 5. Sep 90

THE COMMUNICATIONS SECURITY MATERIAL SYSTEM

Submitted to
Major Snyder
at the Communication Officers School
Quantico, Virginia

Captain J. T. Dillon, USMC
Captain K. M. Fox, USMC
Captain J. J. Jefferson, USA
Captain M. A. Pratt, USMC

23 March 1992

THE COMMUNICATIONS SECURITY MATERIAL SYSTEM

Research Paper Topic Outline

Thesis: During Desert Shield and Desert Storm, the differences in policies, procedures, and attitudes concerning the Communications Security Material System (CMS) caused many problems for the Marine Corps and fewer for the Army. The Navy and Marine Corps CMS program must be changed to provide a more usable, flexible, and effective system.

Introduction: Overview of the research paper

I. Background: Genesis of COMSEC

II. U.S. Navy/Marine Corps COMSEC
    - A. CMS administrative structure
    - B. CMS account management
    - C. CMS distribution structure

III. U.S. Army COMSEC
    - A. CMS policies and procedures
    - B. CMS in a deployed environment
    - C. CMS in Southwest Asia
        1. Problems
        2. Solutions

IV. Existing CMS problems
    - A. Inadequate and inflexible rules for tactical forces
    - B. Incompatibility of software in contingency operations

C. Slow and labor intensive distribution of key

D. Insufficient education on policy and procedures

E. Poor attitude toward CMS

F. Proliferation of data communication devices

G. Excessive amount of software held by each account

V. Possible solutions

A. Establishment of the MCMO

1. MCMO organization and responsibilities

2. Pros and cons

B. Use of OTAR

1. Description

2. Pros and cons

C. Establishment of the CCEO

1. Description and responsibilities

2. Pros and cons

D. Establishment of new training and assignment policies

1. Description of new policies

2. Pros and cons

E. Marine Corps contingency key material

1. Description

2. Pros and cons

VI. Recommendations

A. MCMO

B. OTAR

C. CCEO

D. Education policies

E. DCMS assignments

Conclusion: A long term solution to our CMS problems can be implemented by integrating all of the above recommendations.

THE COMMUNICATIONS SECURITY MATERIAL SYSTEM

During Desert Shield and Desert Storm, the differences in policies, procedures, and attitudes concerning the Communications Security Material System (CMS) caused many problems for the Marine Corps and fewer for the Army. The Navy and Marine Corps CMS program must be changed to provide a more usable, flexible, and effective system.

The present Marine Corps system for employing CMS is inadequate for tactical forces and must be changed to accommodate their particular needs. Operating under the Department of the Navy for CMS policies and procedures, the Marine Corps has been tied to an inflexible system designed for Navy shipboard requirements. In Desert Shield and Desert Storm, both Marine Corps and Army tactical units were faced with similar problems in the Communications Security (COMSEC) arena; however, due to their flexibility, Army units developed and employed corrections in theater. This flexibility minimized the impact of such problems as key distribution from CONUS and to tactical units throughout the theater. Marine Corps units were not able to solve problems as quickly; as a result, COMSEC problems were common. Marine Corps problems in the CMS arena include inadequate and inflexible rules for tactical forces, incompatibility of software in contingency operations, slow and labor intensive

distribution of key, insufficient education on policy and procedures, poor attitude toward CMS, proliferation of data communications devices, and the excessive amount of software held by each account. After examining these problems, we will present possible solutions, and recommend changes to Marine Corps' CMS policies and procedures.

Our recent actions in Southwest Asia revealed that our current CMS system is not adequate to support modern Marine Corps operations.

BACKGROUND

To understand our CMS problems, we need to be familiar with the basics of the COMSEC system and the organizations tasked with managing it. There has been some form of COMSEC since the first time a sensitive message was sent from one commander to another. As electronic communications means, such as the telegraph, became more abundant, governments and military organizations began to rely more heavily on these means, and as a result, it became easier for these same institutions to intercept an adversary's transmissions. With the advent of the radio, it was recognized that these new kinds of transmissions were even more susceptible to unauthorized eavesdropping. Thus, our present day COMSEC system has evolved from the continuous actions of individuals over time attempting to protect their communications from unauthorized parties.

U.S. NAVY/MARINE CORPS COMSEC

So what is the system we have today? The system we have in place is quite extensive. However, it cannot meet the needs of a modern force that projects power around the world. To gain an understanding of this system, it is necessary to look at the COMSEC chain of command. At the very top is the National Telecommunications and Information Systems Security Committee (NTISSC), the national authority for promulgation of policy and guidance on COMSEC. The National Security Agency (NSA), in collaboration with other departments and agencies of the government, under NTISSC policy, develops and issues guidance on control of COMSEC material. NSA also produces most of the COMSEC material used to secure our communications. (7:1) Within the Department of the Navy (DON), the Chief of Naval Operations (CNO) is the COMSEC authority. The Director, Communications Security Material System (DCMS), as the primary agent for CNO, is the overseer of the implementation of national and Navy plans, policies, procedures, and directives in the Navy, Marine Corps, Coast Guard, and Military Sealift Command. DCMS is the organization that publishes procedures for managing the CMS system. (14:1) These publications are the CSP 1A and CMS 4L.

To manage the system, CMS accounts were created. These accounts are assigned down to the lowest units that hold and use COMSEC material on a regular basis. In the Marine

Corps, the lowest level is the battalion or squadron. (Most commands above that have one also.) Each account, by policy, must have at least four custodians who are grade E-6 or above, US citizens, and capable of having a security clearance equal to the highest classification of material held. Marine Corps policy prohibits the unit communications officer (COMMO) from being assigned as a custodian or alternate custodian. (5:2) The Navy Education and Training Command (NETC) offers a 1 week CMS Custodian Course that all custodians must attend within 90 days of appointment. This course is offered at Fleet Training Centers and is exported to USMC installations, when required. The course teaches custodians basic account management and CMS book keeping.

Distribution of COMSEC material within DON is for the most part strictly controlled. NSA produces virtually all COMSEC material used by the Navy and Marine Corps. NSA ships the material to DCMS where it is entered into the Navy system. It is then shipped to the COMSEC Material Issuing Office (CMIO). There are two CMIOs: one in Norfolk, Virginia, and one in San Diego, California. The CMIOs issue the material to each CMS account.

As we have shown, the Marine Corps COMSEC system is based on CMS policies and procedures dictated through the Navy chain of command. As a result, we are operating under policies designed for shipboard requirements. In comparison, the Army's COMSEC system is designed and

maintained for tactical ground forces. This approach provides an effective system that proved more flexible than the Marine Corps' system in solving problems encountered in Southwest Asia.

U.S. ARMY COMSEC

The Army's COMSEC system is governed by Technical Bulletin (TB) 380-41. The TB 380-41 describes procedures for the safeguarding and accounting of COMSEC material. These technical bulletins define minimum safeguards, standard criteria, and procedures for protecting COMSEC information. The technical bulletins also assign responsibilities and define the procedures for requesting, receiving, stocking, and reporting COMSEC key material and publications. TB-380-41 establishes procedures to implement the Department of the Army (DA) COMSEC policy defined in Army Regulation (AR) 380-41. All commanders, warrant officers, and COMSEC custodians within the active Army, Army National Guard and Army reserve must be familiar with the policies and procedures set forth by AR 380-41 and TB-380-41.

Soldiers identified as COMSEC custodians attend the COMSEC Material Handlers Course at Fort Gordon, Georgia. This course teaches the future COMSEC custodian how to properly maintain, safeguard, account for, distribute, and destroy COMSEC material. The course also teaches them how to load keying material into cryptographic devices. The

COMSEC custodian learns what keying material is used with specific items of cryptographic equipment.

Distribution of COMSEC material within the Army is a little different from the Navy. NSA also produces virtually all Army COMSEC material. However, NSA ships this material directly to individual COMSEC accounts -- located down to the corps level -- where it is accounted for and managed. As covered previously, the Navy distribution is more involved. NSA ships Navy COMSEC material to DCMS where it is entered into the system and sent to one of the CMIOs. The CMIOs then send the material to individual COMSEC accounts.

Before any Army unit is deployed on a field exercise or a real world contingency, cryptonets are established. A cryptonet is defined as a cryptographically secure communications net. Establishing cryptonets involves identifying those individuals or operating elements that must intercommunicate in a secure mode. In order to intercommunicate, all cryptonet members must possess identical key and associated communications equipment.

There are three types of key material associated with cryptonets. The first is known as the Current-Operation Key. This key is used for routine day-to-day operations. The second type of key material is known as the Contingency Key. This key is used for operations that occur infrequently. The Army does not use current-operational key

to secure infrequent operations because it results in the costly destruction of unused key. The third type of key material is a Combined Contingency and Current-Operational Key. This key is used when there is a huge difference between the number of cryptonet users participating in day-to-day communications and those involved in real world contingency. Both a current operational cryptonet and contingency cryptonet will be established to meet the two requirements.

When the Army deployed to Southwest Asia, ARCENT decided that the Contingency Key would be used. Each unit deployed with the amount of key necessary to satisfy the immediate operational requirement. Key material normally held by COMSEC accounts or subaccounts is limited to a 4 month supply. This is similar to the amount of software Marine Corps' accounts hold -- 1 month effective and 3 months reserve. As the buildup of Army forces continued, it became increasingly difficult for units to receive new keymat. All keying material was being sent to the deployed unit's account. That account was still located in CONUS.

NSA and Intelligence and Security Command (INSCOM) decided to implement a Theater COMSEC Management Office (TCMO). The TCMO was responsible for distributing and accounting for all cryptographic material in theater. The TCMO's mission was to manage theater COMSEC assets for the Commander-in-Chief (CINC); order, store and distribute codes

and keys; manage theater bulk key sustainment and resupply; validate theater cryptonets; and provide 'one stop' cryptonet shopping. This is similar to what the Navy's CMIO does except the TCMO deploys. The TCMO also provided 12 to 24 hour compromise recovery, warfighting system upgrades, and service for multiservice/joint operations. In short, the TCMO became a deployed version of NSA and INSCOM. NSA sent all keying material to the TCMO. The TCMO would then distribute the keying material to the Major Subordinate Commands (MSC). The MSC's would then issue the COMSEC material to the appropriate account/subaccount holder.

This was an efficient system except for one major problem: many ARMY units deployed to Southwest Asia without the appropriate COMSEC. This problem was further magnified because elements of these units were attached to other units. The receiving units only had enough COMSEC material to fill their systems. The TCMO solved this problem by implementing a facet of cryptonet expansion called Planned Rapid Cryptonet Expansion. Planned Rapid Cryptonet Expansion is used when there is a real possibility that rapid cryptonet expansion will take place and it is known that timely reproduction of the entire key (either by NSA or the stateside controlling authority) is not possible at that time. In this situation extra copies of the key would be distributed by the TCMO (who would be the controlling authority). The TCMO would request a change in copy count for numerous keying material and submit a message to

INSCOM. Even though this material was sent out continuously through Operation Desert Shield/Storm, NSA and INSCOM could not meet the demand. The solution to this problem was to have like cryptographic systems share keying material until each system could be provided its own keying material.

The TCMO proved to be a success in Southwest Asia. Its timely and responsive service filled a void in the current COMSEC system in a joint environment. Also, Over-the-Air-Rekeying (OTAR) was used to transmit the key to selected systems electronically. This helped to reduce the amount of 'hard copy' keying material as well as simplifying the key changing process. Currently, the Army is beginning to implement OTAR over more systems, with the ultimate goal of creating an almost paperless COMSEC environment. OTAR will be covered in detail later, as we present proposed solutions to our CMS problems.

Although no present COMSEC system is flawless, the Army system, which incorporated a TCMO, can limit the size and scope of potential COMSEC problems for the ground forces in a joint theater of operations. The TCMO provides a theater level organization that is responsive to user needs, unlike the Navy's CMIO which is administrative in nature and does not deploy.

EXISTING CMS PROBLEMS

Under the current Navy/Marine Corps' system, some major problems exist. We will cover those problems in depth.

The Marine Corps has been tied to an inflexible system designed for Navy shipboard requirements. There are many examples of this, however, TPI requirements are the most obvious. TPI is the security measure implemented by the DON for all CMS accounts to prevent single-person access to classified CMS keying material and cryptographic maintenance manuals. TPI was implemented by DON after the Walker-Whitworth spy case surfaced. Previous to this, CMS rules allowed single-person access to COMSEC material. This was how Walker was able to steal COMSEC material and sell it to the USSR. To prevent this from happening again, TPI was established. TPI measures must be used by all Marine Corps CMS accounts beginning with the initial pick-up or delivery of material through the final disposition or destruction of the material. TPI is required not only at the CMS account level but also at the user level. Some of the tasks that require TPI are listed below:

(1) Material must be receipted for and destroyed by two people.

(2) Material must be stored under double lock protection, and when not stored, it must be under constant surveillance of two appropriately cleared individuals.

(3) COMSEC equipment that requires the physical

insertion and/or removal of the actual keying material must be filled and operated under TPI.

(4) Mechanical fill devices which allow the viewing of key settings must be provided TPI at all times when filled. While the logistics requirements of TPI may be easily satisfied on board a ship, logistics requirements for qualified personnel, safes, and lockups are more difficult for ground forces.

The above examples indicate how TPI can be a costly procedure in both personnel and equipment, especially in an operational environment. DCMS has granted waivers for tactical units; therefore, TPI now impacts only garrison units. However, TPI is an example of how Navy policy impacts Marine units.

Compatibility of software (key material) in contingency operations became an issue as a result of lessons learned from the Grenada operation. Although these problems were solved, the large scale deployment of Marine units in operations Desert Shield and Desert Storm uncovered others.

The Intertheater COMSEC Package (ICP) software system was developed by the Joint Chiefs of Staff to facilitate secure communications for joint forces. The value of ICP was truly recognized as a result of joint operations in Grenada. At the time, the lack of a common cryptographic keying material system severely hampered secure communications between service components. The component

commanders could maintain secure internal C3, but they could not maintain secure external C3 with adjacent components and higher headquarters. (8)

A serious weakness had been discovered in the conduct of joint operations. Forces deployed on short notice had not planned for external secure communications systems. If they had prepared ahead of time, they would have been forced to specify one services' cryptographic software short title for use by all of the Joint Task Force (JTF) components on any particular circuit. The CMS system was not prepared to provide such quantities of individual short titles on short notice. (17) Additionally, no common CMS short titles were held by all of the services for such joint or combined operations.

The ICP addressed this shortfall. A common package of CMS software was distributed which enabled the JTF commander and his component commanders to maintain effective, secure communication links on short notice. During operations in Southwest Asia, ICP was also used successfully by component commands to communicate to all aircraft in theater. (15)

During operation Desert Shield, the initial Marine forces deployed to Saudi Arabia were from I Marine Expeditionary Force (MEF). On the MEF level and above, ICP was used to initiate secure voice and data communications between the different service components. When II MEF forces were introduced within the I MEF area of

responsibility (AOR), CMS problems became readily apparent. The two MEF's maintained different short titles of CMS material for similar communication circuits, and too few I MEF CMS short titles existed within the system to allow for common software usage by the forces combined under I MEF.

The solution seemed simple: the forces under I MEF would utilize ICP CMS material to ensure interoperability of their communication circuits. This worked well until ICP software losses began to occur. These compromises of ICP material meant that all forces within the theater using the ICP had to change editions of CMS software, as the compromised editions were replaced by emergency releases.

This problem required immediate resolution because the CMS system does not maintain enough ICP material to supply every MSC. The ICP was only meant to be used at the component level. After several such compromises, the Marine Corps was forced to revert to their own CMS short title software for internal communication circuits. The ICP was rendered safe from excessive danger of compromise, but C3 interoperability between the I MEF and II MEF forces under I MEF was hampered because there wasn't enough common CMS software within the MEF. (12)

Recent world events have underscored the absolute requirement for interoperability among the forces, agencies, and nationalities operating in concert on the modern battlefield. During operations Desert Shield and Desert

Storm, CMS distribution to account holders was highly ineffective.

Distribution of CMS material was slow and labor intensive. This was due to the vast distances covered by maneuvering units and the large volume of paper CMS material required at the account level. Distribution of materials from the MSC parent account to the unit account required CMS custodians to drive many miles across open desert to receipt for CMS shipments from the parent account. This was slow, at best, during defensive operations. With the shift to offensive operations, this method of distribution could not keep pace with the tempo of maneuvering units. During sustained operations, secure and effective resupply of unit accounts was virtually impossible. (3)

Inadequate education of Marine commanders, CMS users, and custodians concerning CMS policies and procedures is another area that must be considered.

After-action reports and interviews with Marine commanders reveal that our leaders appreciate the need to maintain reliable secure communications, both in combat and in training. However, few understand how the system is designed, how it is used to support secure C3 among different units on the battlefield, what the CMS custodian must do to maintain the proper levels of CMS hardware and software within the unit account, and how this impacts their command both internally and externally. (10) NAVMC 2900,

"The Commanding Officer's Handbook for CMS Account Management," explains how to manage CMS accounts, but no standardized training is available to commanders. The handbook alone cannot fully prepare them to effectively use and maintain this capability.

CMS user training is conducted at the unit level. As a result, many units have highly proficient CMS users, but many more units do not have proper training in CMS use. Our MOS schools conduct little, if any, CMS user training for enlisted personnel or officers. Furthermore, the training that is provided is not coordinated throughout the service. (10) The quality of training at the unit level reflects experience of the individuals in the unit. Lack of standardized user training weakens an already complex, burdensome, and unresponsive system.

The CMS custodians, though formally trained for their duties at the Navy's CMS Custodian Course, usually are not familiar with their unit's communication circuits or equipment that requires CMS material. They rely upon the COMMO for oversight of CMS holdings. Unfortunately, as a result of being prohibited from custodial duties, many COMMOs do not exercise staff cognizance over this area resulting in a poorly planned, coordinated, and utilized CMS account. (4)

Marine Corps Order (MCO) 2201.1 prohibits communication officers from assignment to duty as unit CMS custodians.

Typically, CMS duties are assigned to personnel from the S-1 or S-3 sections. This was done to enhance system security and avoid the possible conflict of interest between the users of CMS material and its accountability chain. The net effect is to alienate CMS users, primarily the COMMOs, from one of the most important aspects of the system, its day-to-day management and oversight. We seem to be breeding an attitude among our COMMOs that CMS is a bad thing to take an interest in, and that it's not their responsibility.

Existing CMS problems are compounded by the proliferation of data communication devices. The Marine Corps deployed over 30 local area networks in Southwest Asia, more than any other service. This demand was driven by users who had experienced the value of networks in garrison. The local area networks were the engines that drove electronic sitreps, air tasking orders, naval messages, class I data, class II data, logistics reports, weather, and mail. One statistic coming out of Desert Storm was that in the 36 hours before, and until noon the day after G-Day, approximately 1.3 million messages were passed, supporting everything from command and control to Combat Service Support (CSS) functions.

The success of the local area networks in Southwest Asia will surely spark more requirements. The Marine Corps now possesses approximately 25,000 personal computers that can potentially be linked together in local area networks

like those in Desert Storm. This proliferation of data communication devices is a concern, because all internetwork connections must be covered by COMSEC devices. To keep these networks running, compatible key material and timely distribution of that material is essential.

One major administrative problem in our CMS system is the excessive amount of CMS material held in any account. At present all keying materials, codes, and authenticators are on paper. Accounts have to maintain enough copies of each of these in order to support the needs of all its users plus the required 90 days of reserve material, operational and exercise material, and contingency material. As can be seen, every custodian has a lot of paper to account for. The more material held by an account, the greater chance there is for a security violation. This is due to the extensive administrative requirements of accounting for COMSEC material. The problem is greatly compounded if an inexperienced or unqualified individual is assigned as the custodian.

PROPOSED SOLUTIONS

Now that we've looked at the problems plaguing our present CMS system, let's look at the possible solutions. Some solutions are already in place, and some are planned. It's important to understand that these solutions are not designed to correct one specific problem; the implementation of each solution will affect many problem areas.

An idea being tested by I MEF at the present time seems to have a lot of merit. This idea is to establish a MEF COMSEC Management Office (MCMO), based mainly on the Army's TCMO concept. The MCMO will improve CMS coordination for deployed forces, decrease the amount of CMS held by accounts on a daily basis, and ensure proper education for CMS personnel.

The MCMO, an organization or section resident within the MEF headquarters, would hold keying material for contingencies so that subordinate units would not have to maintain it. This arrangement will effectively reduce the copy count and management burdens associated with contingency keymat (i.e. ICP material) for subordinate units. Units can be prevalidated -- that is, authorized by a controlling authority to hold certain keying materials, to receive material (again material such as ICP) without having to actually hold it. The MCMO would coordinate and manage contingency keymat so that when a unit needed it, they would draw it from the MCMO. This concept could also be applied to actual operational keymat as well. Subordinate units would hold exercise key on a day-to-day basis, and the MCMO would hold operational key to issue on an as-needed basis.

The MCMO would be the sole point of contact for the MEF in CMS matters both internal and external. The MCMO would be the main point of contact to external organizations such

as distribution agencies (i.e. COMSEC Material Issuing Office (CMIO)), other services, controlling authorities, etc. The MCMO would also be the main point of effort within the MEF for training and education of CMS.

If the MEF is to deploy, the MCMO would deploy with it and set up in theater and provide the critical coordination, in-theater distribution, and storage functions that were lacking in Southwest Asia. The MCMO would also interface with the Army's TCMO in a joint environment.

This MCMO concept can reduce the amount of CMS software maintained at the subordinate level on a day-to-day garrison basis. As a result, much of the administrative workload would be eliminated at the lower levels. This is particularly desirable where the CMS custodian billet is a collateral duty. It will also facilitate better coordination with other services, controlling authorities, and distribution agencies because these outside organizations will have one command to coordinate with. (16) (19)

Implementation of the MCMO will push most of the work required to manage CMS to the MEF level, but the MEF will have individuals dedicated to dealing with CMS as a full time job.

Some problems with this concept concern manning the MCMO. Where will the staff come from and what rank should

they be? How will operational and contingency key be provided to units? If subordinate units maintain all the key material they could possibly need plus the required 3 months reserve on board (ROB), they can virtually pick up and go without having to worry about drawing CMS material from the MCMO and still receive their required material on a regular basis from the CMIOs.

An initiative is now being implemented to reduce the amount of paper CMS material held and handled at all levels of command. The Navy, through the direction of Vice Admiral Tuttle, CNO Op 094, is moving to a paperless CMS environment. As early as the latter half of 1990 and especially during Desert Shield and Desert Storm, the Navy was electronically sending key material over the fleet broadcast to its deployed battlegroups with much success. After-action reports from these deployed battlegroups greatly acclaimed its use. The Navy has established sound procedures for this technique and actively uses them.

This concept is known as electronic distribution of key or OTAR. Presently it is used tactically, but plans are in the works to abolish most of the paper key and replace it in garrison and in the field with not only the electronic distribution of key but also by electronic management of CMS with personal computers and STU-IIIs. The OTAR concept will replace today's safes, paper keying material, and logbooks with more manageable electronic equipment. This equipment

includes electronic storage devices (such as the KYK-13, KYX-15), a personal computer, and a STU-III. Electronic COMSEC management will greatly reduce administrative burdens.

The security aspects of electronic management are also appealing. When a MEF/Marine Air Ground Task Force (MAGTF) deploys, it can receive all required keys over-the-air, so that it can deploy anywhere and receive any keys necessary within a matter of hours. Additionally, any key material needed for internal requirements can be generated by the sending agency (NCTAMS, MCMO) so that the key material will be completely unique to the MEF/MAGTF. Furthermore, in the event of a compromise, only the MEF/MAGTF is affected, and it can immediately generate a new key.

NSA is working to implement this idea for all the services, so that by the end of the century all keying material, distribution of key, and management of the system will be electronic.

Presently the Marine Corps is still using paper, even though the Navy has proven procedures in place to electronically distribute key material in a tactical environment, and despite the fact that many reports have indicated the severe problems of not having the appropriate version or amount of key material. These problems are easily solved by using over-the-air distribution. The Marine Corps can receive these keys in the electronic form.

As a matter of fact, within the Atlantic Fleet, the Navy has borrowed these electronic storage and key generating devices (KYK-13 and KYX-15) from the Marine Corps to satisfy the needs of its commands. The Marine Corps has practiced electronic distribution of key for years in VINSON (KY-57) operations or Saville Advanced Remote Keying (SARK). Over-the-air-distribution (OTAD) of key uses the same principles as SARK but on a larger scale. The Navy is rapidly moving to a paperless CMS environment, leaving the Marine Corps behind.

OTAD transfers all the key material a unit needs electronically over one secure circuit for use on other cryptographic devices. These cryptographic devices are systems such as the KY-57, KY-65, KG-84, the embedded COMSEC device for SINCGARS, and the new Advanced Narrowband Digital Voice Terminal (ANDVT). We already employ or will employ these systems on virtually all of our circuits now.

Headquarters Marine Corps (HQMC) has proposed an initiative to aid in the management of CMS at the major command level by appointing of a Command COMSEC Employment Officer (CCEO). Although HQMC recognizes that the CCEO responsibilities have been associated with the G-6/CEO section, they state that CMS responsibilities have often been delegated to the CMS custodian, who in many cases does not have the background, experience, or training to perform these duties. Some of the responsibilities that will be

associated with the CCEO are:

1) Keeping the commander abreast of all operational COMSEC matters relating to the command and its subordinate units.

2) Monitoring the command's COMSEC requirements: coordinating with staff sections, internal and external to the command, to ensure that the command's COMSEC plans are integrated into the command's Operations Security (OPSEC) and C3CM planning.

3) Advising subordinate commands of COMSEC keying material requirements for operations and requirements.

4) Advising the CMS custodian of changes in requirements.

5) Acting as the command's item manager for cryptographic hardware by coordinating with the supply officer and CMS custodian to ensure that cryptographic hardware and ancillary devices are on hand.

6) Recommending reallocation of COMSEC assets among subordinate commands to ensure maximum use of available assets.

7) Performing controlling authority duties for keying material for which the command is responsible.

8) Conducting inspections and surveys of subordinate commands COMSEC operational readiness. (20)

HQMC contends that assigning a CCEO in writing, will give each major command a designated focal point for these responsibilities. These functions are the responsibility of

the G-6/CEO and should never be delegated to an individual not directly responsible to the G-6. Proper CMS planning is crucial to the success of any operation.

It is not effective or efficient to assign these responsibilities to someone who must work hand in hand with the CMS custodian. The CMS custodian, in our present system, is usually working for a completely different section head, normally the G-1. Additionally, he has absolutely no experience in the employment of such material. The question therefore is simplicity itself. Why not make the CMS custodian and the CCEO responsible -- administratively and operationally -- to the G-6/CEO for all matters dealing with CMS and COMSEC? The Marine Corps is the only service that does not follow this system. The Navy, Coast Guard, Army, and Air Force all have the CMS custodian and CCEO working for the G-6/CEO.

Defense of our present system raises legitimate concerns. One concern is that the CMS custodian, a full time job, will then have to come from the present G-6 staff. This may be so but, alternate custodians can come from anywhere providing they meet the basic requirements. So theoretically, only the CMS custodian need be from the G-6 shop. Other custodians can be spread evenly throughout the rest of the staff. It only makes good sense to have the CMS custodian from the G-6. He will not only be familiar with the cryptographic material but will know how it is

employed.

HQMC, to reduce the account management problems previously discussed, has proposed more stringent training and assignment requirements. In a nutshell these are:

1) Prohibit assignment of individuals as the CMS custodian or primary alternate until formal training has been completed (1 week course offered by NETC Newport RI). Since each account has four custodians, when the custodian or primary alternate is relieved, simply move the second or third custodian up to take over until training is completed for the incoming custodian.

2) Establish a minimum assignment for the custodian of at least 18 months for a three year tour and nine months for a one-year tour. This tour length will allow the custodian to become familiar with CMS account management. (20)

These sound management proposals can only improve CMS accounts. One more assignment requirement should be added. The responsible assignment of custodians, instead of assigning the billet to the lieutenant or gunny who just can't seem to hold on to a job. Proper COMSEC management is vitally important to everyone, and irresponsible assignment of 'expendable' individuals to be CMS custodians must stop.

ICP material, as discussed earlier, was developed by JCS to improve the interoperability of forces and CINCs during contingency operations. This material has proved to work successfully. After-action reports have highlighted

the need for a Marine-Corps-specific contingency key to be used by Marine forces from different MEFs pulled together. There is a Marine Corps contingency key; however, it was not widely publicized and had a relatively small copy count. (17) Our operations in Southwest Asia revealed the need for more of this Marine Corps contingency keymat with distribution validated to all units down to the battalion/squadron level.

RECOMMENDATIONS

The present CMS system and the way the Marine Corps uses it must change. Short term solutions are being implemented, but we need a comprehensive system to take us into the next century, not a bunch of good ideas being implemented separately. Here's what that system should be.

First and foremost we need full implementation of the MCMO concept. This organization shows a lot of merit. Not only must the MCMO be institutionalized in our MEF headquarters, but it must be supported by the commander and staff. A table of organization (T/O) must be established to adequately meet the requirements, and responsible individuals who have the appropriate experience and training must be assigned to it. Conversations with the MAGTF Integration Team indicate the new proposed MEF structure will have three individuals assigned to a CMS section within the MEF G-6. This could form the nucleus of the MCMO, CMS is a very critical component of successful command and

control and must be treated as such. Furthermore, a MCMO, on a smaller scale, must be sent with a Marine Expeditionary Brigade (MEB) size organization if and when it deploys. This could be just an augmentation from the main MCMO to round out the MEB's G-6 staff.

As electronic distribution of key becomes the standard, the Marine Corps must utilize this procedure in all operations. The MCMO would be the perfect organization to coordinate electronic distribution now and in the future.

To effectively carry out its mission, the MCMO organization must fall under the cognizance of the G-6. The MCMO must also have administrative and operational control of the CMS custodian so that all CMS matters can be properly coordinated. The Command COMSEC Employment Officer can also be integrated into the MCMO. On lower levels of command one individual should be responsible for COMSEC employment and CMS management. If the Command COMSEC Employment Officer and CMS custodian are the same person or if the CMS custodian works both administratively and operationally for the CCEO, then so be it. Separation of these two individuals is unnecessary and causes easily avoidable problems.

Proper education of CMS personnel, users, and command personnel is essential. Through education we can break down misconceptions of the CMS system, so these individuals can understand what COMSEC can do for them. COMSEC is nothing

to be afraid of, in fact when employed properly, it is a combat multiplier. Here again the MCMO can earn money. The MCMO, if staffed properly, can be the focal point of effective CMS training within the MEF. Through the use of mobile training teams, assist visits, and inspections we can really begin to tighten up our CMS programs. Coupled with training is the appropriate assignment policy discussed previously. Again this only makes good managerial sense. It adds stability to a critical job.

The other change that will cement all this together is external to the Marine Corps. It lies with the Navy where policy is developed and implemented, DCMS (Director, COMSEC Material System). The Marine Corps presently only has one Marine Gunnery Sergeant at DCMS and he works in the COMSEC hardware section of DCMS. We need at least two more individuals of appropriate rank, master sergeant to captain, to work in the policy section and the operations section. These individuals, who understand the unique aspects of Marine Corps operations, can help develop policy in conjunction with the Navy. The Navy can benefit from this arrangement as well. Their substantial ground forces operate like the Marine Corps (SEALS, Beachmasters, EOD units, Amphibious CBs, Cargo Handling units). Additionally, as the Secretary of the Navy has directed that certain parts of CNO and HQMC integrate, this area is a good candidate for that integration.

CONCLUSION

We believe, the MCMO concept should be the core of the Marine Corps' CMS program. By localizing the management within each MEF, we can ensure an effective utilization of the system. And within subordinate units of the MEF, the employment and management of COMSEC should rest with one individual, the Communications Officer. Also establishing Marine Corps personnel with the Navy policy makers at DCMS will help tie the whole CMS program into an effective, user-friendly, and responsive system. Only by implementing these basic ideas will the Marine Corps have an effective and responsive COMSEC program at its disposal.

BIBLIOGRAPHY

1. Army Regulation 380-41 (AR 380-41). U.S. Army. Feb 89

2. ADP Support for the Marine Corps. Computer Sciences School, Student Handout, DFO 1000, Dec 91: 1.

3. CMS. MCLLS Long Report, Number 91535-97213 (02252). Submitted by 9thCommBn. 12 May 91

4. Cross, R.N., Chief Warrant Officer-2, USMC. Personal interview. 2d FSSG. 24 Jan 92

5. Commanding Officer's (CO's) Handbook for Communications Security Material (CMS) Account Management. NAVMC 2900, CCT-636, May 89: 4-5.

6. Communications Security Material System (CMS) 4L Manual (CMS 4L). DCMS

7. Cryptographic Security Policy 1A (CSP 1A). COMNAVSECGRU.

8. Dillon, J.T., Captain, USMC. Personal interview, CCSC MCCDC. 3 Feb 92.

9. Fraison, R., CW4, USA. Personal interview, XVIII Airborne Corps. 21 Dec 92

10. Hull, J.E., Lieutenant Colonel, USMC. Personal interview, 2ND FSSG. 24 Jan 92.

11. Ibanez, G., Captain, USMC. Personal interview, FMFLANT. Various Dates.

12. Inter-Theater Communications Security Packages (ICP). MCLLS Long Report, Number 02141-57815 (02281). Submitted by I MEF. 23 Mar 91.

13. Jefferson, J.J., Captain, USMC. Personal interview, CCSC MCCDC. 3 Feb 92.

14. Jensen, L.A. A Description of the Functions of the Office of the Director, COMSEC Materials Systems. Navy Research Laboratory Memorandum Report 6631. 10 May 1990

15. Licari, J., Captain, USMC. Personal interview, MAWTS-1. 6 Dec 92.

16. Malone, Lieutenant, USN. Personal interview, I MEF. 24 Jan 92.

17. Nicosia, Dee. Personal interview, HQMC. 28 Jan 92.

18. Pratt, M.A., Captain, USMC. Personal interview, CCSC MCCDC. 3 Feb 92.

19. Proposal to Establish Marine Corps MEF COMSEC Management Officer (MCMO). CMC Washington DC 191900Z Jun 91

20. Proposed Changes to COMSEC Account Management. CMC Washington DC 081900Z Jan 92

21. Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT) Procedures Manual Promulgation. CNO ltr 2250 Ser 941J/1U556106 dtd 07 Feb 1991.

22. Technical Bulletin 380-41 (TB 380-41). U.S. Army. Volumes 1 thru 5. Sep 90