Director, Operational Test and Evaluation

Mobile User Objective System (MUOS)

Multi-Service Operational Test and Evaluation-2 Report

June 2016

This report on the Mobile User Objective System (MUOS) fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing, the operational effectiveness, suitability and cybersecurity of the MUOS.

J. M.

J. Michael Gilmore
Director

The Mobile User Objective System (MUOS)

Executive Summary

This document reports the evaluation of test adequacy, operational effectiveness, operational suitability, and cybersecurity of the Mobile User Objective System (MUOS). The Director, Operational Test and Evaluation (DOT&E) based this evaluation primarily on data from the second Multi-Service Operational Test and Evaluation (MOT&E-2), conducted from October 19 to November 20, 2015, and a cybersecurity Adversarial Assessment, conducted from April 4 – 8, 2016. The Naval Command Operational Test and Evaluation Force (COTF), with support from the Army Test and Evaluation Command (ATEC) and Air Force Operational Test and Evaluation Command (AFOTEC), conducted the operational test in accordance with the DOT&E-approved test plan, approved on October 13, 2015.

MUOS is not operationally effective in providing reliable worldwide Wideband Code Division Multiple Access (WCDMA) communications to tactical users. MUOS was able to provide WCDMA communications on a limited scale during MOT&E-2, but MUOS cannot achieve this performance worldwide given the significant problems with planning and provisioning, situational awareness, network management, and capacity. MUOS does not provide a communications capability that will support deployed users as the number increases from the 48 tested to the more than 10,000 expected at full operational capacity. When MUOS works it provides message accuracy and quality of service better than legacy ultra-high frequency (UHF) communications. However, MUOS cannot communicate on all types of networks. COTF did not test fixed assigned networks because of known problems with them. The two MUOS satellites in the test operated at 72 percent of capacity and could not mitigate unintentional electromagnetic interference. There is currently no means to monitor WCDMA radio outages, leading to long outages for tactical users. Failed rekey events can result in widespread tactical communications outages – perhaps globally for an entire military Service. MUOS did not provide reliable connectivity to users. Link availability is a measure of the ability of users to connect and maintain communications over MUOS. Based on the 4,609 voice transmissions during the test, DOT&E estimates a 68 percent link availability against a 97 percent threshold requirement during MOT&E-2.[1]

The operational community cannot monitor and manage MUOS. The Army Space and Missile Defense Command/Army Strategic Forces Command (SMDC/ARSTRAT) serves as the Consolidated Satellite Communications (SATCOM) System Expert (C-SSE) for Department of Defense (DOD) narrowband and wideband SATCOM constellations. SMDC/ARSTRAT was unable to perform beam carrier management during the MOT&E because the Navy has not granted the C-SSE access to the controls to perform its mission. MUOS does not provide the U.S. Strategic Command (USSTRATCOM) Satellite Operational Manager (SOM), SMDC/ARSTRAT C-SSE, and resource managers an effective system monitoring and display

[1] If the 854 data transmissions are also considered, then the Link Availability estimate increases to 72.4 percent. However, DOT&E believes this overestimates Link Availability since COTF attributed failures bringing data networks into operation as configuration problems and the failures were not counted as link failures.

capability. The SOM and C-SSE cannot monitor MUOS to evaluate actual system performance against planned performance. The Regional SATCOM Support Center (RSSC) resource managers often cannot access the provisioning system to plan user communications. Long outage times with the provisioning system can prevent tactical users from accessing the system when needed. The geolocation capability could not be tested.[2] The Navy deferred the capability to geolocate an interferer prior to MOT&E-2. This capability and the system fixes should be tested in the Follow-on Operational Test and Evaluation (FOT&E) tentatively planned for fiscal year 2018 (FY18).

MUOS is not operationally suitable. The ground system lacks the stability and maturity to enter into and sustain global operations. MUOS does not provide communications that deployed users can rely on when the system is in widespread use or at full capacity. MUOS performed poorly in almost every area of operational suitability. The cumulative effects of these failures could have grave operational consequences to deployed forces. MUOS does not meet the user-defined threshold for operational availability. The Network Management Segment (NMS), the nerve center of MUOS operations, was available 6.3 percent of the time during MOT&E-2 against a 95 percent threshold criterion. NMS had long repair times, numerous high-priority problem reports, poor usability, poor documentation, and high reliance on depot maintainers. Further, NMS is under-manned and operators do not consider themselves adequately trained to perform their mission. MUOS does not meet threshold requirements for segment repair times. The MUOS threshold segment repair time is 45 minutes (0.75 hours). The NMS median repair time based on 37 repair actions was 89 hours. NMS mean repair time was 1,058 hours. MUOS demonstrated repair times in terms of hours, even with depot maintainers on-site, in violation of the Navy’s own published logistic support plans. The MUOS Program Manager created a depot support forward presence to reduce downtime. The Navy saw these problems in the June 2015 Technical Evaluation and decided to go to operational test rather than delay the test and fix the problems. The system satellite controllers, planners, provisioners, and network managers were dissatisfied with the provided training, documentation, and system usability.

The system is not secure from cyber-attacks. The COTF Adversarial Assessment team and USSTRATCOM conducted independent cyber assessments and obtained similar results. They discovered over 1,000 cyber vulnerabilities in the MUOS ground system. Approximately half of these vulnerabilities are Category-II (CAT-II) and above. CAT-II vulnerabilities have the potential to result in loss of confidentiality, availability, or integrity. COTF did not evaluate the cybersecurity for the parts of MUOS involved in satellite control. During FOT&E planned for FY18, COTF should evaluate the cybersecurity of the entire MUOS. The Navy should address the many cyber vulnerabilities in the MUOS prior to FOT&E. The details of the COTF Adversarial Assessment may be found in the classified annex to this report.

[2] Geolocation is the identification of the real-world geographic location of an intentional (jammer) or unintentional interferer.

MUOS is not ready to support military operations. Until the problems are fixed and verified in the FOT&E, the system use should be limited to small non-combat missions, testing, training, and exercises in the United States and protectorates in order to develop, exercise, and mature operational concepts and processes with a particular focus on addressing known issues and MOT&E-2 findings.

System Description and Mission

MUOS is the DOD's next-generation narrowband military SATCOM system, replacing the UHF Follow-On (UFO) constellation that is reaching end of life. MUOS is a satellite-based communications network designed to provide worldwide, narrowband, beyond line-of-sight, point-to-point (P2P), and netted communication services to multi-Service organizations of fixed and mobile terminal users. MUOS is designed to provide 10 times the throughput capacity of current narrowband SATCOM. The Navy designed MUOS to provide increased levels of system availability over the current constellation of UFO satellites, as well as improved availability for small, disadvantaged terminals that is typical for a current mobile user over UFO. The MUOS has six segments that compose the system.

The Space Transport Segment is intended to consist of four operational satellites and one on-orbit spare. Each satellite hosts two payloads: a legacy communications payload that mimics the capabilities of a single UFO satellite, and a MUOS WCDMA communications payload. The satellite constellation is designed to provide coverage between 65 degrees North and 65 degrees South latitudes and provide dual coverage to more than 65 percent of the service area.

The Ground Transport Segment is planned to consist of four radio access facilities (RAFs) and two switching facilities (SFs) to manage MUOS communication services including the allocation of radio resources and user authentication, routing, switching, and mobility management. The program manager intends for the Ground Transport Segment to provide an interface into the DOD Teleport system to access Defense Information Systems Network (DISN) services including the Defense Switch Network, Non-classified Internet Protocol Router Network, and the Secret Internet Protocol Router Network (SIPRNet).

The NMS consists of one Network Management Facility (NMF) that hosts equipment to conduct network management functions, support communications planning, and determine the location of UHF narrowband interferers. The NMF will be collocated with an SF and RAF at Wahiawa, Hawaii.

The Ground Infrastructure Segment (GIS) provides terrestrial mesh connectivity between ground facilities, including the Satellite Control Segment (SCS), the NMF, and RAFs. The GIS uses the existing DISN infrastructure.

The SCS consists of a primary MUOS Telemetry, Tracking, and Commanding facility at Naval Satellite Operations Center (NAVSOC) Headquarters at Point Mugu, California, and a backup facility at Detachment Delta at Schriever Air Force Base (AFB), Colorado. The SCS consists of two main sub-systems: the Satellite Control Subsystem and the Orbital Analysis System (OAS). The control subsystem commands and controls the functions for maintaining the satellites on-orbit and receives telemetry from the satellites to monitor the health of the satellites. The control subsystem also controls the UHF communications payload on the satellites.

The User Entry Segment provides the software interface between the MUOS terminals and MUOS. This includes the protocols, formats, and physical layer characteristics for MUOS-compatible communication services. The Services are responsible for developing and fielding MUOS-compatible terminals. The Handheld, Manpack, Small-Form Fit (HMS) Manpack radio (AN/PRC-155) is currently the only production representative terminal available and participated in the MOT&E-2.

The MUOS mission is to provide narrowband satellite communications support for a wide-range of DOD and government operations, especially those involving mobile users.[3] MUOS is designed to support ad-hoc communications between single users via P2P networks, allow groups of users to participate in pre-planned networks, give individuals and groups access to services on connected networks (such as SIPRNet), and enable users to reach outside telephone systems.

The DOD intends for MUOS to provide users with priority-based access to a broad range of P2P, point-to-network (P2N), and group communication services supporting voice, data, and mixed voice and data. Group services provide netted communications to two or more users and are pre-planned. Users may quickly activate P2P, P2N, and pre-defined group services on demand in the field and then release them, freeing resources for other users. The Program Manager plans for MUOS to provide assured access to designated high priority communication services, with the ability to preempt lower priority services when necessary. MUOS is not required to be functional in a nuclear scintillation environment or against a radio frequency jamming attack. However, it is expected to spectrally adapt to unintentional interference and apply electromagnetic interference mitigation techniques to maintain capacity.

Test Adequacy

The operational testing of MUOS was adequate to support an evaluation of the system’s operational effectiveness, suitability, and cybersecurity. COTF, with support from ATEC and AFOTEC, conducted the operational test in accordance with the DOT&E-approved test plan, approved on October 13, 2015. The Navy is planning an FOT&E in FY18. COTF collected sufficient data to evaluate the operational effectiveness, suitability, and cybersecurity of MUOS.

DOT&E’s evaluation is primarily based on data collected by COTF and supporting Service Operational Test Agencies (OTAs) from October 19 to November 20, 2015, and a COTF-conducted cybersecurity Adversarial Assessment from April 4 – 8, 2016. Data included satellite control digital log files, NMS automated logs, manually recorded logs, user surveys, and DOT&E staff observations of testing. The data were collected at the satellite control center, at the NMS and Wahiawa RAF, and at ground sites.

[3] Narrowband is typically defined as 64 kilobits per second or less.

Operational Effectiveness

MUOS is not operationally effective in providing reliable worldwide WCDMA communications to tactical users. MUOS was able to provide WCDMA communications on a limited scale during MOT&E-2, but cannot achieve this performance worldwide given the significant problems with planning and provisioning, situational awareness, network management, and capacity. When MUOS works, it provides message accuracy and quality of service better than legacy UHF communications. However, MUOS cannot communicate on all types of networks. COTF did not test fixed assigned networks because of known problems with them. The two MUOS satellites in the test operated at 72 percent of capacity and could not mitigate unintentional electromagnetic interference. There is currently no means to monitor WCDMA radio outages in the MUOS, leading to long outages for tactical users. Failed rekey events can result in widespread tactical communications outages. DOT&E estimates a 68 percent link availability against a 97 percent threshold requirement during the MOT&E-2 period, based on the voice message accuracy.

The operational community cannot monitor and manage MUOS. The SMDC/ARSTRAT C-SSE was unable to perform beam carrier management during MOT&E-2 because the Navy has not granted the C-SSE access to the controls to perform its mission. MUOS does not provide the USSTRATCOM SOM, SMDC/ARSTRAT C-SSE, and resource managers an effective system monitoring and display capability. The SOM and C-SSE cannot monitor MUOS to evaluate actual system performance against planned performance. The RSSC resource managers often cannot access the provisioning system to plan user communications. Long outage times with the provisioning system can prevent tactical users from accessing the system when needed. The geolocation capability could not be tested. The Navy deferred the capability to geolocate an interferer prior to MOT&E-2. This capability and the system fixes should be tested in the tentatively planned FY18 FOT&E.

Capacity (Key Performance Parameter)

MUOS does not meet the threshold capacity Key Performance Parameter (KPP) criteria, based on the two satellite configuration in MOT&E-2. The 2 satellites under test operated at 72 percent of capacity during MOT&E-2. DOT&E did not consider the Indian Ocean region and Atlantic region satellites’ configurations since they were not available for operational testing. Regardless, the constellation cannot meet required capacity, even if the remainder of the constellation was fully populated and all ground stations operational. If the remaining MUOS satellites operated at full capacity, MUOS could only reach approximately 86 percent capacity.

DOT&E determined that 92 of the possible 128 Satellite Beam Carriers (SBCs) were active on the Pacific (PAC) and Continental United States (CONUS) region satellites for an availability of 71.9 percent. The Navy either locked or turned off 28.1 percent of the capacity to prevent problems with interference from ambient radio frequency signals. A locked SBC means users cannot access it, effectively losing 5 megahertz of potential spectrum in that beam. A majority (56 percent) of 32 satellite beams across the two satellites were in a degraded mode. DOT&E determined that:

- 6 of 32 beams were at 25 percent capacity
- 6 of 32 beams were at 50 percent capacity
- 6 of 32 beams were at 75 percent capacity
- The remaining 14 beams were at 100 percent capacity

Additionally, prior to MOT&E-2, the MUOS program modified control parameters to improve WCDMA call completion performance based upon the June 2015 Technical Evaluation results. These changes traded call performance for capacity. The decrease in capacity is not fully understood because the Program Manager ceased funding of the MUOS Performance Model (MPM) in 2014 for cost avoidance reasons. The developing contractor estimated the capacity losses based on the multiple changes as an additional 2-5 percent, but the actual figure may be more. Without the MPM, the government has no capability to validate the performance and capacity trades regarding MUOS capacity. There are additional details in the classified annex to this report.

Link Availability

Link availability is a measure of the ability of users to connect and maintain communications over MUOS. DOT&E estimates that MUOS did not meet the Link Availability KPP during MOT&E-2. MUOS Link Availability was 68 percent against a threshold Link Availability criterion of 97 percent availability averaged over a year. This is not a directly testable measure. The MUOS Program Manager uses block error rates (BLER) to determine if a link is available, through the MPM is no longer available to the government. BLER is a ratio of the number of erroneous blocks to the total number of blocks received on a digital circuit and a typical performance measure in WCDMA communications. COTF did not measure BLER during MOT&E-2, as BLER testing is typically done in a lab environment and not easily done operationally. DOT&E believes the message accuracy is an appropriate proxy metric for BLER because both metrics count the loss of information on a transmission. Based on the 4,609 voice transmissions during the MOT&E, MUOS achieved a link availability of 68 percent during MOT&E-2. If the 854 data transmissions are also considered, then the Link Availability estimate increases to 72.4 percent. However, DOT&E believes this overestimates Link Availability since COTF attributed failures bringing data networks into operation as configuration problems and did count the failures against Link Availability.

Beam Carrier Management

The SMDC/ARSTRAT C-SSE is USSTRATCOM's daily manager of MUOS and is responsible for making operational decisions related to communications performance. Beam carriers are the building block of MUOS and are equivalent to cells in a cellular network. The C-SSE was unable to perform beam carrier management during the MOT&E because the Navy has not granted the C-SSE access to the controls. Beam carrier management is designed to provide the C-SSE with the ability to create a beam management region and configure satellite beams and carriers for each MUOS satellite and analyze configurations for viability. Beam Carrier management is currently performed by the developing contractor.

System Monitoring

The MUOS does not provide the SOM, C-SSE, and resource managers an effective system monitoring and display capability. The SOM, C-SSE, and resource managers access MUOS via a web portal called the MUOS Planning and Provisioning Application (PlanProvApp). This web portal is their window into MUOS and is designed to provide them with a shared understanding of the system state – thus providing decision makers with tools to effectively make strategic decisions. During MOT&E-2, resource planners were able to obtain information from the system in 61 percent (52 of 85) of attempts. USSTRATCOM and SMDC/ARSTRAT cannot monitor MUOS and evaluate actual system performance against planned performance. MUOS does not provide them with an accurate, real-time status of the system state. The system was unable to maintain call records for the 60 terminals that participated in MOT&E-2.

Testers observed Situational Awareness Views and Reports failures, including page loading errors, partially loaded web pages, incomplete reports, and inaccurate reports. For example, MUOS reported that there were no user communications occurring when, in fact, there were known active networks that MUOS should have reported. The Navy recorded similar results from the June 2015 Technical Evaluation in preparation for MOT&E-2. Based on the Navy Technical Evaluation data, DOT&E found that the developmental testers assessed the aggregate situational views and reports as passing in 63.9 percent (131 of 205) of attempts.

MUOS provides a web portal for users to understand system status. When successful, web portal accesses took a mean time of 5 minutes with a 95 percent confidence interval of 4.8 to 5.2 minutes during MOT&E-2.

The problems discussed above will grow exponentially when more users operate more networks across different theaters of operations. While the Navy made efforts to speed up latent processing times, the problems with time-outs, inaccuracy, and incomplete reports remained uncorrected and resurfaced in MOT&E-2. Two situational reports are indicative of the types of problems the C-SSE and resource planners experienced: Global System View and Call Detail Records (CDRs). The Global System View, which provides an overview of the system status, was inaccurate over the entire MOT&E-2 period. For example, this view showed MUOS satellites in the wrong positions and the SBC status table was completely empty. MUOS users stopped using it because it was known to be inaccurate. The status can be manually overridden but then the changes sometimes cannot be easily undone. There is no concept of operations (CONOPS) to update the Global System View and no one is tasked to keep the status current within MUOS. The MUOS network managers have found the Global System View to be so unreliable that they now manually track the status of the various components of MUOS using Microsoft PowerPoint presentations.

The MUOS C-SSE, resource planners, and network managers could not determine who was using MUOS during MOT&E-2 because the MUOS NMS was unable to accurately maintain CDRs in a timely manner. The CDR data are the primary data that NMS uses for Situational Awareness Group Usage reports. The RSSC-West resource planners queried the system for

Group Call Usage Reports 234 times during the MOT&E. Only 40.6 percent (95 reports) were successfully displayed.

NMS CDRs could not be retrieved in a timely manner, even though there were few users on the system. The latency in retrieving CDRs grew to 31 hours with a backlog of 24,500 records. The Navy experienced latent and inaccurate CDRs during the June 2015 Technical Evaluation and chose not to correct them prior to MOT&E-2. The root cause for the inaccurate and late CDRs was never determined in either in the Technical Evaluation or MOT&E-2, but the problems were likely caused by servers and databases running at capacity and running in "debug" mode, a non-operational troubleshooting configuration.

Provisioning

Provisioning of Terminals by the Provisioning Authority

SMDC/ARSTRAT is the provisioning authority for MUOS. The SMDC/ARSTRAT provisioners were able to provision terminals 100 percent (60 of 60) of the time during MOT&E-2, but not without problems. MUOS treats internet protocol (IP) addressing differently, depending upon the enclave. The current MUOS end-to-end architecture has a generic discovery server (GDS) for the Secret U.S.-Only enclave (red-side), but not for the unclassified For Official Use Only (FOUO) enclave or the Top Secret enclave. As a result, planners use dynamic IP addressing on the Secret enclave but static IP addressing on the FOUO and Top Secret enclaves.

A GDS enables the use of website names and e-mail addresses rather than requiring users to know specific numerical IP addresses. A GDS also enables dynamic versus static IP addressing.[4] If terminals use static IP addresses, then the terminal will require re-provisioning anytime a new route is required or the user needs to place a call to another user whose terminal information was not previously provisioned in that terminal. During military operations static IP addressing would become burdensome to MUOS users.

Since there is no GDS on the FOUO enclave, the SMDC/ARSTRAT provisioner has to assign terminals static IP addresses for MUOS users to conduct P2N communications. The SMDC/ARSTRAT provisioner has to use a limited set of static black-side IP addresses that he has to manage using an offline spreadsheet program. When the provisioner places the static IP addresses in the MUOS PlanProvApp and executes the provisioning, the manual bookkeeping of IP addresses induces errors. The SMDC/ARSTRAT provisioner has to transfer the terminal profile request information from a USTRATCOM tool – the Joint SATCOM Mission Planning System (JSMPS) – to MUOS. He performs the terminal provisioning actions and then transfers the information back to JSMPS. Through this cumbersome process it is possible to mismatch IP addresses between the MUOS terminals and the MUOS ground system. A mismatch can occur because the two systems sort the planning information and auto-populate that information

[4] A static IP address is when a device has an IP address that never changes. In dynamic IP addressing the Dynamic Host Configuration assigns a different address every time a device connects to a network. These IP addresses are temporary, and can change over time.

differently. This mismatch will result in failed user communications unless the problem is caught and fixed by the provisioner prior to the provision being sent to the ground system and unit planner. In MOT&E-2, the SMDC/ARSTRAT provisioner was able to correct the errors before the test began for the limited number of radios used during the test. However, it will be, difficult to impossible, for provisioners to make such corrections when there are thousands of MUOS radios deployed.

The MUOS PlanProvApp allows the provisioner to select fixed IP addresses for P2P and P2N networks outside of the appropriate subnetworks without warning when allocating resources. If the provisioner does not catch the error, this results in failed P2P and P2N services for deployed users. The Navy has been aware of this problem since the priority (PRI)-2 problem report submission in January 2015. The Navy should fix the erroneous IP address allocation outside IP subnetworks to avoid deployed user failed communications.

The MUOS lacks a long-term solution to resolve NIPRNet and SIPRNet website names and provide content back to users. The MOT&E-2 used temporary assets housed in a test laboratory in San Diego. However, long-term tactical Domain Name Service (DNS) capabilities are needed to support future MUOS to NIPR and SIPR requirements. A DNS enables the use of website names and e-mail addresses rather than requiring users to know specific numerical IP addresses. Without a DNS, users are unable to access NIPRNet and SIPRNet websites without direct knowledge of the specific server IP address. The Navy should work with the Defense Information Systems Agency to implement a SIPRNet and NIPRNet DNS capability for MUOS.

The MUOS waveform lacks a Dynamic Host Configuration Protocol (DHCP) capability that assigns unused IP addresses from MUOS radios to their attached computers used for processing data communications. Unit planners have to manually assign static IP addresses to connect the MUOS radios to IP devices such as SIPRNet or NIPRNet computers. If the connected devices are moved and paired with a different radio or a new device is connected to the radio. When this occurs, unit planners have to manually reconfigure the IP addresses to enable the radio to communicate with the connected device. This can be especially problematic when unit planners do not have authorization to reconfigure computers, such as those computers fielded through the Navy Marine Corps Intranet program. The Navy should implement a DHCP capability in the MUOS waveform to enable dynamic IP assignments for connected devices.

Group Network Provisioning

MUOS does not meet the KPP threshold criterion to configure and reconfigure high-priority networks in 5 minutes, and routine networks in 15 minutes. The user-specified definition of configuring and reconfiguring networks includes planning, allocating, and prioritizing accesses to resources. Planning the network and ensuring they will work (network analysis) took on average 27.9 minutes (10.5 – 45.2 minutes at the 95 percent confidence interval) for high-priority networks. The network analysis sometimes failed to complete and required the planner to close the application and restart the process. The Navy was aware of the analysis engine timeouts and lock-ups from at least October 2014 when it performed an independent contractor assessment developmental test event and briefed the results to their development contractors. The resource planners experienced the same problems in the Navy's June 2015 Technical Evaluation.

The network analysis process had to be done serially. DOT&E observed that failures often occurred when more than two network analyses were queued in the system. The resource planners perform analyses one at a time for each request and in the order in which requests were received. There is no system mechanism to prioritize high-priority requests or routine requests. The RSSC resource planners must be told the request is high-priority and then manually search the queue (that could contain hundreds of requests) to find the high-priority request and pull it out of queue to service it. System performance will only get worse when there are four RSSCs using the provisioning tool simultaneously – instead of the single RSSC employed during the test – and these RSSCs are analyzing thousands of group networks. For example, based on emerging doctrine at the Army's Cyber Center of Excellence, a Brigade Combat Team (BCT) may have as many as 65 group networks. When the Army completes its reorganization it will have 33 active BCTs resulting in at least 2,200 active group networks.

The MUOS provisioning system is often not available. The MUOS Program Manager has tracked provisioning outages from January to March 2016. The MUOS provisioning capability was down 99,420 minutes over that timeframe, the equivalent of 69 days. Provisioning availability was 55.7 percent in January, 0.0 percent in February, and 7.1 percent in March 2016. Poor provisioning availability has a direct and negative impact on operational effectiveness. If provisioners cannot access the system, then they are incapable of provisioning radios. If they cannot provision radios, then operational units cannot access the system and conduct mission communications.

Terminal Provisioning

Terminal provisioning takes place at the unit locations and is the final step in preparing the terminals to communicate with MUOS. Soldiers in MOT&E-2 were able to provision their terminals successfully 64.2 percent (61 of 95) of attempts, with a 95 percent confident interval between 42.3 and 68.4 percent. When provisioning worked, soldiers took on average 26.4 minutes to complete the provisioning of their terminals. There is no user-defined time requirement levied on MUOS for provisioning. However, the provisioning time requirement of 11 minutes for the HMS Manpack terminal was not met. The testers observed a high number of provisioning failures at Fort Bragg (50.0 percent) and Fort Drum (38.2 percent) compared to Joint Base Lewis McChord (4.8 percent). These failures may have been due to "mobility events" where the terminals lost communications with the CONUS satellite during provisioning and never recovered.

WCDMA Communications

When available, MUOS provided WCDMA voice communications on a limited scale; however, during the majority of the testing there were isolated and widespread communications outages that could result in failed operational missions. MUOS demonstrated that the WCDMA communications provide better voice accuracy and quality than the legacy UHF channels that

MUOS provides as a secondary payload on each satellite.[5] MUOS demonstrated the ability to transfer data between users and with the DISN at up to 64 kilobits per second (kbps).

There is a known problem with fixed assigned networks and the MUOS Program Manager requested COTF avoid testing them, rather than fix the problem prior to MOT&E-2. The Navy generated a PRI-2 problem change record (PCR) on August 21, 2015. A PRI-2 PCR adversely affects the accomplishment of an essential capability. The problem causes the fixed assigned networks to either have poor call quality or experience unexpected termination of the group network. The Navy discovered this problem in the June 2015 Technical Evaluation and recommended that fixed networks not be used. The MUOS C-SSE does not believe this is a viable long-term operational solution. COTF provisioned and tested only immediate assigned networks.[6] DOT&E believes that this is a PRI-1 PCR, which is defined as a problem preventing the accomplishment on an essential capability.

WCDMA versus Legacy UHF Performance

MUOS WCDMA provides better message accuracy and quality of service than legacy UHF. There is no specified user criterion that compares MUOS WCDMA performance to legacy UHF performance. MUOS WCDMA group service performs better in Army company-sized networks (13 participants). DOT&E modeled legacy UHF performance at battalion- (16 participants) and brigade-sized networks (31 participants), and MUOS performed better than the theoretical legacy UHF group networks.

Terrain Types

MUOS WCDMA communications performed as DOT&E expected in clear and urban terrain. Functionally, each group network is comprised of individual links. Thus, as more members are added to groups, the likelihood that all members of a group will receive a transmission grows worse. However, when the transmitter initiates calls from forested terrain, where the MUOS signal is attenuated, the performance improves as the group size grows. DOT&E used Probability of Effective Communications – Voice (PECV) as a performance metric. PECV is the percent of transmissions that all members of the group received correctly. For example, Group PECV in forested terrain for a company command network of 13 participants was 64 percent, while Group PECV in forested terrain for a BCT command network of 31 participants was 74 percent.

This behavior is a cumulative effect of the open loop power control functions in MUOS. In open loop power control, the transmitting terminal sets the output power for initial uplink and downlink transmissions. If the signal is attenuated, then the transmitter increases the power levels for all members in that group and all members benefit, whether or not they are in

[5] DOT&E determined that the UHF payload on MUOS provides better quality communications than a UHF Follow-On (UFO) satellite (*Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation Report,* January 2013).

[6] A fixed assigned network is activated and deactivated at specified times and has priority over immediate assigned networks. Immediate assigned networks can be used when needed, but compete for available resources.

challenging terrain. The Navy increased the open loop power control stress margin just prior to MOT&E-2 to improve call performance. However, increasing the stress margin and boosting the signal consumes additional power and reduces overall capacity. While this had no negative effects for the relatively small number of terminals in the test event, it may have unintended operational effects when MUOS has to service the full communications requirements. The SMDC/ARSTRAT C-SSE has expressed concerns about the performance and planning constraints to future operations.

Network Topology

MUOS is able to support group, P2P, and P2N networks. P2P service is when a single MUOS user communicates with another single MUOS user or data terminal. P2P service is most closely related to a typical phone call. A P2N occurs where a MUOS terminal connects to another network and can talk to a single user or multiple users over that network. DOT&E found no statistically significant performance difference between group, P2P, and P2N communications services that MUOS provides. The user-defined criterion is that MUOS must support broadcast (P2N), P2P, and netted topologies.

Speaker Recognition

The user-defined threshold criterion is that MUOS must support speaker recognition for selected circuits for important users. The Navy implemented this capability through the use of voice encoders that turn analog voice transmissions into binary data. Conversational voice is lower fidelity and uses 2.4 kbps compared to higher fidelity voice recognition that uses 9.6 kbps. DOT&E found that users could not tell the difference between the two different types of voice encoders used by MUOS and the voice encoders did not have a significant effect on mission information. The users rated the voice quality for both encoder types as excellent.

Communications Path

MUOS WCDMA communications can take six different paths through MUOS depending on transmitter and receiver location. DOT&E found no significant statistical difference in performance when MUOS communications are routed through different spot beams on the same satellite, different satellites, or through different RAFs.

Communications-on-the-Move (COTM)

The MUOS and PRC-155 radios demonstrated the ability to provide COTM to users. COTF tested the ability of MUOS to provide COTM by using AN/PRC-155 Manpack in vehicle-on-the-move and soldier-on-the-move configurations. Due to the available vehicle configurations, COTF could only test these radios at speeds limited to 40 miles per hour and below.

Mobility

MUOS does not provide the capability for a transparent transfer of communication services as a user transitions between satellite coverage areas and between satellite beams. Commercial cell phone service handles users moving between cells seamlessly. MUOS does not. MUOS breaks the connection between users when the system determines a transition to a new cell is needed and then reconnects the users. While the mobility event is occurring the user has a complete loss of communications. The mean duration of a mobility event during MOT&E-2 was 78 seconds. The 50th percentile, based on a lognormal parametric best fit of the distribution times, was 64 seconds.

Data Communications

MUOS demonstrated the ability to transfer data between users and with the DISN at data rates up to 64 kbps over the three data transport modes of burst, flow, and streaming. The 854 data transmissions during the test included texting, web accesses, and file transfers. DOT&E assessed data transmission performance based on the successful transmission of a file from one MUOS user to another MUOS user. There is no specified user threshold criterion for data accuracy or quality. Overall, MUOS demonstrated a probability of successful data transmission of 96.0 percent (94.8 – 97.0 percent at the 95.0 percent confidence level. COTF attributed failures bringing data networks into operation as configuration problems. These initiation failures were not used in the evaluation of data transmission accuracy and quality.

Network Management

Network management is a broad range of functions including activities, methods, procedures, and the use of tools to administrate, operate, and reliably maintain computer and communications networks. MUOS is complex and operates differently than legacy UHF. Most, if not all, of the MUOS network managers do not fully understand how the system operates. The system was designed by engineers to be run by engineers. The MUOS network managers are not able to effectively manage the MUOS network.

Fault management is the focus of MUOS network management. The MUOS fault management system is ineffective because it provides the network managers fault alarm events that are cryptic, inconsistently prioritized, and often excessive. The MUOS Program Manager applied filtering of alarm events to triage alarm events. The filtering effort was incomplete and arbitrary. The system filters alarm events as Critical, Major, Intermediate, or Minor, and applies these criteria differently between the FOUO enclave and the Secret enclave. A fault that is critical on one enclave display may be shown as informational on the other enclave display, causing network managers confusion over what actions they should take. Compounding this problem is that alarm events, including critical ones, can display many thousands of times. These problems prevent the network managers from performing their mission and have a profound consequence on effectiveness. Without sound network management, MUOS cannot be a system the operational users can depend upon.

MUOS does not provide a proactive means to monitor WCDMA communication failures, resulting in potentially extended outages for deployed users. The MUOS network managers cannot assess and report on WCDMA satellite beam carrier availability. Key systems associated with WCDMA call services, such as the Radio Base Stations in the RAFs, do not provide fault information to the fault management system.

There were at least four outages during testing that the MUOS NMS was not aware of until the depot contractor submitted trouble tickets. There may have been more outages that were not discovered.

- On October 26, one-half of the capacity of the Pacific satellite and the Wahiawa RAF was unavailable. The outage lasted approximately 2 days, starting the afternoon of October 24 and ending almost 49 hours later on October 26.
- On November 12, RBS #12 at the Wahiawa RAF was out of synchronization, and calls could not be made through cells 259, 379, 307, and 267 on Pacific satellite beams 1, 2, 7, and 16, covering the areas of Japan, Korea, and the Western Pacific.
- On November 18, radios were not able to join groups on CONUS satellite beams 2 (cell 137) and 8 (cell 185) through the Wahiawa RAF.
- On November 18, there was a group service interruption on 25 percent of the Pacific satellite for approximately 15.5 hours.

MUOS has not provided the network managers with a tool to monitor the connections between the different ground sites. Without active monitoring of DISN interconnectivity, the NMS personnel cannot determine if there is latency in the circuits, and degradations can go unchecked. This can lead to longer reaction times when there is a loss of connectivity.

Cryptographic Keying

Using the current processes, the MUOS NMS security personnel will not be able to keep up with the demand for keys given a full operational population of terminals. The MUOS security manager estimates that NMS can transfer 85 pairs of keys a day at current manning levels, taking into account administrative tasks and other responsibilities. The NMS personnel will need to transfer 250 key-pairs a day to meet demand and not result in provisioning delays to the terminal users. The Navy estimates this will be a problem by FY18 given the expected terminal fieldings.

MUOS was able to conduct routine Over-the-Air Rekeys (OTARs) but cannot reliably conduct compromised terminal operations. The reliability problems could result in global communications outages for an entire branch of Service or all Special Operations units. An outage would persist until its root cause is resolved and the MUOS ground system broadcasts a new group cover key (GCK). The MUOS NMS successfully conducted 89.5 percent of all OTAR operations, with a 95 percent confidence interval from 66.7 to 98.7 percent. The MUOS NMS successfully conducted 100 percent (15 of 15) of routine OTARs, with a 95 percent lower confidence bound of 81.7 percent. Half (2 of 4) of the compromised terminal operations succeeded, with a 95 percent confidence interval between 6.7 and 93.3 percent. The wide range of uncertainty is a result of the small sample size. COTF did not conduct additional compromised terminal OTAR operations because failed OTARs led to long outages that were disruptive to the test.

Terminal compromise is an unscheduled, on-demand rekey event to disable a terminal from communicating with MUOS if the terminal is lost, compromised, or captured by threat forces. The unit commander of the terminal can decide to delete the terminal from the MUOS databases. He would direct his communications planner to delete the terminal and user profiles of the compromised MUOS terminal. Once the compromised terminal is deleted from the MUOS databases, it can no longer register with the system to make P2P or group calls. However, if the compromised terminal remains on-air after, it can still receive group call traffic even after its profiles have been deleted from the MUOS databases. Therefore, all other terminals using that GCK must be updated with a new key. The updated GCK is sent via OTAR to all other terminals in the group to eliminate the possibility of a threat listening in on U.S. or coalition forces communications. Although MUOS OTAR will make several attempts to send a new GRK to every affected user, there is a chance that some terminals will not receive the broadcasted rekey. Upon their next registration, those terminals will recognize that their group key is out of order and must use OTAR to obtain the correct key.

Profile Portability

The current MUOS profile and cryptographic key procedures do not allow profile and crypto-key portability and therefore do not support the standard operational concept for tactical radios. All services will be affected to varying degrees by the lack of MUOS profile and crypto-key portability.

The MUOS ground system selects Advanced Encryption Standard (AES) cover and OTAR keys for exclusive use with each individual profile. The system replaces (rekeys) the AES cover key over-the-air to the terminal radio at the end of the one-year expiration period. There is currently no other method of obtaining the replacement cover key. If a terminal operator zeroizes a terminal for any reason (accident, maintenance, CONOPS) after a rekey of the cover key (i.e., after one year), then the user must request a new profile.[7] If the user tries to refill the terminal with the original (or pre-expiration) cover key, then the cover key will fail to authenticate and the ground system will not resend the new cover key. The user must request and receive a new profile, which changes the terminal phone number. Any group networks that terminal participates in would need to be reconfigured and associated terminals updated.

Under such scenarios, the only way to bring a terminal back into operations is to request a new profile. This is a time-consuming process and requires ready access to SIPRNet, which may not be possible in all operational locations. When obtaining a new profile, the user receives a new phone number which is not known to the rest of the force. The Navy should work with the other Services and the National Security Agency (NSA) to develop a materiel solution, policies, and procedures for profile and cryptographic key portability to support the users' CONOPS.

[7] Zeroize: To electronically erase the cryptographic key materiel, thereby destroying it.

Outage Notification

There is no MUOS CONOPS, procedure, or system for the MUOS network managers or satellite controllers to notify the resource planners, satellite operational manager, satellite system expert, provisioners, and deployed users of outages or system degradations and their operational effects.

Cybersecurity

The system is not secure from cyberattacks. The COTF Adversarial Assessment team and USSTRATCOM conducted independent cyber assessments and obtained similar results. They discovered over 1,000 cybersecurity vulnerabilities in the MUOS ground system. Approximately half of these vulnerabilities are Category-II (CAT-II) and above. CAT-II vulnerabilities have the potential to result in loss of confidentiality, availability, or integrity. The details of the COTF Adversarial Assessment may be found in the classified annex to this report.

Operational Suitability

MUOS is not operationally suitable. The ground system lacks the stability and maturity to sustain global operations. The MUOS does not provide communications that deployed users can rely on when the system is in widespread use or at full capacity. MUOS performed poorly in almost every area of operational suitability.

The NMS is the nerve center of MUOS, managing the ground system and WCDMA operations. During most of the test it was not operationally available. NMS had long repair times, numerous high-priority problem reports, poor usability, poor documentation, and high reliance on depot maintainers. Additionally, NMS is under-manned and operators do not consider themselves adequately trained to perform their mission. Multiple failures in the NMS and the Ground Transport Segment (GTS) during MOT&E-2 created long communications outages. Deficiencies with the communication planning system and cryptographic key management system will prevent planners and network managers from provisioning and maintaining communications for a large user population.

MUOS does not meet the user-defined threshold operational availability. NMS was available 6.3 percent of the time against a 95.0 percent threshold criterion. The GTS was available 87 percent of the time against a 99 percent threshold requirement. There were large, contiguous blocks of time during which a subset of MUOS users/operators would have experienced an outage. There was no time after hour 36 of the month-long test that the NMS did not experience an operational mission failure. The ground system availability problems were known to the MUOS Program Manager at least as early as the Technical Evaluation in June 2015. While the program never published availability metrics outside of the Program Office, the Technical Evaluation report states that, “Collective observations of system downtime resulted in Ground Segment availability for GTS and NMS not met.” MUOS has no user-specified reliability requirements. The NMS had a Mean Time Between Operational Mission Failure (MTBOMF) of 46 hours, with a 95 percent confidence interval between 21 and 103 hours.

MUOS does not meet threshold requirements for segment mean repair times. The MUOS threshold segment repair time is 45 minutes (0.75 hours). MUOS demonstrated repair times in terms of hours, even with depot maintainers on-site, in violation of their published logistic support plans. The median repair time for the NMS based on 37 repair actions was 89 hours. The NMS mean repair time was 1,058 hours. DOT&E believes a median repair time is a better statistical estimate for skewed distributions. The median repair time for the GTS was 185 hours, Satellite Control Segment (SCS) was 100 hours, and Ground Infrastructure Segment (GIS) was 114 hours.

Long repair times are driven in part by the MUOS organizational-level personnel having a high dependency on depot support to maintain operations. The Navy's User's Logistics Support Summary for MUOS, dated June 2015, specifies a two-tiered maintenance approach: The Naval Computer and Telecommunications Area Master Station – Pacific performs organizational maintenance; a contractor depot performs depot maintenance for complex repair of defective items. The MUOS Program Manager deployed contractor depot maintainers on-site during the test to minimize depot maintainer reaction time and in recognition of the complex system's lack of stability. The MUOS operators generated 128 unique trouble tickets, when duplicate trouble tickets were removed; 73 percent requested depot support. The depot maintainers provided on-site assistance at the Wahiawa site 90 times during the 20 test days.

Preventive maintenance procedures on key NMS servers and databases were not being performed and the servers and databases were nearly at full capacity. The organizational system administrators were not authorized to perform these routine actions. The procedures were in the organization technical manuals but the depot maintainers removed the procedures in the latest update. The quantity and magnitude of the maintainability problems will escalate as MUOS is required to service the expected large operational radio population.

Ground system problem change requests (PCRs) remained uncorrected for long periods and seldom contained operational effect statements. PCR submitters sometimes incorrectly prioritized severity levels because they did not view the system operationally. At the end of MOT&E-2 there were over 900 ground system software PCRs open, with 242 categorized as PRI-2. A PRI-2 PCR, by definition, adversely affects the accomplishment of an essential capability and there is no known work-around solution. Remarkably, the Navy believes only 35 of 242 of the PRI-2 PCRs have an operational impact. The PCR operational impact assessments are not based on what would be required of MUOS as a fully operational system. The "operational impact" section of high-priority PCRs is often not completed or left completely blank. The assessment of operational impact by the PCR submitter is often based on current WCDMA usage that is sparse and sporadic based on test events and demonstrations. DOT&E believes that some of these PCRs should be classified as PRI-1 PCRs. For example, there are PCRs that resulted in one-half of coverage and capacity on two satellites being lost, and these were classified as PRI-2.

DOT&E performed an independent assessment of the 242 open PRI-2 PCRs and assesses that at least 151 of them will negatively affect MUOS operations. The MUOS Program Manager lacks an executable plan to resolve known problems. DOT&E calculated the mean age of the open PRI-2 PCRs as 526 days. Of the set provided to DOT&E, the oldest is 1,307 days old and the newest is 39 days old. Trouble tickets were generated at least as fast as the MUOS Program Manager could close them. Some percentage of the trouble tickets will be converted to PCRs. As of February 29, 2016, there were 550 open trouble tickets. As of March 30, 2016, there were 576 open trouble tickets.

MUOS help desk personnel were unfamiliar with MUOS. The Navy gave MUOS help desk support responsibilities to the Space and Naval Warfare Systems Command (SPAWAR) consolidated Help Desk in August 2015. The recent addition of help desk support meant that the help desk personnel were not familiar with MUOS at the time of MOT&E-2. They failed to recognize the importance of problems, inappropriately prioritized problems, and even assigned the problems to the wrong system.

MUOS operational components (NMS, SCS, Planning and Provisioning) currently act as separate enclaves with little interaction between the different user groups. The Navy has not created a system or process to notify all users of MUOS service outages. If there are outages in the system, then the NMS, NAVSOC, or RSSC-West personnel submit trouble tickets. However, users are not notified that they will experience outages. Further, no notification is given to the C-SSE as a cue to determine the operational effects and execute operational alternatives to mitigate the problems.

The SCS controllers indicated general satisfaction with the classroom training but 80 percent disagreed that the training prepared them for the tasks they need to perform. 100 percent (5 of 5) of the satellite controllers disagreed that the training simulator was relevant to the tasks they need to perform, specifically complaining that it lacked an Orbit Analysis System capability. Most satellite controllers indicated on-the-job training (OJT) was unsatisfactory and not well organized. 100 percent (10 of 10) of NMS personnel were dissatisfied with classroom training and 70 percent (7 of 10) of the respondents disagreed or strongly disagreed that the training prepared them for their assigned duties. The planners and provisioners indicated satisfaction with the classroom training but said it was difficult to understand. Satellite controllers, network managers, and planners and provisioners all complained the training taught them how to push buttons but not the reasons why they were pushing the buttons or how the system worked. The Navy did not provide the planners and provisioners with the OJT and web-based sustainment training that are required by the MUOS Lifecycle Support Plan.

The system documentation is immature, missing information, and cannot be accessed by all the personnel who need to access it. The documentation is inaccurate, incomplete, and does not work on DOD standard internet browser configurations. During MOT&E-2, 38 percent (55 of 146) of trouble tickets submitted by the network managers, satellite controllers, and communications planners included problems with documentation support. Network managers, satellite controllers, and planners all expressed dissatisfaction with the documentation. There is no transition plan in place to prepare the SMDC/ARSTRAT personnel to assume C-SSE responsibilities.

The majority (71 percent) of NMS personnel were dissatisfied with the usability of the system. The network managers did not believe the system supported their ability to monitor the system (7 of 11); thought system alerts were not adequate to initiate action (8 of 11); thought displayed information was useful (7 of 11); and thought automated action facilitated ease of operations (9 of 11). The network managers thought the failure notification system was too cryptic to be useful and they had no way to monitor the status of WCDMA communications. In responses to survey questions, 57 percent (12 of 21) of the planners and provisioners indicated they were dissatisfied with the usability of the MUOS PlanProvApp and the Situational Awareness application and reports.

There is no electronic interface between the USSTRATCOM's Joint Integrated Satellite Communications Tool (JIST) and MUOS. Planners must manually cut and paste information in satellite access requests (SARs), field-by-field, from JIST into MUOS and from MUOS back into JIST to create satellite access authorizations (SAAs). The Navy should develop the capability to electronically import JIST SAR data into the MUOS PlanProvApp and auto-populate the SAR fields.

When conducting network analysis the system returns with a "Likelihood of Success" of low, medium, or high for the planned network. The MUOS PlanProvApp does not provide any indications to the operator of what is considered when determining the network Likelihood of Success, or how the planner could improve the outcome in the event of a low Likelihood of Success. The Interactive Electronic Technical Manual (IETM) does not provide any amplifying information. There are also known differences between how MUOS is configured and how the planning application models MUOS to determine the likelihood of success. These differences can result in group networks provisioned in satellite beans they cannot actually use.

The network analysis Likelihood of Success and provisioning audit status appear contradictory at times and there is no documentation or explanation of how each status is determined. When the system provisions a group network, it provides an analysis on the Likelihood of Success and an audit status in different windows within the application. The analysis engine may render a "High Likelihood of Success," but the audit status may show that the "Provision Failed." This seems contradictory to the planners and provisioners and there is no automated guidance or information in the IETM. Network analysis and system audits have no indications of progress or even if the system is still working. The planners have to either assume the system is working and continue to wait, or assume that the system is not working and cancel the process and restart. This contributes to inefficient processing of group SARs. The Navy should provide the planners and provisioners a progress indicator so they can tell whether the plan is working or failed.

Network audits are presented to the planner from the oldest on top to the most recent in reverse order of how it should be presented. This forces the planner to scroll through hundreds to thousands of audit statuses to view the most recent audit. The Navy should order the audit status in the PlanProvApp from newest to oldest instead of oldest to newest as it is currently is.

Recommendations

The Navy and USSTRATCOM should take the following actions to make MUOS operationally effective and operationally suitable. COTF should verify the corrections in the FOT&E, planned for FY18.

Operational Effectiveness

The Navy should:

- Restore funding to sustain the MUOS Performance Model so the government can perform independent performance and capacity trades.
- Train the C-SSE and transfer the responsibility for beam carrier management per the established MUOS documentation.
- Fix the problem with MUOS being unable to process SARs with multiple group networks.
- Perform root cause analysis and fix the problem with preventing fixed assigned group networks.
- Perform root cause analysis and correct the problems with the Global System View.
- Perform root cause analysis and correct the problems with latent and inaccurate Call Detail Records.
- Fix the problems with inaccurate, incomplete, missing situational awareness and performance webpage views, reports, and graphs.
- Work with the Defense Information Systems Agency to implement a GDS for the MUOS FOUO and Top Secret enclaves to resolve IP addresses and enable dynamic IP addressing.
- Modify the MUOS PlanProvApp so the provisioner can load a series of IP addresses and the system assigns the IP addresses in the sequence loaded. The Navy should also update system documentation and training appropriately.
- Fix the erroneous IP address allocation outside IP subnets to avoid deployed user failed communications.
- Work with the Defense Information Systems Agency to implement a SIPRNet and NIPRNet DNS capability for MUOS.
- Implement a DHCP capability is the MUOS waveform to enable dynamic IP assignments for connected devices, and provide network access controls to prevent unauthorized access to the MUOS network .
- Perform root cause analysis and correct the underlying problems causing the routine analysis engine failures.
- Conduct loading testing and analysis to determine analysis engine performance based on the Capabilities Production Document's Communication Service Requirements

and on multiple RSSCs analyzing networks simultaneously. Resolve any discovered performance constraints.

- Provide the resource planners an automated means to prioritize network provisioning to plan high-priority networks before lower-priority networks.
- Jointly develop with USSTRATCOM, a MUOS outage notification tool to notify the C-SSE, provisioners, and deployed users of system degradations, outages, carrier frequency problems, and their potential operational effects.
- Explore and implement a plan for the other Services' terminal offices to reduce the overall terminal provisioning time and to increase terminal provisioning success rates.
- Further investigate the differences in terminal provisioning performances observed during MOT&E-2 – including terminals provisioning with a single-satellite field of view and terminals provisioning in a two-satellite field of view – and correct any identified problems.
- Model, in coordination with USSTRATCOM, the power control parameter effects on call performance and system capacity when MUOS is at the full communications service requirement.
- Make the MUOS default setting for provisioning voice communications as conversational voice (2.4 kbps) instead of the current default of voice recognition (9.6 kbps), to conserve satellite resources.
- Explore and implement system improvements so users can transition between satellites and beams seamlessly rather than have communication outages.
- Improve network management alert filtering at the NMS to make the alerts descriptive, relevant, timely, and actionable.
- Filter and prioritize alert event notifications consistently across the FOUO and Secret network management enclaves.
- Develop and provide the NMS a tool to directly and actively monitor DISN interconnections between MUOS sites without operator intervention.
- Develop a technical solution and procedures to perform bulk loading of MUOS AES keys into the MUOS Key Management System. If a technical solution cannot be developed, then the Navy should review staffing levels and adjust them appropriately to ensure military operations are not impaired due to delays in loading sufficient numbers of operational keys.
- Fix the reliability problems with rekey operations that can result in communications outages on wide-raging scales.
- Develop the capability to abort rekeys when it is clear a rekey event will result in communication outages.

- Investigate and implement a means to disable a compromised terminal without requiring a rekey of all other networked terminals.
- Work with the other Services and the National Security Agency to develop a materiel solution, policies, and procedures for profile and cryptographic key portability to support users' CONOPS.
- Fix the known problems with how MUOS determines a group network Likelihood of Success that can result in provisioning networks that will fail.
- Fix or mitigate the cybersecurity problems (see recommendations in the classified annex to this report).

USSTRATCOM should:

- Jointly develop with the Navy, a MUOS outage notification tool to notify the C-SSE, provisioners, and deployed users of system degradations, outages, carrier frequency problems, and their potential operational effects
- Review the automated calling performed by the depot contractor and determine if this is a viable operational solution when MUOS enters into full operations.
- Reconsider their emerging group cover key concept, considering the potential for catastrophic outages for failed rekey events.

Suitability

The Navy should:

- Update the IETM to ensure there is consistency between the NMS-displayed fault severity and the fault severity contained in the IETM. The Navy should update the IETM to include all alert events, including the methods to correct the faults and their potential operational effects.
- Review the allocation of required maintenance actions and allocate maintenance actions to the lowest possible level.
- Update SCS, and NMS maintainer documentation to correct inaccuracies – to include missing troubleshooting procedures – and provide added detail for in-depth understanding of the purpose behind the procedures.
- Reassess problem change request (PCR) priorities with the user community in light of true operational effects and prioritize and correct the problems accordingly.
- Develop and adequately fund an executable plan to resolve the large number of high-priority PCRs and trouble tickets before the next operational test.
- Determine the root causes of contractor staffing turnover and modify policies as necessary.
- Retrain the MUOS operators, developing contractors, users, and help desk personnel on how to initially prioritize problems.

- Provide additional training to the SPAWAR help desk personnel on how to handle and assign MUOS help desk calls.
- Perform a configuration audit to determine what systems are in debug mode and bring debug operations under configuration control.
- Improve the SCS simulator, including adding Orbit Analysis Subsystem capability, to make the test and training simulator relevant and effective in training satellite controllers to perform their assigned duties.
- Update the satellite control IETM to include adequate satellite control warnings and cautionary notes and to include comprehensive fault isolation procedures.
- Create a comprehensive list of the failures, faults, and alarms seen at all ground segment sites. Update the IETMs with descriptions of the alarms, the operational effect of the failures, and procedures for operators and maintainers to follow.
- Update the technical manuals to provide a theory of operation, what the selectable range of each value is, and explanations for why an operation manager, provisioner, or network manager would select one value over another.
- Work with the MUOS network managers to provide them with the information they need to fully understand faults and alarms given by the system.
- Update the PlanProvApp to provide feedback to planners as to why the system renders a network failing provisioning audit and what steps they should take to rectify the failure.
- Provide the planners and provisioners a progress indicator so they can tell whether the plan is working or failed.
- Reorder the audit status in the PlanProvApp from newest to oldest instead of oldest to newest as it is currently is.
- Provide an automated means, or update the IETM, to provide RSSC planners guidance on how the group network Likelihood of Success is determined and what planning steps they can take to improve a network outcome.
- Update the PlanProvApp to provide voice communications type (recognition, conversational) and authorized data rate (2.4, 9.6, 32, 64 kbps) based on type of access authorized in the satellite access authorizations (SAA) report.
- Fix the problem with “zombie networks” that cannot be deleted and consume capability.
- Fix the problems with MUOS situational awareness inaccuracies, failed renderings, and missing information.
- Fix the problems with the slow and unresponsive Situational Awareness screens, outdated information of the screens, and the inability to perform auto-refreshes.

- Fix the problems with downloading situational awareness and performance reports to Microsoft Excel, including but not limited to missing column headings, system time-outs, page errors, and “no items found” errors.
- Add operationally relevant information such as data rates, services, min/max power, type of access to the Situational Awareness screens and reports.
- Improve the training and provide SCS, NMS, RSSC, and SMDC/ARSTRAT personnel additional training with an emphasis on in-depth understanding of the purpose behind the actions rather than simply “pushing buttons.”
- Provide the planning and provisioning OJT and web-based sustainment training as required by the MUOS Lifecycle Support Plan.
- Provide IETMs that work in DOD standard internet browser environments.

USSTRATCOM should:

- Develop the capability in the Joint Integrated Satellite Communications Tool (JIST) to electronically import MUOS PlanProvApp SAA output data into JIST and auto-populate the SAA fields.

J. M.

J. Michael Gilmore
Director

Contents

This page intentionally left blank.

Section One
System Overview

This document reports on the evaluation of the Mobile User Objective System's (MUOS) operational effectiveness, suitability, and cybersecurity. This evaluation is based primarily on data collected during the second Multi-Service Operational Test and Evaluation (MOT&E-2), conducted from October 19 to November 20, 2015, and a cybersecurity Adversarial Assessment, conducted from April 4 – 8, 2016. The Naval Command Operational Test and Evaluation Force (COTF) and supporting Service Operational Test Agencies conducted the operational test. Data included satellite control digital log files, Network Management Segment (NMS) automated logs, manually recorded logs, user surveys, and DOT&E staff observations of testing at the satellite control center, the NMS and Wahiawa Radio Access Facility, and Army ground sites. COTF collected sufficient data to evaluate the operational effectiveness, suitability, and cybersecurity of MUOS.

The Navy is planning a follow-on test and evaluation (FOT&E) in fiscal year 2018 (FY18) to verify corrective actions and re-evaluate the operational effectiveness, suitability, cybersecurity, and mission capability of MUOS. MUOS converts commercial third-generation (3G) Spectrum Adaptive (SA)-Wideband Code Division Multiple Access (WCDMA) commercial cellular phone system technology to a military ultra high frequency (UHF) satellite communications (SATCOM) radio system using geosynchronous satellites in place of cell towers.

Mission Description

The MUOS mission is to provide narrowband satellite communications support for a wide range of Department of Defense (DOD) and government operations, especially those involving mobile users.[8] MUOS is designed to support ad-hoc communications between single users via point-to-point (P2P) networks, allow groups of users to participate in pre-planned networks, and give both individuals and groups access to services on connected networks, such as the Secret Internet Protocol Router Network (SIPRNet), as well as enable them to reach outside telephone systems.

The DOD intends for MUOS to provide users with priority-based access to a broad range of P2P, point-to-network (P2N), and group communication services supporting voice, data, and mixed voice and data. Group services provide netted communications to two or more users and are preplanned. Users may quickly activate P2P, P2N, and pre-defined group services on demand in the field and then release them, freeing resources for other users. The program manager plans for MUOS to provide assured access to designated high-priority communication services, with the ability to preempt lower-priority services when necessary. MUOS is not required to be functional in a nuclear scintillation environment or against a radio frequency jamming attack.

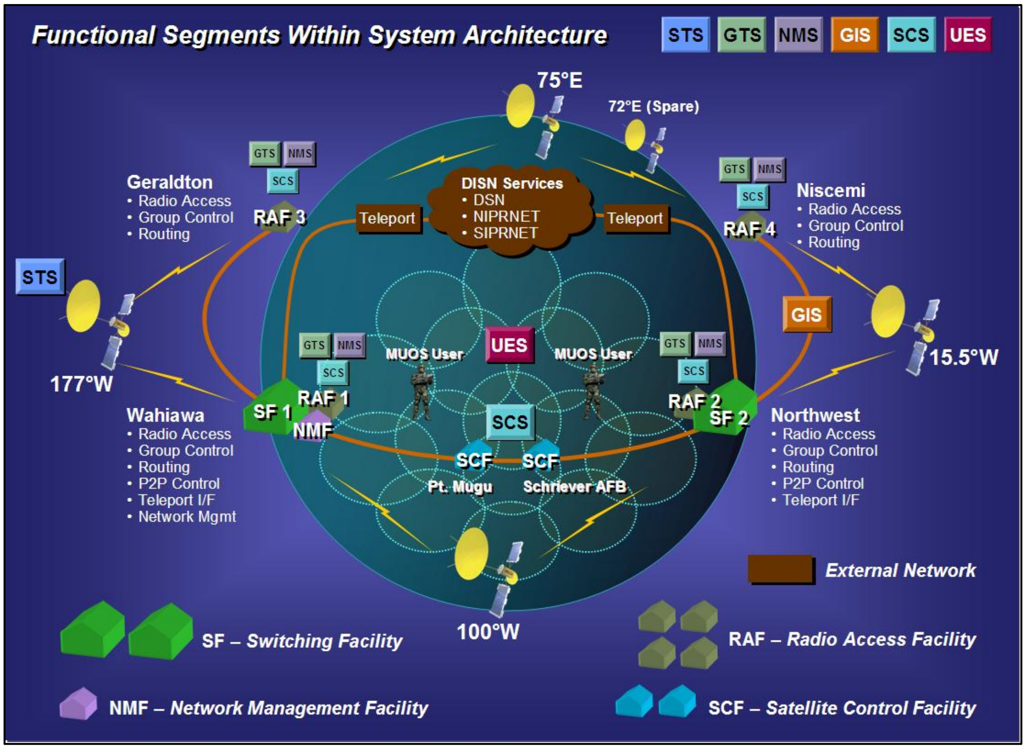
[8] Narrowband is typically defined as 64 kilobits per second or less.

MUOS converts a commercial 3G SA-WCDMA cellular phone system to a military UHF SATCOM radio system using geosynchronous satellites in place of cell towers. Each MUOS satellite also carries a legacy payload similar to that deployed on the UHF Follow-On (UFO) satellite system. The DOD intends for MUOS legacy payloads to extend the useful life of legacy systems past the original UFO constellation's planned phase-out. The WCDMA waveform cannot directly interoperate with the legacy UHF waveform. The DOD Teleport program is intended to provide interoperability between both the WCDMA waveform and UHF legacy terminals. MUOS WCDMA users will connect to Defense Information System Network (DISN) services via the Teleport interface.

MUOS provides the information transport segment, via satellites and ground infrastructure, for narrowband communications. However, MUOS does not provide an inherent end-to-end communications capability. End-to-end communications capability will only be delivered to the deployed user through the fielding and employment of MUOS, DOD Information Network (DODIN) interfaces (e.g., Teleport), and user terminals.

System Description

MUOS is the DOD's next-generation narrowband military SATCOM system, replacing the UFO constellation that is reaching end-of-life. It is a satellite-based communications network designed to provide worldwide, narrowband, beyond line-of-sight, P2P, and netted communication services to multi-Service organizations of fixed and mobile terminal users. MUOS is designed to provide 10 times the throughput capacity of current narrowband SATCOM. The Navy designed MUOS to provide increased levels of system availability over the current constellation of UFO satellites, as well as improved availability for small, disadvantaged terminals that is typical for a current mobile user over UFO. Figure 1-1 depicts the six segments composing MUOS: space transport, ground transport, network management, ground infrastructure, satellite control, and user entry segments.



STS – Space Transport Segment; GTS – Ground Transport Segment; NMS – Network Management Segment; GIS – Ground Infrastructure Segment; SCS – Satellite Control Segment; UES – User Entry Segment; NIPRNet – Non-classified Internet Protocol Router Network; SIPRNet – Secret Internet Protocol Router Network; DISN – Defense Information Systems Network

Figure 1-1. MUOS Operational View

The Space Transport Segment is intended to consist of four operational satellites and one on-orbit spare. Each satellite hosts two payloads: a legacy communications payload that mimics the capabilities of a single UFO satellite, and a MUOS WCDMA communications payload. The satellite constellation is designed to provide coverage between 65 degrees North and 65 degrees South latitudes and provide dual coverage to more than 65 percent of the service area.

The Ground Transport Segment (GTS) is planned to consist of four radio access facilities (RAFs) and two switching facilities (SFs) to manage MUOS communication services, including the allocation of radio resources and user authentication, routing, switching, and mobility management. The program manager intends for the GTS to provide an interface into the DOD Teleport system to access DISN services including the Defense Switch Network, Non-classified Internet Protocol Router Network (NIPRNET), and SIPRNET.

The NMS consists of one Network Management Facility (NMF) that hosts equipment to conduct network management functions, support communications planning, and determine the location of UHF narrowband interferers. The NMF is collocated with an SF and RAF at Wahiawa, Hawaii.

The Ground Infrastructure Segment (GIS) provides terrestrial mesh connectivity between ground facilities, including the Satellite Control Segment (SCS), the NMF, and RAFs. The GIS relies on existing DISN infrastructure.

The SCS consists of a primary MUOS Telemetry, Tracking, and Commanding (TT&C) facility at Naval Satellite Operations Center Headquarters at Point Mugu, California, and a backup facility at Detachment Delta at Schriever Air Force Base (AFB), Colorado. The SCS consists of two main subsystems: the Satellite Control Subsystem and the Orbital Analysis System (OAS). The control subsystem commands and controls the functions for maintaining the satellites on-orbit and receives telemetry from the satellites to monitor the health of the satellites. The control subsystem also controls the UHF communications payload on the satellites.

The User Entry Segment provides the software interface between the MUOS terminals and MUOS. This includes the protocols, formats, and physical layer characteristics for MUOS-compatible communication services. The Services are responsible for developing and fielding MUOS-compatible terminals. The Handheld, Manpack, Small-Form Fit (HMS) Manpack radio (AN/PRC-155) is currently the only production representative terminal available and participated in MOT&E-2.

Concept of Employment

The MUOS architecture mimics Universal Mobile Telecommunications System (UMTS) 3G cellular telephone infrastructure to provide a broad range of full-duplex P2P voice and data communication services, and a very efficient internet protocol (IP) data transport capability. Because the warfighter uses predominantly netted communications, MUOS has added group services to provide half-duplex netted communications to groups of two or more users. The operational provisioning authority must first provision a user before they can register their terminal and communicate over MUOS.

Satellite Beams & Satellite Beam Carriers

A MUOS satellite footprint consists of 16 beams. Figure 1-2 shows the footprint for the Pacific (PAC) Satellite (MUOS-1) in red and the footprint for the Continental United States (CONUS) satellite (MUOS-2) in blue. There are 4 beam-carriers operating on different frequencies within each of the 16 satellite beams for a total of 64 satellite beam carriers (SBCs), also referred to as cells, per satellite. Each SBC contains 5 megahertz (MHz) of potentially available UHF spectrum for users to communicate over.

Each MUOS satellite is within field of view of at least two RAFs. The 64 SBCs are transported across each satellite with half originating and terminating at each supporting RAF. For example, 32 of the CONUS satellite SBCs terminate in the Northwest, Virginia, RAF and the 32 terminate in the Wahiawa, Hawaii, RAF. During provisioning, users are designated which SBCs they are authorized to transmit and receive in. Flexibility is built into the system to anticipate a user operating outside their assigned SBCs. When a MUOS user roams into a non-provisioned satellite beam carrier (outside of its provisioned plan, such as a different satellite, a different beam, or a different beam carrier), then it is normally out of service for that group. However, during provisioning, the resource planner can authorize an “AddMe” function that will provide service in a region the user may travel to, such as on a deployment. While this adds flexibility, it consumes satellite capacity resources. Therefore, the resource planner has to trade the flexibility benefits with capacity costs.

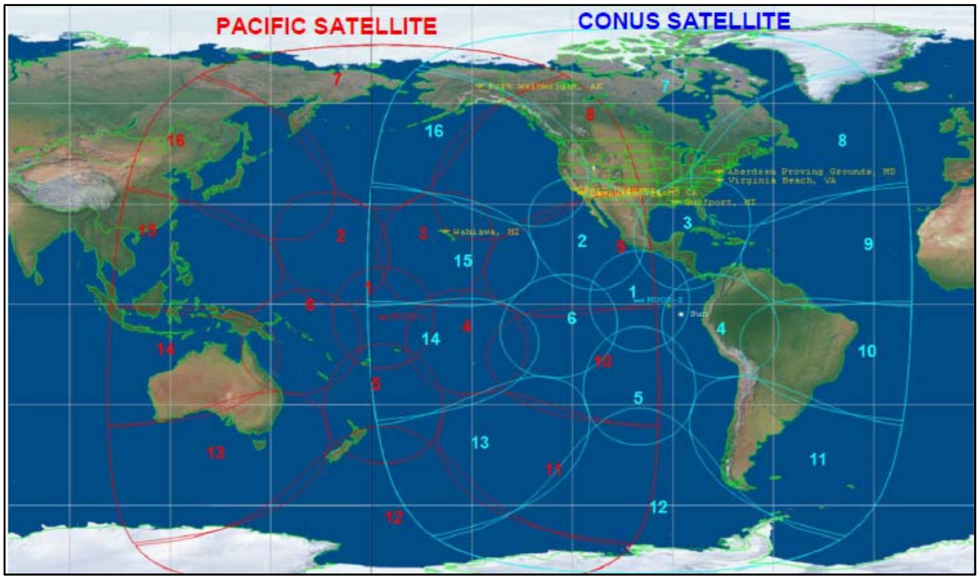


Figure 1-2. Pacific and Continental United States (CONUS) Satellite Beam Footprint

WCDMA Planning

The Navy defines MUOS WCDMA planning as beam carrier management, Satellite Authorization Request (SAR) management, and situational awareness.

- Beam carrier management is planned to provide the ability to create a beam management region and configure satellite beams and carriers for each MUOS satellite and analyze those configurations for viability. Per the MUOS technical manuals, this capability is intended to facilitate the determination of frequency availability using the defined regions, in conjunction with factors such as traffic profiles, apportionment adjustments, past capacity performance, and the current system configuration. Beam carrier management will be exercised by the U.S. Strategic Command (USSTRATCOM) Consolidated SATCOM System Expert (C-SSE).

- SAR management supports group network provisioning and allows networks to be scheduled in advance of their anticipated usage. SAR management provides the capability to create, review, and delete SARs when they are no longer needed. SAR management is discussed further below as the first step in the group provisioning process.

- Situational awareness is an important and shared responsibility across MUOS: The satellite controllers in Point Mugu, California, maintain situational awareness of the MUOS satellite constellation; the MUOS network managers maintain awareness of the ground system components; and the MUOS C-SSE and Regional SATCOM Support Center (RSSC) – West resource planners focus on end-user communications and resource utilization. Situational awareness and performance reports are provided via the MUOS Planning and Provisioning Application (PlanProvApp) to the MUOS network managers at Wahiawa, Hawaii, and to the C-SSE and the RSSC resource planners. This situational awareness portal is available via SIPRNET. Generally, status is indicated by “red yellow green” indicators. Users may access lower hierarchical level information through a "drill-down" capability if more detail is required. Resource utilization data are derived from comparing planned resource usage against actual call metrics for the group services and beam-carriers of interest.

- The PlanProvApp situational awareness and performance information is the only point of access into MUOS for the Satellite Operational Manager (SOM), C-SSE, and RSSC resource planners. This web portal is designed to provide them with a shared understanding of the system state and thus provide decision makers with tools to effectively make operational decisions. The situational awareness application provides informational views of MUOS meant to facilitate the overall understanding of MUOS mission performance to support the deployed users.
- Situational awareness creates informational views of the entire system, consisting of fault information and system status, performance, resource usage, and plan execution views. These views are geared towards informing the planning and provisioning operators about actual and potential problems. The SOM, C-SSE, and resource planners will use the situational awareness tool to monitor how performance problems, system outages, configuration changes, and other issues affect current plan execution.
- The MUOS situational awareness portal is meant to display plan execution views that contrast planned resource utilization against actual resource utilization. If discrepancies between planned and actual resource utilization are noticed, then the operator can look at the situational awareness global system view to see if there are any malfunctioning components. The operator is intended to have the capability to drill down to the satellite and beam where the discrepancy was observed – using the available status, performance, plan execution, and call usage views – and attempt to identify the issue and the plans affected by the issue.

Terminal Provisioning

The MUOS WCDMA terminal users gain access to MUOS using a new provisioning process. The provisioning process places essential configuration data into appropriate MUOS ground system databases and into MUOS terminals to enable WCDMA communications. Provisioning is comprised of two complementary processes to set up the MUOS terminal for communications through MUOS, consisting of terminal provisioning and group provisioning.

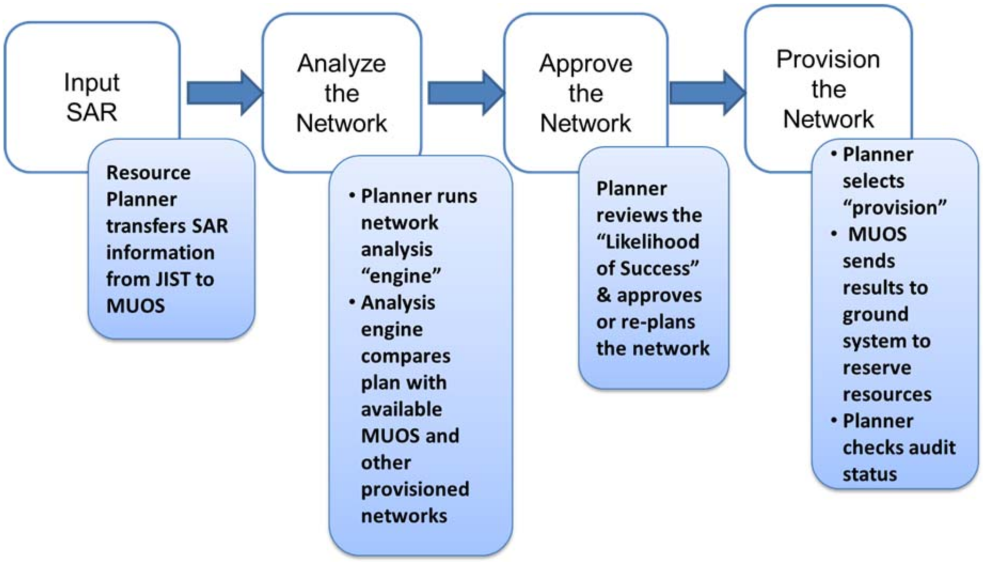
Terminal provisioning is the process of initially configuring the MUOS terminals and communications services enabling P2P communications. During initial provisioning, seed data are associated with an individual MUOS terminal. The seed data consist of the International Mobile Subscriber Identifier (IMSI), Mobile Station Integrated Services Digital Network (MSISDN), Advanced Encryption Standard (AES) cover key and over-the-air rekey (OTAR) tags.[9]

[9] An IMSI is a unique 15-digit number, associated with Global System for Mobile Communications and Universal Mobile Telecommunications System network mobile phone users. An MSISDN is a 10-digit mobile subscriber telephone number. A key tag is an AES key short title that uniquely identifies the key.

Unit planners submit requests through the USSTRATCOM web-enabled tool – the Joint SATCOM Mission Planning System (JSMPS) – to the operational provisioning authority at Army Space and Missile Defense Command/Army Strategic Forces Command (SMDC/ARSTRAT). The operational provisioning authority enters the information into the MUOS PlanProvApp. The provisioner then sends seed data back to the unit, where the unit planners combine the seed data with the group provisioning information using the Joint Enterprise Network Manager and load the information into the MUOS terminal.

Group Network Provisioning

The second provision stage is group provisioning. Group provisioning follows a process similar to terminal provisioning and results in group network services configured in the MUOS ground system and MUOS terminals to enable netted communications. The unit planner identifies which terminals need to participate in specific netted communication groups and submits a SAR to the RSSC using a USSTRATCOM web-enabled tool called the Joint Integrated SATCOM Tool (JIST).


Input SAR
Resource Planner transfers SAR information from JIST to MUOS
Analyze the Network
• Planner runs network analysis "engine"
• Analysis engine compares plan with available MUOS and other provisioned networks
Approve the Network
Planner reviews the "Likelihood of Success" & approves or re-plans the network
Provision the Network
• Planner selects "provision"
• MUOS sends results to ground system to reserve resources
• Planner checks audit status

SAR – Satellite Authorization Request; JIST – Joint Integrated Satellite Communications Tool; MUOS – Mobile User Objective System

Figure 1-3. Group Network Creation Process

Figure 1-3 illustrates the group network creation process. The RSSC resource planner transfers the group SAR information from JIST to the MUOS PlanProvApp and runs a network analysis. If the network is successful, the RSSC personnel approve the planned group network and provision it in the MUOS ground system. The provisioner transfers the group network results back to JIST and sends the Satellite Access Authorization (SAA) electronically back to the unit planner, who combines the group and terminal provisioning information using the Joint Enterprise Network Manager (JENM) and manually transfers the file into the MUOS terminal. Upon terminal power-on and login, the terminal registers with the network and downloads the remainder of the MUOS operational profile through over-the- air – file transfer (OTA-FT) provisioning.

Key Management

The loading of cryptographic keys is an orchestrated process between the MUOS ground system and the MUOS terminal.[10] During terminal provisioning, the SMDC/ARSTRAT Operational Provisioning Authority (OPA) at Peterson AFB, Colorado, assigns an unused cryptographic key-pair to each terminal via the seed profile. As discussed above, the OPA populates two AES key tags in the terminal seed profile. The key tags identify the unique keys for the MUOS terminal to download upon registration with MUOS. The Naval Computer and Telecommunications Area Master Station – Pacific (NCTAMS-PAC) communication security (COMSEC) custodian generates the AES cover key and OTAR keys using the Electronic Key Management System (EKMS) key processor and delivers the key pairs to the MUOS security manager at the NMS in Wahiawa, Hawaii. The NMS security manager manually loads the terminal cover and OTAR key pairs into the MUOS Key Management System using a simple key loader (SKL).

Likewise, there is a group cover key (GCK) that the OPA assigns during the provisioning process. The GCK provides protection of signaling of group services and supports the separation of different security enclaves. There are only eight possible GCKs available in the system. The concept of operations for GCKs is still being developed by SMDC/ARSTRAT. The current concept is that the Army, Navy, Air Force, Marine Corps, Special Operations, and Coast Guard will each have a unique GCK.

The unit planners receive the terminal seed profile and group network SAA from the OPA and RSSC via JSMPS and JIST, respectively. When the unit planners enter the terminal information into MUOS to create the initial terminal profile, MUOS assigns a key short title to the terminal profile. When the terminal provisioner loads the MUOS terminal using the terminal profiles, the associated key tags are transferred to the MUOS terminal. Upon boot-up and registration, MUOS downloads via OTA-FT the correct keying material to update the terminal. The unit planner transfers the key tags to the MUOS terminal using JENM. When the user powers on the terminal it logins and registers with the MUOS network. At that point, MUOS downloads the user cover key, OTAR key, and GCK to the terminal through OTA-FT provisioning. The user cover key and OTAR key are updated annually via OTA-FT. The GCK is updated weekly via OTA-FT or when needed during a terminal compromise. Users need additional High Assurance Internet Protocol Encryptor (HAIPE) and Secure Communications Internet Protocol (SCIP) cryptographic keys for netted communications, and communicating with the DISN.

Terminal compromise is an unscheduled, on-demand rekey event to disable a terminal from communicating with MUOS if the terminal is lost, compromised, or captured by threat forces. The unit commander of the terminal can decide to delete the terminal from the MUOS databases. He would direct his communications planner to delete the terminal and user profiles of the compromised MUOS terminal. Once the compromised terminal is deleted from the

[10] The term “ground system” refers to both the MUOS Ground Transport Segment (RAFs, SFs) and the MUOS Network Management Segment (NMS).

MUOS databases, it can no longer register with the system to make P2P or group calls. However, if the compromised terminal remains on-air after, it can still receive group call traffic even after its profiles have been deleted from the MUOS databases. Therefore, all other terminals using that GCK must be updated with a new key. The updated GCK is sent via OTAR to all other terminals in the group to eliminate the possibility of a threat listening in on U.S. or coalition forces communications. Although MUOS OTAR will make several attempts to send a new GRK to every affected user, there is a chance that some terminals will not receive the broadcasted rekey. Upon their next registration, those terminals will recognize that their group key is out of order and must use OTAR to obtain the correct key. The Navy should investigate and implement a means to disable a compromised terminal without requiring a rekey of all other networked terminals.

Spectrum Adaptation

MUOS intends to use static and adaptive notching to achieve spectrum adaptation for each user. Static adaptation, or notching, is pre-planned while dynamic notching occurs post-planning when the system scans the local electromagnetic environment.

Static Notching. The USSTRATCOM or regional combatant command spectrum manager creates an operational and radio access node (RAN) UHF spectrum mask for each MUOS satellite beam carrier (also referred to as a cell). This prohibits radio transmissions in known frequencies (known as notching) and filters those same frequencies from reception (known as whitening). These prohibited frequencies could include search and rescue frequencies from the Coast Guard, restricted frequencies from the Department of Energy, frequencies used by emergency medical services, or frequencies prohibited in host nation agreements. The operational mask with approved and restricted frequencies is loaded into the MUOS terminals as part of the provisioning process.

Dynamic Notching. SA-WCDMA is designed to use adaptive power control to minimize interference and maximize system capacity by providing each user with the minimum signal power required to meet quality of service (QoS) requirements. The MUOS radios with the MUOS SA-WCDMA waveform are designed to detect the presence of nearby unplanned emitters and notch that frequency. Likewise, the MUOS base station receivers are capable of remotely detecting the presence of a legacy UHF uplink user on a MUOS SA-WCDMA uplink channel and notching the frequency used by the legacy UHF user.[11] Upon terminal power-on and registration, it scans the local UHF frequency usage and creates a local spectrum mask by notching out occupied portions of the spectrum that it might interfere with, if transmitting. The MUOS terminal combines these operational, RAN, and local masks into a “composite mask” that then governs its occupied spectrum. The composite mask and other key parameters are reported by the MUOS terminal to the MUOS GTS, which forwards the report to the NMS for storage. This information contributes to the NMS network engineer’s and C-SSE’s ability to assess

[11] The International Telecommunication Union defines a radio link as a communication path between a transmitting earth station and receiving earth station through one satellite.

network load and performance and, if necessary, modify existing frequency profiles to better utilize capacity or improve interference mitigation.

SA-WCDMA Communication Services

Voice. MUOS is intended to provide intelligible, acceptable voice service between users of various terminal types in a variety of surroundings. Voice quality is largely determined by the specific voice encoder (vocoder) used and the background noise from a user's surroundings. MUOS is designed to provide voice two QoS levels: "conversational" voice and "recognition" voice. MUOS uses the Mixed Excitation Linear Predictive – enhanced (MELPe) low-rate vocoder, at a rate of 2.4 kbps for conversational voice service. MUOS uses the G.729 speech codec transported at a rate of 9.6 kbps for recognition voice services.[12] The MUOS Program Office employs the voice recognition protocol to provide high-priority users superior voice quality compared to conversational voice.

Data. The Navy designed MUOS to support three types of data transport service: stream, burst, and flow. The streaming transport service transports bits across MUOS with low tolerated errors and without retransmitting erroneous bits. A typical application of streaming is video or video teleconferencing. Burst service delivers short messages with constraints on the total transmission delay and message loss probability. Burst messages are essentially error free. That is, when errors are detected in received messages, these messages will be resent until they are received with no errors detected. A typical application of a burst service is texting. Flow is a transport service that transfers data from source to destination in non-real time. Flow service delivers data error-free. When errors are detected, the data will be retransmitted. A typical application of a flow service is e-mail.

MUOS Network Types

- Point-to-Point (P2P): P2P service is when a single MUOS user communicates with another single MUOS user or data terminal. P2P service is most closely related to a typical phone call. P2P service can support either voice or data communications. A user only needs to register his terminal in MUOS to be able to call another MUOS terminal.
- Point-to-Network (P2N): A P2N occurs where a MUOS terminal connects to another network and can talk to a single user or multiple users over that network. P2N occurs when a MUOS terminal connects to an IP network – such as SIPRNET or NIPRNET – or it may occur at the tactical level where a MUOS terminal connects to a tactical server, such a Command Post of the Future (CPOF), which enables a simultaneous tactical chat capability to other MUOS terminals.

[12] A codec is a device or computer program for encoding or decoding a digital data stream or signal.

- Group (or netted): Group service occurs when a MUOS terminal transmits to multiple receiving MUOS terminals simultaneously. In a group call, the transmitting MUOS terminal can communicate with multiple MUOS terminals over multiple beams, beam-carriers, or MUOS satellites. MUOS employs two types of group services:
  - Immediate assigned networks are the standard group calls in MUOS. They are available for use at their planned priority level immediately upon being provisioned into the system. An immediate assigned network's satellite resources are dynamically allocated each time a MUOS terminal transmits data.
  - Fixed assigned networks are nets that are scheduled as part of their provisioning process. A Fixed assigned network's satellite resources (i.e., downlink codes and power) are not dynamically allocated as is the case for P2P calls and immediate assigned networks. Rather, fixed assigned networks' resources are reserved for use during particular times or days, as scheduled. Therefore, these networks have priority over immediate assigned networks.

Network Management

The NMS is operated by NCTAMS-PAC personnel located in Wahiawa, Hawaii. They manage the physically dispersed MUOS ground system components and supporting user communications from a single location. The NMS provides operator displays for the configuration, health, and status of the ground system components, including Fault, Configuration, Accounting, Performance and Security (FCAPS) Management.

The NMS has two management enclaves: the Secret and For Official Use Only (FOUO) enclaves. The NCTAMS-PAC network managers use the Secret Enclave for MUOS resource management, communication planning and apportionment, frequency management, provisioning management, and security. The FOUO enclave is intended to provide network managers the capability manage the MUOS terrestrial network, including GTS and GIS network elements.

The NMS requires 30 people at Wahiawa operating in shifts and 2 on-call maintainers at each of the other three RAF/SF sites for a total of 36 staff members to support "24/7" operations. The primary functions necessary for the MUOS network managers to manage the ground system are the following:

- Network Health. The NMS staff must maintain the health of the network by monitoring events, predicting and isolating problems, and monitoring system performance. Managing network health involves collecting and managing FCAPS data. The managers collect Simple Network Management Protocol (SNMP) faults using the IBM Tivoli Netcool fault management application.
- Provisioning. The NMS staff must be able to modify the network in order to provide end user services, and maintain the health of the network.
- Situational Awareness. The NMS staff needs to be capable of measuring and monitoring system resources and metrics.

- Communications Planning. The NMS staff must support SMDC/ARSTRAT and RSSC planning and provisioning.
- Security. The NMS Security Administrator has to enforce security policy and procedures to protect against unauthorized entry and for handling encryption keys in accordance with the MUOS Key Management Plan.

Switchover

Each RAF has three earth terminals (ETs). Two of the terminals provide active Ka-band links to different satellites, and the third ET is a spare. Should an ET switchover be required for planned or unplanned maintenance, or to overcome ET failure or performance degradation, the spare may be brought online remotely using tools provided to the NMF and SCF. The NMF has control over the ET and the ET Interface (ETI) configuration, but the SCS has control over the TT&C configuration including the Modem Transmission Security (TRANSEC) Controller (MTC), which must be initialized on the spare ET. Therefore, both facilities must participate in the switchover process. Coordination between the SCS and NMS is imperative so that the SCS can conduct a change of TT&C operations to use the opposite RAF. The operation may drop a number of SA-WCDMA calls not supported by an overlapping satellite beam footprint. While the change in RAFs is being accomplished by the SCS Operator, the NMS operator must acquire satellite track with the replacement ET.

Section Two
Test Adequacy

The operational testing of the MUOS in the second Multi-Service Operational Test and Evaluation (MOT&E-2) was adequate to support an evaluation of the system's operational effectiveness, suitability, and cybersecurity. The Naval Command Operational Test and Evaluation Force (COTF), with support from the Army Test and Evaluation Command (ATEC) and the Air Force Operational Test and Evaluation Command (AFOTEC), conducted the operational test in accordance with the DOT&E-approved test plan, approved on October 13, 2015. COTF did not evaluate the cybersecurity for parts of the MUOS involved in satellite control. The Navy is planning a follow-on test and evaluation (FOT&E) in FY18. During the FOT&E, COTF should evaluate the cybersecurity of the entire MUOS. The Navy should address the many cybersecurity vulnerabilities discovered during MOT&E-2 prior to the FOT&E.

DOT&E bases this evaluation primarily on data collected by COTF and supporting Service operational test agencies from October 19 to November 20, 2015, and a COTF-conducted cybersecurity Adversarial Assessment from April 4 – 8, 2016. Data included satellite control digital log files, Network Management Segment (NMS) automated logs, manually recorded logs, user surveys, and DOT&E staff observations of testing at the satellite control center, at the NMS and Wahiawa Radio Access Facility (RAF), and at ground sites.

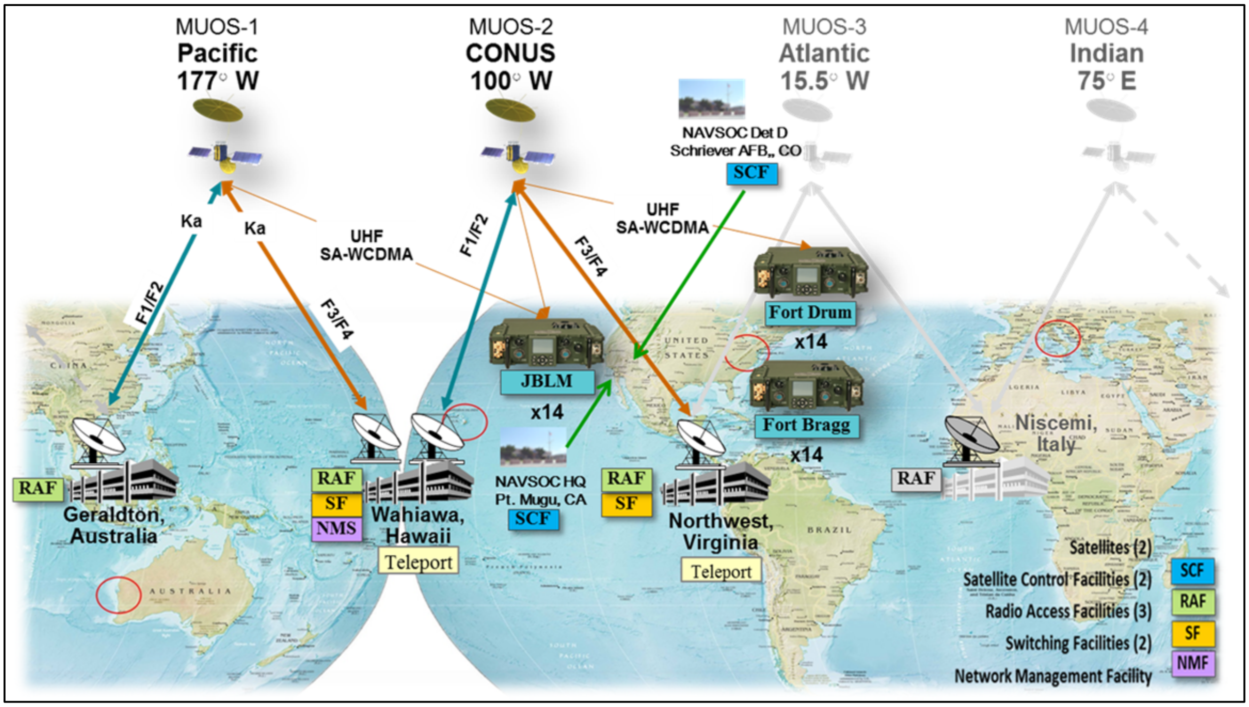
Test Configuration

The MOT&E-2 test configuration consisted of the two on-orbit satellites located at 177 degrees (Pacific region satellite – MUOS-1) and 100 degrees (Continental United States (CONUS) satellite – MUOS-2) west longitudes. The satellites operated both legacy UHF channels and Spectrum Adaptive (SA)- Wideband Code Division Multiple Access (WCDMA) communications cells. Three radio access facilities (RAFs) – at Northwest, Virginia; Wahiawa, Hawaii; and Geraldton, Australia – were configured with Build-3 hardware and software. Those three RAFs communicated with the orbiting satellites and serviced mobile user communications. The Northwest, Virginia and Wahiawa, Hawaii switching facilities routed user traffic. The NMS – located at Wahiawa, Hawaii – performed network and key management.

Army Space and Missile Defense Command/Army Strategic Forces Command (SMDC/ARSTRAT) personnel at Peterson Air Force Base (AFB) used the NMS web portal to provision terminals. Regional Satellite Communications (SATCOM) Support Center (RSSC) – West personnel provisioned group network requests. Army personnel located at Fort Bragg, North Carolina; Fort Drum, New York; and Joint Base Lewis McChord (JBLM), Washington, conducted point-to-point (P2P), point-to-network (P2N), and group communications in soldier at the pause, soldier on the move, and vehicle on the move configurations.

The Naval Satellite Operations Center (NAVSOC) at Point Mugu, California, controlled the satellites under normal operations. NAVSOC Detachment Delta performed as the alternate satellite controllers. The Ground Infrastructure Segment (GIS) provided interconnectivity between the sites and interconnectivity to the Air Force Satellite Control Network (AFSCN). The AFSCN provided system-of-system support during MOT&E-2.

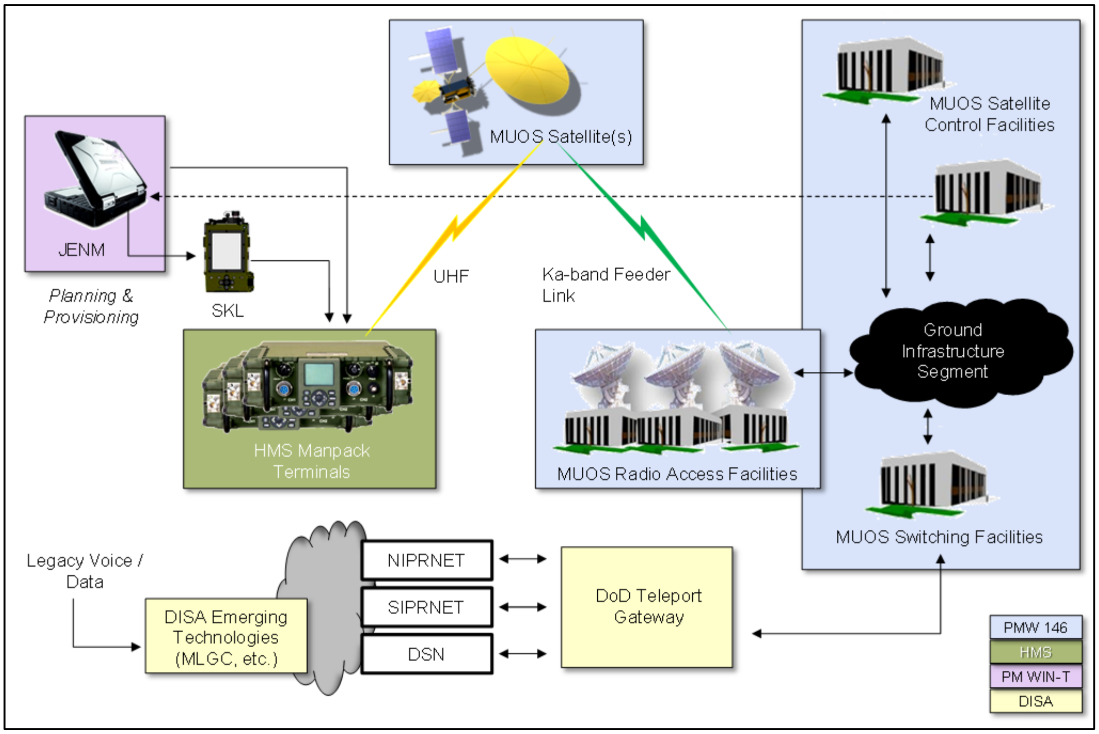
Two satellites – MUOS-3 at 15.5 degrees west and MUOS-4 at 75 degrees east, both depicted in Figure 2-1 – did not participate in MOT&E-2, consistent with the DOT&E-approved test plan. MUOS-3 was just arriving in its orbital location and MUOS-4 was still undergoing on-orbit developmental testing. Likewise, the Niscemi, Italy, RAF is not yet operational due to local Sicilian legal challenges against MUOS going operational and electromagnetically radiating.



NAVSOC – Navy Satellite Operation Center; JBLM – Joint Base Lewis McChord; Det D – Detachment Delta; UHF – Ultra High Frequency; F – Frequency; SA-WCDMA – Spectrally Adapted Wideband Code Division Multiple Access; HQ – Headquarters; Ka – Frequency Band; AFB – Air Force Base; NMS – Network Management Segment

Figure 2-1. MOT&E-2 Test Configuration

MUOS relies on other systems to achieve an end-to-end operational capability. COTF required several of these complementary systems to test and evaluate MUOS. These cooperating systems included the SA-WCDMA-capable Handheld, Manpack, and Small-Form-Fit (HMS) Manpack radios; the Joint Enterprise Network Manager (JENM) for provisioning of the radios; and the Teleport Defense Information Systems Network (DISN) services of NIPRNet, SIPRNet, and Defense Switched Network (DSN). Figure 2-2 shows the system-of-systems view that illustrates the complimentary systems from various program agencies required to complete MUOS end-to-end capability.



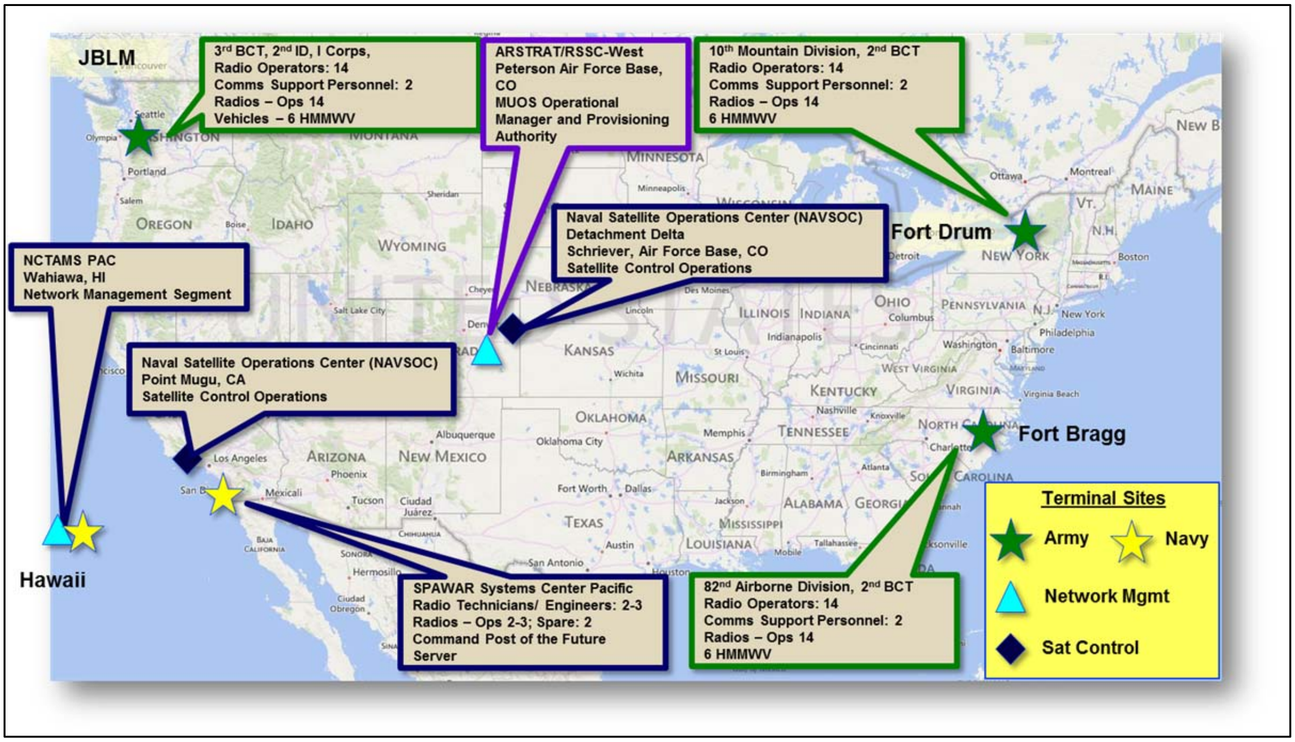
JENM – Joint Enterprise Network Manager; SKL – Simple Key Loader; UHF – Ultra High Frequency; HMS – Handheld, Manpack, Small Form-Fit; DISA – Defense Information Systems Agency; NIPRNet – Non-classified Internet Protocol Router Network; DSN – Defense Switched Network; SIPRNet – Secret Internet Protocol Router Network; PMW 146 – MUOS Program Office; PM, WIN-T – Project Manager, Warfighter Information Network – Tactical; MLGC – MUOS-to-Legacy UHF SATCOM Gateway Component

Figure 2-2. MUOS System-of-Systems View

Operational Testing

COTF conducted the operational test with the participation of ATEC and AFOTEC. COTF required multiple ground sites with military and civilian personnel performing their assigned missions to collect the data necessary to evaluate MUOS operational effectiveness, suitability, and cybersecurity.

As shown in Figure 2-3, the ground sites included elements of the 82nd Airborne Division in North Carolina, the 10th Mountain Division in New York, the 2nd Infantry Division and I Corps in Washington, satellite control sites in California and Colorado, the operational provisioning authority in Colorado, a Navy supporting communications site in California, and the Naval Computer and Telecommunications Area Master Station – Pacific in Hawaii.


JBLM
3rd BCT, 2nd ID, I Corps,
Radio Operators: 14
Comms Support Personnel: 2
Radios – Ops 14
Vehicles – 6 HMMWV
ARSTRAT/RSSC-West
Peterson Air Force Base, CO
MUOS Operational Manager and Provisioning Authority
10th Mountain Division, 2nd BCT
Radio Operators: 14
Comms Support Personnel: 2
Radios – Ops 14
6 HMMWV
Fort Drum
Naval Satellite Operations Center (NAVSOC)
Detachment Delta
Schriever, Air Force Base, CO
Satellite Control Operations
NCTAMS PAC
Wahiawa, HI
Network Management Segment
Naval Satellite Operations Center (NAVSOC)
Point Mugu, CA
Satellite Control Operations
Fort Bragg
Hawaii
SPAWAR Systems Center Pacific
Radio Technicians/ Engineers: 2-3
Radios – Ops 2-3; Spare: 2
Command Post of the Future Server
82nd Airborne Division, 2nd BCT
Radio Operators: 14
Comms Support Personnel: 2
Radios – Ops 14
6 HMMWV
Terminal Sites
Army
Navy
Network Mgmt
Sat Control

BCT – Brigade Combat Team; ops – operators; HMMWV – High Mobility Multipurpose Wheeled Vehicle; SPAWAR – Space and Naval Warfare Systems Command; ARSTRAT – Army Strategic Forces Command; RSSC-W – Regional SATCOM Support Center –West; NCTAMS-PAC – Naval Computer and Telecommunications Area Master Station – Pacific; Comms – Communications; HI – Hawaii; CA – California; CO – Colorado

Figure 2-3. Ground Elements

At the time of MOT&E-2, the Army had not fielded production MUOS radios or a network planning capability. The Army's Project Manager, Tactical Radio and Product Manager, Joint Enterprise Network Manager (JENM) provided 20 production AN/PRC-155 Manpack radios and JENM network planners for each Army site along with new equipment training and logistic support.

The radios and JENM are in the system-of-systems that comprise MUOS as an end-to-end capability but DOT&E did not evaluate these systems in MOT&E-2. DOT&E will evaluate these systems in their own respective operational test events. Figure 2-4 displays the radio and antenna configurations COTF employed during MOT&E-2.

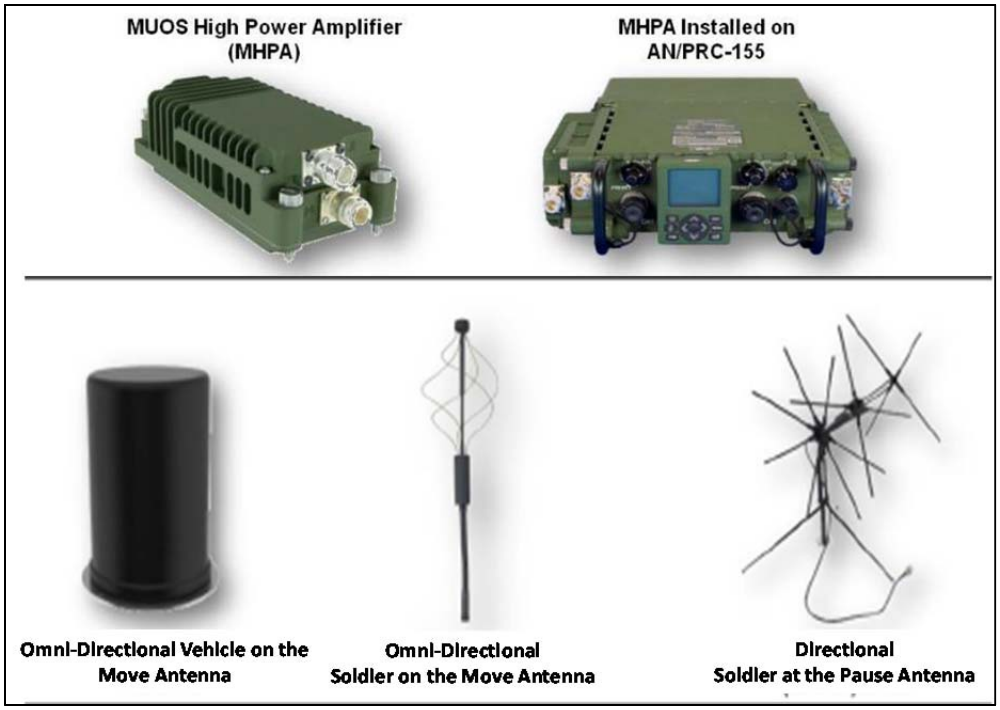

MUOS High Power Amplifier (MHPA)
MHPA Installed on AN/PRC-155
Omni-Directional Vehicle on the Move Antenna
Omni-Directional Soldier on the Move Antenna
Directional Soldier at the Pause Antenna

Figure 2-4. Radio and Antenna Configurations in MOT&E-2

Situational Awareness & Performance Management

The test team used naturally occurring and scripted events to capture the network managers, provisioner, and resource planners' ability to monitor the system status and performance. COTF and DOT&E observed the MUOS network and security managers at Wahiawa, Hawaii, and the provisioners and resource planners at Peterson AFB, Colorado, as they worked to execute performance management tasks. These tasks included displaying performance data, updating the data collection interval, and generating reports consisting of performance parameters from network components. The test team verified whether Call Detail Records were being collected and processed every 15 minutes, then transferred over to the Secret enclave for situational awareness usage. COTF observed performance metrics and statistics from the Planning and Provisioning Application (PlanProvApp) to evaluate whether MUOS reported properly and that information was timely, complete, and accurate.

Provisioning

Army unit planners created terminal profile requests for their respective terminals and submitted those requests via the Joint SATCOM Mission Planning System (JSMPS) to the Army Space and Missile Defense Command/Army Strategic Forces Command (SMDC/ARSTRAT) in Colorado Springs, Colorado. SMDC/ARSTRAT serves as USSTRATCOM's UHF Consolidated SATCOM System Expert (C-SSE) and Operational Planning Authority (OPA).) COTF collected effectiveness data on MUOS's terminal profile creation capability, based on provisioning the 60 terminals in MOT&E-2. COTF collected user survey information from the operational provisioner on the provisioning application's effectiveness and suitability.

Army unit planners created group satellite access requests (SARs) using USSTRATCOM's Joint integrated SATCOM Tool (JIST) web portal and submitted the SARs to the RSSC-West resource planners. The test team observed the resource planners using the MUOS PlanProvApp and generating group satellite access authorizations (SAAs). COTF observed the resource planners and collected effectiveness data on MUOS's capability to support the resource planners' mission. COTF collected user survey information on the effectiveness and suitability of the MUOS group provisioning and SAA creation capability.

COTF, with ATEC support, collected data to answer time and success metrics at Fort Bragg, Fort Drum, and JBLM when the unit planners and terminal operators received their terminal profiles and group configurations. The unit communication planners used simple key loaders (SKLs) to load communications security cryptographic keys into the MUOS radios, and used JENM version 3.2 to provision the AN/PRC-155 Manpack radios with the combined seed data and group network configurations. The SKLs available at the units were not capable of loading MUOS profiles so the units used a two-step process. Once the crypto-keys and MUOS profiles were loaded, the units powered on their terminals and registered them in MUOS. ATEC provided COTF with data collection quality control on site at all three Army locations and back at the ATEC home station (Fort Hood, Texas) throughout the MOT&E-2.

Network Management

The test team continuously monitored and observed the MUOS network managers performing their tasks throughout the entirety of MOT&E-2. The testers collected automated system data, manually generated logs and trouble tickets, and performed user surveys of the MUOS network managers, security managers, and maintainers. COTF and DOT&E observed NMS network managers using Fault, Configuration, Accounting, Performance, and Security (FCAPS) software (e.g., IBM Tivoli Netcool, Ericsson OSS) to monitor alarm events and attempt to isolate problems within MUOS. The test team observed the NMS network managers performing scheduled and unscheduled configuration changes, such as an earth terminal switchover.

WCDMA and Legacy UHF communications

The test team employed operational Army units at three locations across CONUS to gather data to evaluate MUOS SA-WCDMA SATCOM voice and data communications:

- Army 2nd Brigade Combat Team (BCT), 10th Mountain Division, Fort Drum, New York
- Army 2nd BCT, 82nd Airborne Division, Fort Bragg, North Carolina
- Army 3rd BCT, 2nd Infantry Division and I Corps elements, JBLM, Tacoma, Washington

The Army units conducted Army-relevant mission scenarios to test MUOS end-to-end communications in a realistic operational environment including open, forested, and urban terrain, executing radio reporting scripts. The scripts were developed by ATEC and based on Army operational doctrine and formats. The three geographically separated units sent voice transmissions consisting of preformatted Army reports and data files consisting of chat, e-mail, and file attachments over P2P, P2N, and group networks. The group network sizes the test team evaluated ranged from 2 to 38 participants. As shown in Table 2-1, based upon emerging Army fielding plans and doctrine, Army MUOS groups at BCT and below can range from 4 to 31 participants, depending upon the network.

Table 2-1. Army MUOS Group Networks

Army Network Type	Typical Number of Participants*
Platoon Command and Control	4 to 9**
Company Command	12
Battalion Administration and Logistics	12
Battalion Command	16
Brigade Command	26
Brigade Operations and Intelligence	31

* Actual numbers may vary depending upon mission requirements

** Typical platoon may have four participants while a scout platoon can have up to nine participants.

COTF conducted MOT&E-2 through the execution of 952 mission scenarios transmitting over 271 established group networks with 4,609 individual terminal transmissions to evaluate the diversity of factors that could affect performance of the MUOS.

The test team gathered SA-WCDMA communications performance data in terms of data rate, voice quality of service, probability of call completion, supporting communications-on-the-move (COTM), and MUOS's capability to support disadvantaged users in open, urban, and forested terrain. The test team also collected data to evaluate MUOS performance – whether the users were under the same satellite or different satellites – and evaluate the different possible communication paths through the MUOS ground segment.

The test team conducted a comparative test of 341 legacy UHF transmissions to compare the Legacy UHF performance with that of MUOS under the different terrain types. COTF executed the comparative tests with legacy UHF operators on legacy UHF (AN/PRC-117) radios. Legacy operators shadowed the MUOS terminal operators, executing the same mission scenarios for P2P and group networks at the same time and in the same locations. COTF kept the legacy UHF and MUOS operators 100 feet apart at the request of the MUOS Program Office to avoid co-site interference.

Communication Performance Scoring

DOT&E evaluated the quality of MUOS communications based upon the following quantitative and qualitative metrics:

- Group Probability of Effective Communications –Voice (PECV) – The probability that everyone in a group of users will receive the information necessary to complete their mission.
- Link PECV – The probability that a single MUOS user will receive the information necessary to complete his mission.
- Probability of Effective Communications – Data (PECD) – The probability that a MUOS user will successfully and accurately receive the intended data transmission.
- Message Accuracy – The percent of messages sent over MUOS for which every word was received and recorded correctly.
- User Rating – The percent of transmissions over MUOS for which a user gave the highest rating for volume and clarity to the transmission.

DOT&E calculated the Link PECV and PECD transmissions by dividing the number of total transmissions successfully received by the number of total transmissions. There is no specified user threshold criterion for PECV or PECD.

$$PEC = \frac{\#\ of\ Successul\ Transmissions\ Received}{Total\ Transmissions}$$

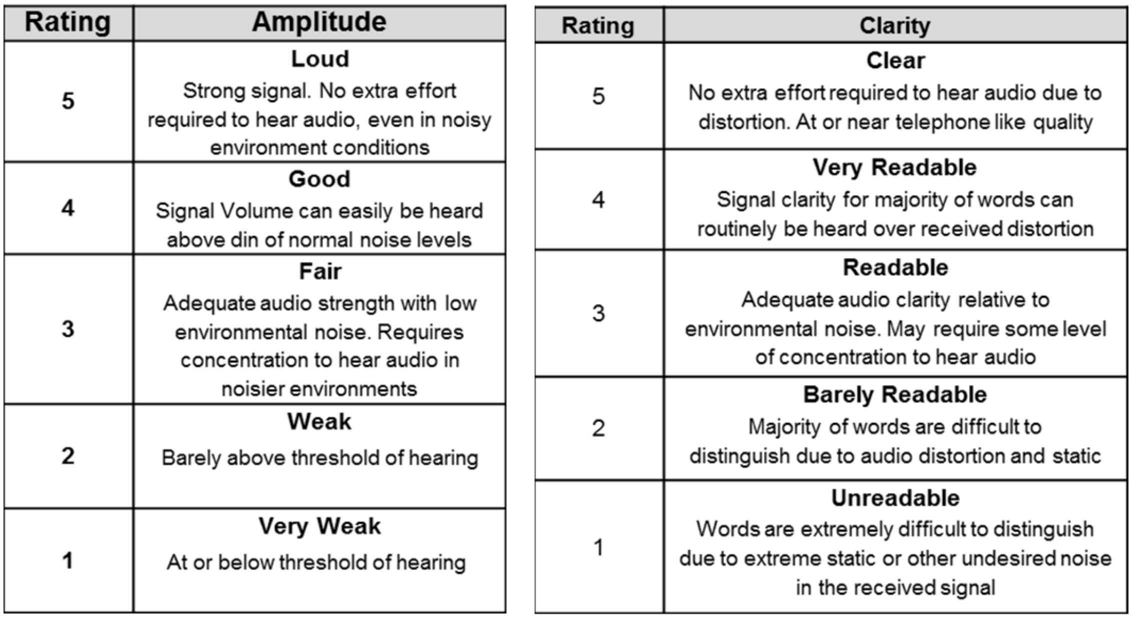
DOT&E scored PECV for group calls by two methods. The first method is based on the operational need for unit commanders to communicate with all members of their units simultaneously to execute battle orders. DOT&E evaluated the probability that all members of a radio network would successfully receive the transmission when sent. DOT&E also evaluated individual link performance – that is, the probability that a single MUOS user will receive the transmission when a message is sent in a group service. Functionally, a group communication is composed of a number of individual links. DOT&E scored each radio link independently of the others in the group, for success or failure of a received transmission. DOT&E defines a radio link as a transmission from one radio terminal to a receiving radio terminal. DOT&E is confident that scoring by both methods provides more comprehensive and accurate information than scoring by either method alone. Failures resulting from non-MUOS reasons (e.g., operator error, HMS Manpack terminal hardware problems) were excluded from the evaluation.

The test team also evaluated voice communications performance qualitatively by having terminal operators subjectively score transmissions using the Mean Opinion Score (MOS) methodology.[13] Terminal operators scored each received transmission by the amplitude and clarity of each transmission received, based on the criteria shown in Table 2-2. The test team considered a MOS score of 3x3 to be the minimum allowable score for a voice transmission to be counted as successful. If an operator scored the transmission below three in either amplitude or clarity, then DOT&E considered it a failed transmission. Although scoring can vary by

[13] Mean Opinion Score (MOS) is a test that has been used for decades in telephony networks to obtain the human user's view of the quality of the network.

operator and is subjective in nature, it nonetheless presents an overall level of voice performance as judged by the actual radio operators.

Table 2-2. Mobile User Objective System Mean Opinion Score Ratings



Rating	Amplitude
5	**Loud** Strong signal. No extra effort required to hear audio, even in noisy environment conditions
4	**Good** Signal Volume can easily be heard above din of normal noise levels
3	**Fair** Adequate audio strength with low environmental noise. Requires concentration to hear audio in noisier environments
2	**Weak** Barely above threshold of hearing
1	**Very Weak** At or below threshold of hearing

Rating	Clarity
5	**Clear** No extra effort required to hear audio due to distortion. At or near telephone like quality
4	**Very Readable** Signal clarity for majority of words can routinely be heard over received distortion
3	**Readable** Adequate audio clarity relative to environmental noise. May require some level of concentration to hear audio
2	**Barely Readable** Majority of words are difficult to distinguish due to audio distortion and static
1	**Unreadable** Words are extremely difficult to distinguish due to extreme static or other undesired noise in the received signal

DOT&E assessed data transmission performance based on the successful transmission of a file from one MUOS user to another MUOS user. The team verified the integrity of each file on transmission and upon receipt. DOT&E also evaluated MUOS terminal operators' ability to access NIPRNet and SIPRNet webpages. DOT&E considered the transmission a success if the MUOS terminal operator was able to access the desired webpage and it loaded fully and correctly. The test team also had the soldiers set up a tactical chat network (using the capabilities of a Command Post of the Future (CPOF) server) and perform missions employing tactical chat. DOT&E considered a transmission successful if the MUOS terminal operator received it as accurate, complete, timely, and usable.

Satellite Telemetry, Tracking, and Commanding

The test team collected automated system logs and operator logbooks on a daily basis. These logs provided data to evaluate the successes and failures of the system to perform satellite control tasks, issue and transmit satellite commands, direct the satellite to execute those commands, and receive acknowledgement from the satellite that the commands had been executed. The logs included the status of the commands, the time commands were issued, the time the satellite acknowledged the commands, and information regarding specific subsystems associated with the commands. Navy satellite control operators at the primary Satellite Control Facilities located at the NAVSOC Headquarters at Point Mugu, California, and the backup Satellite Control Facility located at NAVSOC Detachment Delta at Schriever AFB, Colorado, performed the tasks tracking and commanding the MUOS-1 and MUOS-2 satellites.

Cybersecurity

COTF and the Naval Information Operations Command (NIOC) conducted an operational cybersecurity Cooperative Vulnerability and Penetration Assessment from November 9 – 20, 2015, at the NMF, RAF, and SF in Wahiawa, Hawaii, and the SCS in Point Mugu, California. The cybersecurity test team reviewed their data and after determining the likely avenues of attack returned to conduct the cybersecurity Adversarial Assessment at the SCS in Point Mugu, California, and at the NMF in Wahiawa, Hawaii, from April 4 – 8, 2016. The results of the cybersecurity testing may be found in the classified annex accompanying this report.

Surveys

The testers assessed areas such as usability, training, documentation, and safety, through provisioner, resource planner, network manager, satellite controller, and maintainer surveys. COTF scored the surveys on a four-point Likert-like scale from one (strongly agree) to four (strongly disagree). The testers considered a score of three or four to be negative and a score of one or two to be positive, unless otherwise noted in the report.

Reliability

MUOS has no user-specified reliability requirements.[14] DOT&E used the MUOS user-defined ground system availability and maintainability requirements to calculate the required reliability for the ground system subcomponents using the following equation:

$$MTBOMF = MTTR\frac{A_o}{(1 - A_o)}$$

MTBOMF is the required Mean Time Between Operational Mission Failure, if the system achieved the required Mean Time to Repair (MTTR) and the required operational availability (A_o). This equation traditionally uses Mean Time Between Failure (MTBF) vice MTBOMF. However, MUOS is built with redundancy in many subsystems; a failure that counts against MTBF may not result in operational downtime. DOT&E considers MTBOMF to be more accurate in relation to operational availability in the case of MUOS.

Test Limitations

The following limitations were present for dedicated operational testing but do not affect the ability to form conclusions regarding effectiveness and suitability.

Geolocation

The Navy deferred the MUOS capability to perform geolocation from intentional and unintentional UHF interferers from MOT&E-2 prior to test because the materiel solution was not ready for test. Geolocation is the capability to locate the geographical location of a threat

[14] The reliability requirements specified in the 2008 MUOS Capability Production Document are actually availability requirements.

jammer or unintentional emitter. This capability will need to be operationally tested in the planned FY18 FOT&E, or other operational test event.

Capacity

The MUOS terminal population was not sufficient to load satellite beams and beam carriers with bearer traffic to evaluate capacity on a worldwide basis. DOT&E assessed capacity based on the two available satellites and associated RAFs that participated in MOT&E-2.

Link Availability

Link availability is a system-wide requirement evaluated over a year. The MUOS terminal population during MOT&E-2 was not sufficient to load satellite beams and beam carriers with bearer traffic nor was the time sufficient to evaluate link availability worldwide over a year's time. DOT&E assessed link availability based upon the 4,000 links used during the MOT&E-2 period.

Priority Based Access and Queuing

The available MUOS terminal population was not sufficient to saturate the available system capacity and force priority based access and queuing. The mitigation strategy is to operationally demonstrate saturating in the FY18 FOT&E using multiple terminals (estimated at 35 or greater under a single beam), operating at 64 kilobits per second (kbps) as the terminal population increases. There will not be a terminal population large enough for this to naturally occur until FY18 or later.

Communications-on-the-Move (COTM)

Testing was limited to the HMS Manpack terminal with MUOS applique provided to, and operated by, Army ground forces. Because the other Services have decided to pursue other terminal options, testing for COTM beyond 65 miles or in a shipboard environment will not be feasible until the FY18 FOT&E or later. Production-representative Air Force and Navy MUOS terminals are not anticipated to be available until the FY17/FY18 timeframe.

MUOS Doctrine, Concept of Operations (CONOPS), and Tactics, Techniques, and Procedures

At the time of MOT&E-2, there was not an approved CONOPS on how the Army plans to use MUOS. The Army Cyber Center of Excellence (Cyber CoE) is in the process of developing a CONOPS for how MUOS will be used, and the test team worked closely with Cyber CoE to emulate the evolving CONOPS. Likewise, SMDC/ARSTRAT is developing the MUOS CONOPS in anticipation of the operationalizing of MUOS. The test team worked closely with SMDC/ARSTRAT and Cyber CoE to ensure they incorporated the latest guidance into test execution.

MUOS User Terminals

The HMS Manpack terminal was the only production representative terminal available at the time of the MOT&E-2 test event. There were limited production terminals available for test and they had not yet been fielded to the Army. The Army's Program Manager for Tactical

Radios conducted new equipment training and a temporary fielding to support MOT&E-2. The Army units in MOT&E-2 returned the radios after the event.

MUOS Data Terminal Applications

There are no operational end-user applications developed to work with MUOS or MUOS terminals. The test team employed the texting functions on CPOF to perform tactical chat in a P2N configuration.

Section Three
Operational Effectiveness

MUOS is not operationally effective in providing reliable worldwide Spectrum Adaptive (SA)- Wideband Code Division Multiple Access (WCDMA) communications to tactical users. MUOS was able to provide SA-WCDMA communications on a limited scale during the second Multi-Service Operational Test and Evaluation (MOT&E-2), but MUOS cannot achieve this performance worldwide given the significant problems with planning and provisioning, situational awareness, network management, and capacity.

The MUOS satellites in MOT&E-2 operated at approximately 72 percent of capacity and could not mitigate unintentional electromagnetic interference. There is currently no means for the network managers, the Satellite Operational Manager (SOM), or the Consolidated Satellite Communications (SATCOM) System Expert (C-SSE) to monitor SA-WCDMA beam failures, leading to long outages for tactical users. Failed rekey events can result in widespread tactical communications outages. DOT&E estimates an achieved link availability of 68 percent against a 97 percent threshold requirement during the MOT&E-2 period, based on message accuracy.

The C-SSE, Army Space and Missile Defense Command/Army Strategic Forces Command (SMDC/ARSTRAT), was unable to perform beam carrier management during MOT&E-2 because the Navy has not granted the C-SSE access to the controls or training it needs to perform its responsibilities. There is no transition plan in place to achieve this. MUOS does not provide an effective system monitoring and display capability. The SOM and C-SSE cannot monitor MUOS status or evaluate actual system performance against planned performance. Provisioning outages lasting days to weeks can prevent tactical users from accessing the system when needed. The Navy deferred the MUOS capability to geolocate an interferer prior to MOT&E-2.[15] This capability and the system fixes should be tested in the Follow-on Operational Test and Evaluation (FOT&E) tentatively planned for FY18.

When available, MUOS provided SA-WCDMA voice communications on a limited scale. However, during the majority of the testing, there were isolated and widespread communications outages that could result in failed operational missions. MUOS demonstrated that the SA-WCDMA communications provide better voice accuracy and quality than the legacy ultra high frequency (UHF) channels that MUOS provides as a secondary payload on each satellite.[16] MUOS demonstrated the ability to transfer data between users and with the Defense Information Systems Network (DISN) up to 64 kbps. There is a known problem with fixed assigned networks; the MUOS Program Manager requested the Naval Command Operational Test and Evaluation Force (COTF) to avoid testing them rather than fix the problem prior to

[15] Geolocation is the identification of the real-world geographic location of an intentional (jammer) or unintentional interferer.

[16] DOT&E determined that the UHF payload on MUOS provides better quality communications than a UHF Follow-On (UFO) satellite (*Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation Report*, January 2013).

MOT&E-2. The SMDC/ARSTRAT C-SSE does not believe avoiding the use of fixed assigned networks to be a viable long-term operational solution.

MUOS is complex and operates differently than legacy UHF. Most, if not all, of the MUOS network managers do not fully understand how the system operates. The system was designed by engineers to be run by engineers. The MUOS network managers are not able to effectively manage the MUOS network. The MUOS fault management system is ineffective because it provides the network managers fault alarm events that are cryptic, inconsistently prioritized, and often excessive. The MUOS Program Manager applied filtering of alarm events to triage alarm events. The filtering is incomplete and arbitrary. These problems prevent the network managers from performing their mission and have a profound consequence on effectiveness. Without sound network management, MUOS cannot be a system the operational users can depend upon.

MUOS does not provide a proactive means to monitor SA-WCDMA beam carriers that causes extended outages for deployed users. The MUOS network managers cannot assess and report on SA-WCDMA satellite beam carrier availability. Key systems associated with SA-WCDMA call services, such as the radio base stations in the radio access facilities (RAFs), do not provide fault information to the fault management system.

MUOS has not provided the network managers with a tool to monitor the connections between the different ground sites. Without active monitoring of the DISN interconnectivity, the Network Management Segment (NMS) personnel cannot determine if there is latency in the circuits and degradations go unchecked, leading to longer reaction times when there is a loss of connectivity.

There is no MUOS concept of operations (CONOPS), procedure, or system for the MUOS network managers or satellite controllers to notify the Regional SATCOM Support Center (RSSC) resource planners, Satellite Operational Manager, C-SSE, provisioners, and deployed users of outages or system degradations and their operational effects.

Using the current processes, the MUOS NMS security personnel will not be able to keep up with the demand for keys given a full operational population of terminals. The MUOS security manager estimates that NMS can transfer 85 pairs of keys a day at current manning levels. The NMS personnel will need to transfer 250 key-pairs a day to meet demand and not result in provisioning delays to the terminal users. The Navy estimates this will be a problem by FY18 given the expected terminal fieldings.

MUOS was able to conduct routine over-the-air rekeys (OTARs) but cannot reliably conduct compromised terminal operations. The reliability problems could result in global communications outages for an entire branch of Service or all Special Operations units. An outage would persist until its root cause is resolved and the MUOS ground system broadcasts a new group cover key (GCK). The MUOS NMS successfully conducted 89.5 percent of all OTAR operations, with a 95 percent confidence interval from 66.7 to 98.7 percent. The MUOS NMS successfully conducted 100 percent (15 of 15) of routine OTARS, with a 95 percent lower confidence bound of 81.7 percent. Half (2 of 4) of the compromised terminal operations succeeded, with a 95 percent confidence interval between 6.7 and 93.3 percent. The wide range of uncertainty is a result of the small sample size. COTF did not conduct additional compromised terminal OTAR operations because failed OTARs led to long outages that were disruptive to the test.

COTF, with Naval Information Operations Command (NIOC) support, conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) from November 9 – 20, 2015, from the MUOS SCS in Point Mugu, California, and the NMF, SF, and -RAF in Wahiawa, Hawaii. After allowing time for the MUOS Program Manager to fix or mitigate vulnerabilities, COTF and NIOC followed up with a cybersecurity Adversarial Assessment at the SCS and NMS from April 4 – 8, 2016. The results of the cybersecurity testing can be found in the classified annex to this report. The Navy should fix or mitigate the numerous cybersecurity problems discussed in the classified annex to this report.

Coverage (Key Performance Parameter)

DOT&E did not re-evaluate coverage in MOT&E-2. Coverage was successfully addressed in the first MOT&E (MOT&E-1) conducted in 2012. Coverage is a MUOS Key Performance Parameter (KPP) and defined by the user as being able to provide communications for 24 hours a day, from 65 degrees north latitude to 65 degrees south latitude at all longitudes. The 4-satellite MUOS constellation will provide nearly 100 percent coverage from 65 degrees north latitude to 65 degrees south latitude if a minimum terminal look angle of zero degrees above the horizon is used. Coverage decreases as the minimum acceptable look angle is increased. Terminal elevation angle or “look angle” refers to the angle between the satellite terminal antenna pointing directly at the satellite and the local horizontal plane of the earth’s surface. As Figure 3-1 shows, a terminal look angle of 5 degrees above the horizon results in coverage of 99.99 percent, regardless of orbital parameters. Coverage below a 5 degree look angle is generally undesirable, because terrain and man-made features sometimes block line-of-sight with the satellite and ground interference attenuates the communications signal.

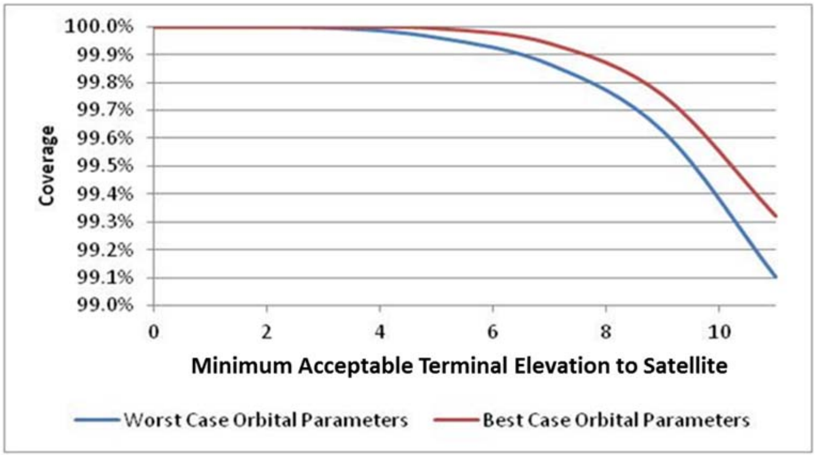


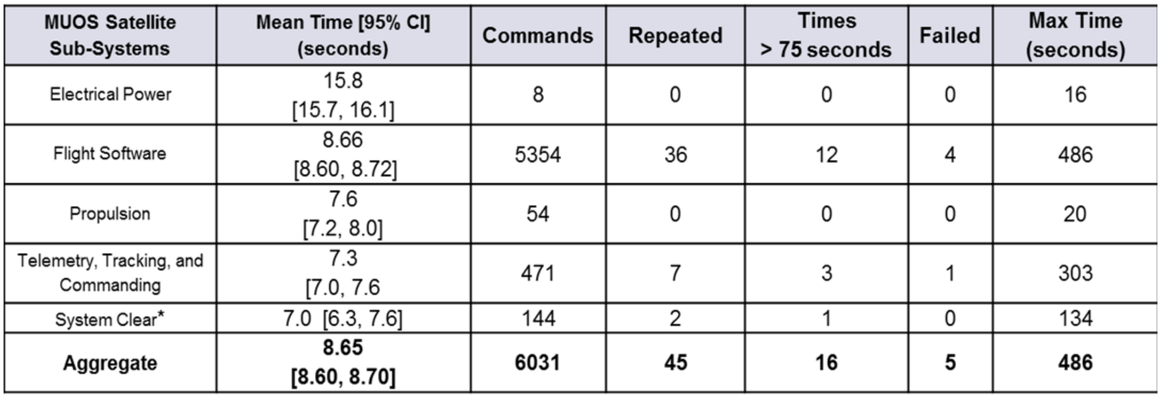
Figure 3-1. The MUOS Constellation Coverage as a Function of Look

DOT&E evaluated coverage using modeling and simulation (M&S). Verifying coverage by direct measurement is not feasible because it would require measurements over the entire globe. DOT&E used Analytical Graphics Incorporated Satellite Toolkit (STK) to calculate the coverage with measurements the contractor recorded of the antenna gain pattern for the MUOS-1 satellite in developmental testing. STK is the industry standard for calculating the orbital dynamics and coverage of satellites, and is used widely on military and commercial SATCOM. COTF accredited the specific MUOS input parameters that determine the output.

Satellite Telemetry, Tracking, and Commanding (TT&C)

The Naval Satellite Operations Center (NAVSOC) satellite controllers, using the Satellite Control Segment (SCS), were able to perform TT&C of the Pacific (PAC) and Continental United States (CONUS) satellites throughout MOT&E-2. The user-defined threshold criterion for TT&C is that the NAVSOC satellite controllers, using the MUOS space control subsystem, must transmit a command to and receive a confirmation from a MUOS satellite in 75 seconds or less. As Table 3-2 shows, the satellite controllers were able to transmit commands to and receive acknowledgements from the MUOS satellites in a mean time of 8.65 seconds.

Table 3-2. Mean Satellite Access Time by Satellite Subsystem



MUOS Satellite Sub-Systems	Mean Time [95% CI] (seconds)	Commands	Repeated	Times > 75 seconds	Failed	Max Time (seconds)
Electrical Power	15.8 [15.7, 16.1]	8	0	0	0	16
Flight Software	8.66 [8.60, 8.72]	5354	36	12	4	486
Propulsion	7.6 [7.2, 8.0]	54	0	0	0	20
Telemetry, Tracking, and Commanding	7.3 [7.0, 7.6	471	7	3	1	303
System Clear*	7.0 [6.3, 7.6]	144	2	1	0	134
Aggregate	**8.65 [8.60, 8.70]**	**6031**	**45**	**16**	**5**	**486**

* System Clear commands do not belong to a single subsystem; CI – Confidence Interval

The commands NAVSOC sent to the satellites were successful 99.9 percent of the time. Sixteen of the commands exceeded the 75-second threshold because they were failed commands that the system resent until the satellites acknowledged receipt. DOT&E measured the time between the first transmission and the satellite acknowledgement. The system automatically retransmits failed commands acknowledged by the satellite. The failed commands did not result in any operational mission failures. COTF tested TT&C in MOT&E-1 with successful results. The results from MOT&E-2 are consistent with the previous testing results where mean satellite access time was 7.5 seconds.

Capacity (KPP)

MUOS does not meet the threshold Capacity KPP criteria. Capacity is a measure of the total number of users that MUOS can support. The Capacity KPP stipulates that MUOS must provide 1,997 worldwide simultaneous accesses (39.2 Megabits per second [Mbps]), with

502 simultaneous accesses (3 Mbps) in a theater – as defined in the Communications Service Requirements – while applying electromagnetic interference (EMI) mitigation techniques as necessary to maintain the required system capacity, availability, and quality of service.

As stated in the Test Limitations section of this report, in order to evaluate this requirement DOT&E would need more than 10,000 radios distributed across the world, transmitting operationally representative messages. Thus, this requirement cannot be feasibly tested in an operational test.

Based on the configuration of the two satellites in MOT&E-2, MUOS does not meet the threshold Capacity KPP criteria. The 2 satellites under test were operating at approximately 72 percent of capacity. DOT&E did not consider the configurations of the Indian Ocean and Atlantic satellites since they were not available for operational testing. Regardless, the constellation cannot meet required capacity, even if the remainder of the constellation was fully populated and all ground stations operational. If the remaining 2 MUOS satellites operated at full capacity, MUOS could only reach approximately 86 percent capacity (220 satellite beam carriers (SBCs) of 256 possible SBCs). Further discussion of MUOS capacity and spectral EMI mitigation techniques is contained in the classified annex to this report.

As discussed under Concept of Employment in this report, each MUOS satellite radiates 64 SBCs, or cells, with 5 MHz of potential spectrum to provide the necessary capacity to meet the defined user KPP threshold. DOT&E determined that 92 of the possible 128 SBCs were active on the two satellites, for an availability of 71.9 percent. The Navy either locked or turned off 28.1 percent of the capacity. A locked SBC means users cannot access it, subtracting 5 MHz of potential spectrum from the beam. A majority (56 percent) of 32 satellite beams across the 2 satellites were in a degraded mode. DOT&E determined that:

- 6 of 32 beams were at 25 percent capacity
- 6 of 32 beams were at 50 percent capacity
- 6 of 32 beams were at 75 percent capacity
- The remaining 14 beams were at 100 percent capacity

Additionally, prior to MOT&E-2, the MUOS program modified control parameters to improve WCDMA call completion performance based upon the June 2015 Technical Evaluation results. These changes traded capacity for call performance. The decrease in capacity is not fully understood because the program manager ceased funding of the MUOS Performance Model (MPM) in 2014 for cost avoidance reasons. The developing contractor estimated the capacity losses based on the multiple changes as an additional 2-5 percent, but the actual figure may be more. The Navy relies solely on contractor estimates and is unable to perform their own estimates on performance. This has long-term implications because, when the system is transferred to U.S. Strategic Command (USSTRATCOM), the C-SSE will not be able to model performance to make informed decisions when making trades on MUOS performance and capacity. The Navy should restore funding to sustain the MPM so the government can perform independent performance and capacity trades.

The method the Navy proposed for evaluating capacity is the computer model, MPM. The configuration of MPM that the program manager proposed does not match the configuration of MUOS during MOT&E-2. COTF did not accredit the MPM model for MOT&E-2. Configuration changes made to the system were not reflected in modeling prior to the government defunding the effort. Therefore, the modeling outputs are not valid because they no longer reflect the MUOS configuration. DOT&E does not consider the MPM to be an accurate portrayal of the capacity of the MUOS.

Three MUOS power control parameters were tuned prior to the dedicated operational test to improve MUOS quality of service. As noted above, changes made that improve quality of service can decrease system capacity.

- The stress margin was increased to provide more initial power to the physical control channels. This would give users a greater chance to receive power control information and consume additional user-to-base capacity.
- Only "AddMe" groups were provisioned. This would allow users to join a group using any beam carrier, which would reduce capacity because the system would not be able to restrict users from using certain beams and carriers to balance congestion.
- The Navy liberally increased the "AddMe" limit for groups to give users a better chance to join a group. On average, more beam carriers would be used for each group. This would consume more resources, decreasing capacity.

Link Availability (KPP)

DOT&E estimates that MUOS did not meet Link Availability KPP – the proxy metric of message accuracy – during MOT&E-2. MUOS Link Availability was 68 percent against a threshold Link Availability criterion of 97 percent availability averaged over a year. This is not a directly testable measure.

Link availability is a measure of the ability of users to connect to, and maintain communications with, MUOS. The user-defined Link Availability KPP threshold criterion requires that communication must be 97 percent, averaged over any year of operation.[17] As stated in the Test Limitations section, in order to evaluate this requirement DOT&E would need more than 10,000 radios distributed across the world and operating for several years. COTF could not feasibly test this requirement in an operational test.

Link availability and capacity are interrelated in MUOS. MUOS balances power for all users so that each user is given just enough radio frequency power to maintain an acceptable quality of service, measured by block error rates (BLER).[18] As MUOS increases power to each link, to maintain link availability for individual users, the total power available to other users

[17] The International Telecommunication Union defines a radio link as a communication path between a transmitting earth station and receiving earth station through one satellite.

[18] BLER is the proportion of erroneous blocks of data received to the total number of blocks of data transmitted.

decreases. MUOS has dozens of tunable parameters to control power between the users and the satellites.

The Navy proposed using MPM to evaluate link availability. MPM is the Navy's MUOS performance and Link Availability model. The configuration of MPM does not match the configuration of MUOS during MOT&E. DOT&E does not consider the MPM to be an accurate portrayal of the link availability of MUOS. Instead, DOT&E evaluated link availability and tracked the number of users for the duration of MOT&E-2.

COTF did not measure BLER during MOT&E-2, as BLER testing is typically done in a lab environment and is not easily done operationally. DOT&E believes message accuracy is an appropriate proxy metric for BLER, because both metrics count the loss of information on a transmission. Based on the 4,609 voice transmissions, MUOS achieved a link availability of 68 percent during the MOT&E-2.[19]

DOT&E used two thresholds in place of BLER to assess the possible link availability value: message accuracy and failed transmission proportion. Message accuracy is the percentage of transmitted words that were successfully received. Successful transmission proportion is the percentage of attempted connections to the MUOS satellite that were successful.

Successful transmission proportion overestimates the link availability (98 percent), because a connection can be successful but have a quality of service that falls below the acceptable BLER threshold. In other words, links that should have failed based on the user-defined criterion for low quality were passed, and only those links that never connected to the satellites were counted.

Message accuracy slightly underestimates link availability (68 percent), because it introduces human error during data collection. DOT&E considers this error to be minor. DOT&E believes the message accuracy metric of 68 percent to be a closer BLER approximation proxy than the transmission proportion method. As recommended above, the Navy should restore funding to sustain the MPM so the government can perform independent performance and capacity trades.

Spectrum Adaptive (SA)-Wideband Code Division Multiple Access (WCDMA) Communications Planning

SA-WCDMA planning includes three areas: beam carrier management, satellite access request management, and situational awareness. All three areas either experienced problems or could not be tested during MOT&E-2.

[19] If the 854 data transmissions are also considered then the Link Availability estimate increases to 72.4 percent; however, DOT&E believes this overestimates Link Availability since failures bringing data networks into operation were attributed as configuration problems and not counted as link failures.

Beam Carrier Management

The C-SSE was unable to perform beam carrier management during MOT&E-2 because the Navy has not granted the C-SSE access to the controls. Beam carrier management is designed to provide the C-SSE with the ability to create a beam management region, configure satellite beams and carriers for each MUOS satellite, and analyze configurations for viability. Per the MUOS technical manuals, this capability is intended to facilitate the C-SSE determining frequency availability using the defined regions, in conjunction with factors such as traffic profiles, apportionment adjustments, past capacity performance, and the current system configuration. During MOT&E-2, the developing contractor performed all beam carrier management activities. The Navy should train the C-SSE and transfer the responsibility for beam carrier management per the established MUOS documentation.

Satellite Access Request (SAR) Management

SAR management is required for group network creation and reconfiguration. COTF tested and collected data for SAR management as part of group network provisioning; therefore, DOT&E is reporting the SAR management results under the group network provisioning and usability sections of this report.

During the Navy's Technical Evaluation, the RSSC-West resource planners discovered that MUOS is unable to process SARs that have more than one network group requested under a single SAR. The Navy's near-term solution is to increase the administrative burden on unit planners and have them submit individual SARs for every group network they are requesting, rather than submit multiple group networks under a single SAR. The Navy should fix the problem of MUOS being unable to process SARs with multiple group networks, and COTF should test this capability in a future operational test event.

There is also a known problem with fixed assigned networks. The Navy requested COTF avoid testing them, rather than fix the problem. The MUOS C-SSE does not believe this is a viable long-term operational solution. The Navy generated a priority (PRI)-2 problem change request (PCR) based on problems seen in the June 2015 Technical Evaluation. Problems with fixed assigned networks had resulted in either poor call quality or the group network being unexpectedly terminated. A PRI-2 PCR adversely affects the accomplishment of an essential capability. At the request of the MUOS Program Manager, COTF provisioned and tested only immediate assigned networks during MOT&E-2. DOT&E challenges the PRI-2 categorization and asserts that this should be a PRI-1 PCR – which is defined as a problem preventing the accomplishment on an essential capability – since this problem would result in an operational unit losing beyond-line-of-sight communications. The SMDC/ARSTRAT C-SSE does not believe avoiding using fixed assigned networks is an operationally viable long-term solution. The Navy should fix the problem with fixed assigned group networks and COTF should test this in the next operational test event.

Situational Awareness & Performance Monitoring

MUOS does not provide the Satellite Operational Manager (SOM), C-SSE, and resource managers an effective system monitoring and display capability. The SOM, C-SSE, and RSSC resource planners cannot monitor MUOS status or evaluate actual system performance against planned performance. MUOS does not provide them with an accurate, real-time status of the system state. The system was unable to maintain call records for the 60 terminals that participated in MOT&E-2.

The SOM, C-SSE, and resource managers depend on the MUOS web portal application over Secret Internet Protocol Router Network (SIPRNet) to obtain situational awareness and performance information as their primary means to manage MUOS operations. DOT&E interviews with resource planners and network managers revealed that the planners and managers feel the situational awareness web portal is so inaccurate and unreliable that they cannot depend upon it to perform their missions. The user-defined threshold criterion is that MUOS must have a system monitoring and display capability that supports the SOM (or C-SSE as his delegated representative) and resource managers within 5 minutes.

Situational Awareness Reports

The C-SSE and RSSC-West resource planners at Peterson Air Force Base (AFB), Colorado, access the MUOS Network Management Segment (NMS) via a SIPRNet web portal called the Planning and Provisioning Application (PlanProvApp). This web portal is their window into MUOS and is designed to provide them with a shared understanding of the system state. This provides decision makers with the tools to effectively make necessary operational decisions about MUOS communication resources. As Table 3-3 shows, during MOT&E-2, resource planners were able to obtain information from the system in 61.0 percent (52 of 85) of attempts, with a 95.0 percent confidence interval between 53.7 and 68.3 percent.

Table 3-3. Situational Views and Reports Results

REPORT TYPE	ATTEMPTS	REPORTS PASSED	REPORTS FAILED	PASS RATE PERCENTAGE	95% Confidence Interval
STATUS VIEW	15	14	1	**93.3**	76.4 - 99.3
STATUS REPORT	2	0	2	**0.0**	55.2*
PROVISIONING REPORT	2	0	2	**0.0**	55.2*
CALL USAGE REPORT	34	24	10	**70.6**	58.3 - 80.9
CALL USAGE GRAPH	9	8	1	**88.9**	63.1 - 98.9
MAP REPORTS	4	4	0	**100.0**	66.9**
REPORT DOWNLOADS	19	2	17	**10.5**	2.8 - 25.7
AGGREGATE	**85**	**52**	**33**	**61.0**	**53.7 – 68.3**

* Upper Confidence Bound; ** Lower Confidence Bound

The failures that testers observed for Situational Awareness Views and Reports were page loading errors, partially loaded web pages, incomplete reports, and inaccurate reports. For example, MUOS reported that there was no activity when there were known active networks that should have been reported. When successful, web accesses took a mean time of 5 minutes, with a 95 percent confidence interval of 4.8 to 5.2 minutes.

The Navy recorded similar results from the June 2015 Technical Evaluation in preparation for MOT&E-2. Based on the Technical Evaluation data, DOT&E determined that the developmental testers assessed the aggregate situational views and reports as passing on 63.9 percent (131 of 205) of attempts. The report latency was worse in Technical Evaluation and partially improved by the time of MOT&E-2. While the Navy made efforts to speed up latent processing times, the problems with time-outs, inaccuracy, and incomplete reports remained uncorrected and resurfaced in MOT&E-2. Two important situational reports are indicative of the types of problems the C-SSE and resource planners experienced: Global System View and Call Detail Records.

Global System View

The top-level monitoring tool is called the Global System View. The purpose of the Global System View is to provide the MUOS network managers, C-SSE, and resource planners with a shared, real-time health status of the various ground sites and satellites that comprise MUOS. Status is coded green, yellow, or red: Green indicates the component is fully mission-capable; yellow indicates a degraded status; and red indicates the component is not mission-capable. During MOT&E-2, DOT&E observed that the Global System View showed the Indian Ocean MUOS satellite in the wrong orbital position over CONUS, and that the Table of Satellite Beam Carrier status was empty. The Global System View was never accurate during the entire MOT&E-2 period.

The Navy knew of these problems at least as early as May 18, 2015, when the developmental testers reported that the Global System View indicated the MUOS satellites were in the wrong orbital slots, and that the view also indicated all terrestrial sites (RAFs, NMF, SF, etc.) had erroneous "Red – Not Operational" statuses. The SMDC/ARSTRAT and RSSC-West planners reported the problems multiple times in the June 2015 Technical Evaluation. The problems resurfaced in MOT&E-2 since the Navy did not take corrective action between the two test events.

The Global Systems View status is fed from the NMS by the fault management application, IBM Tivoli Netcool (Netcool). There are numerous problems with how the Navy instantiated Netcool within MUOS. These problems – discussed in the Network Management section below – are propagated into the PlanProvApp situational awareness and performance management views and reports. The Global System View can be manually overridden if the network managers know the true status of MUOS; however, this is often not the case. When managers do override the system status, the override does not always work correctly. In one case when the status was overridden and saved, the refreshed screen did not provide the expected results and in another case after deleting an overridden status it still persisted.

There is no CONOPS to update the Global System View and no one is tasked to keep the status current within MUOS. The MUOS network managers have found the Global System View to be so unreliable that they now manually track the status of the various components of MUOS using Microsoft PowerPoint presentations. The Navy should perform root cause analysis and correct the problems the Global System View.

Call Detail Records

The MUOS C-SSE, resource planners, and network managers could not determine who was using MUOS during MOT&E-2, because the MUOS NMS was unable to accurately maintain Call Detail Records (CDRs) in a timely manner. The CDR data are the primary data that MUOS uses to generate situational awareness point-to-point (P2P) and group usage reports. CDRs provide the MUOS C-SSE, resource planners, and network managers with the status of MUOS users, call activity of MUOS users, and an indication of the MUOS communications resources being used. The CDRs are generated by the Radio Network Controllers located in the four RAFs and populated to the database at the NMS.

The RSSC-West resource planners queried the system for Group Call Usage Reports 234 times during MOT&E-2. Only 40.6 percent (95 reports) were successfully displayed. RSSC-West planners queried the system in a manner that took into account the system's latency. The records that were queried were sufficiently back in time that they should have been available and accurate.

The latency in retrieving CDRs grew to 31 hours during the MOT&E. This latency caused a backlog of 24,500 records (Figure 3-2). As Figure 3-2 shows, on October 22, 2015, the RSSC-West submitted a PRI-2 trouble ticket because the system was not processing CDRs. The Navy elevated the problem to depot maintenance. The depot maintainer determined the usage processing server was not connecting to the Java Message Service (JMS) Broker Server. The NMS network managers overlooked the fault alarm because it was displayed to them via Netcool as "informational" and did not alert them to take action. The depot maintainer could not recover the 37,400 unprocessed CDRs and purged them from MUOS.

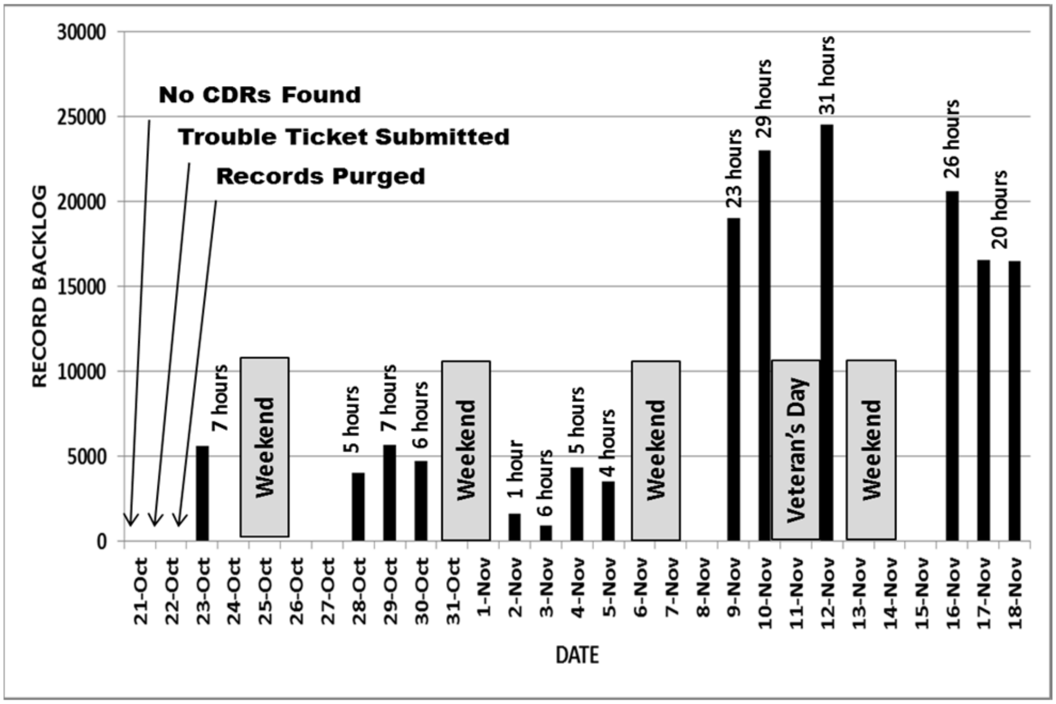


Figure 3-2. Latency and Backlog Retrieving Call Detail Records

COTF did not test on weekends or Veterans Day, at which points the system was able to recover somewhat. DOT&E believes the reduction in backlog at the end of MOT&E-2 (November 17 – 18, 2015) is explained by Fort Bragg's 82nd Airborne Division not participating in the final week of test due to other mission requirements. MOT&E-2 had, on average, 48 terminals communicating a day. The system response will be significantly worse when MUOS is under a full load of 1,997 users simultaneously accessing it.[20]

The Navy experienced latent and inaccurate CDRs during the June 2015 Technical Evaluation but did not to correct them prior to MOT&E-2. The root cause for the inaccurate and late CDRs was never determined with certainty in either in the Technical Evaluation or MOT&E-2. The cause was most likely related to the use of an overloaded database, on the Operating System Support – Radio and Core server, which is at 97 percent capacity. This database is used for provisioning information, CDRs, and correlated system alarms and statuses. This situation was compounded by the server operating in "debug mode," which increased processing overhead. Debug mode is a software engineering and troubleshooting mode, not an operational mode. These problems are discussed in further detail in the Operational Suitability section of this report. The Navy should perform root cause analysis and correct the problems with latent and inaccurate CDRs.

System Performance Monitoring

MUOS does not provide the C-SSE, resource planners, and network managers with a reliable or accurate means to perform their mission of monitoring actual system performance against planned performance. As Table 3-4 shows, planners were able to successfully access system performance information 21.6 percent (19 of 88 attempts) of the time (15.9 to 28.2 percent of the time at the 95.0 percent confidence interval). Performance views and graphs consist of either individual or aggregated performance reports, including power and communication resource codes used per beam, beam load factors, aggregated bandwidth, and total bandwidth per beam. When successful, performance reports and graphs took a mean time to obtain of 5.4 minutes, with a 95 percent confidence interval of 5.1 to 5.8 minutes.

Table 3-4. Performance Report Results

Report Type	Report Attempts	Reports Passed	Reports Failed	Pass Rate Percentage [95% Confidence Interval]
Performance Reports	73	15	58	20.5 [14.5 - 27.9]
Performance Graphs	15	4	11	26.7 [12.2 - 46.4]
Aggregate	**88**	**19**	**69**	**21.6 [15.9, 28.2]**

[20] There were 20 radios at each Army test location but 4 MUOS terminals at each location were spares, used only if other MUOS terminals failed.

The failures that testers observed for the performance reports and graphs were page loading errors, partially loaded web pages, erroneous reports, and incomplete reports. The problems observed with the situational portal are endemic within the MUOS. Inadequate fault management at the NMS, inconsistent alert filtering, and poor system reliability are fed into the NMS PlanProvApp and propagated to the performance reports and graphs, rendering them unusable. This undermines the ability of the SOM, C-SSE, and resource managers to perform their mission of monitoring and controlling MUOS communication resources. DOT&E observed during the test that users of the situational awareness portal have minimized their usage or even stopped using it altogether because they do not trust the results. There are additional problems with situational awareness in the discussion of usability in the Operational Suitability section of this report. The Navy should fix the problems with inaccurate, incomplete, and missing situational awareness and performance webpage views, reports, and graphs.

Provisioning

The SMDC/ARSTRAT provisioner was successful in 100 percent (60 of 60) of the attempts to create MUOS terminal profiles. As Table 3-5 shows, the 95 percent lower confidence bound based on the 60 successes is 93.9 percent. The SMDC/ARSTRAT provisioner was able to create the 20 terminal profile seed files for each group in a mean time of 5.6 minutes. There is no defined user threshold criterion for this function.

Table 3-5. Summary of Terminal Profile Creation Results

Source	Attempts	Successes	Pass Rate Percentage	95% Lower Confidence Bound
Fort Drum	20	20	100	82.9
Fort Bragg	20	20	100	82.9
JBLM	20	20	100	82.9
Aggregate	**60**	**60**	**100**	**93.9**

JBLM – Joint Base Lewis McChord

As discussed previously, the SMDC/ARSTRAT provisioner receives the terminal profile requests through the Joint SATCOM Mission Planning System (JSMPS) and imports requests into the MUOS PlanProvApp to generate the terminal seed file, known as a synopsis file, which includes the necessary terminal profile data. These profile data include:

- One or more frequency profiles
- Cryptographic key tags
- The International Mobile Subscriber Identifier (i.e., a unique terminal identification number)
- The Mobile Station Integrated Services Digital Network (MSISDN) identifier (i.e., a MUOS phone number)
- Internet Protocol (IP) addresses

While the SMDC/ARSTRAT provisioner was able to create the necessary terminal profiles, there are problems with the process that can lead to errors. MUOS treats IP addressing differently, depending upon enclave. The current MUOS end-to-end architecture has a generic discovery server (GDS) for Secret U.S.-Only enclaves (red-side), but not for the unclassified For Official Use Only (FOUO) enclave or the Top Secret enclave. As a result, planners use dynamic IP addressing on the Secret enclave but static IP addressing on the FOUO and Top Secret enclaves.

The Generic Discovery Server (GDS) is a software application that simplifies the configuration process and increases the efficiency of High Assurance IP Encryptors (HAIPE) in the MUOS radios. HAIPE devices can be configured to automatically register with the GDS, enabling dynamic versus IP addressing.[21] Planners prefer dynamic IP addressing over dynamic addressing because it is easier to manage and more efficient.

The purpose of a static IP address is to prescribe the communication address routes within the MUOS terminal so it can talk with another terminal, server, or the Defense Information Systems Network (DISN). If terminals use static IP addresses, then the terminal will require re-provisioning anytime a new route is required or the user needs to place a call to another user whose terminal information was not previously provisioned in that terminal. During military operations, this will become burdensome to MUOS users. The Navy should work with the Defense Information Systems Agency to implement a GDS for the MUOS FOUO and Top Secret enclaves to resolve IP addresses and enable dynamic IP addressing.

Since there is no GDS on the FOUO enclave, the SMDC/ARSTRAT provisioner has to assign terminals static IP addresses for MUOS users to conduct point-to-network (P2N) communications. The SMDC/ARSTRAT provisioner has to use a limited set of static IP addresses that he has to manage using an offline spreadsheet program. When the provisioner places the static IP addresses in the MUOS PlanProvApp and executes the provisioning, the manual bookkeeping of IP addresses induces errors. Additionally, when the provisioner inputs the IP address list into the MUOS PlanProvApp, it assigns terminal MSISDNs to the profiles without regard to the static IP address order. When the provisioner transfers the MUOS-generated synopsis files to JSMPS, it reads the synopsis file and places the MSISDNs in the sequential order of the reserved IP addresses.

The outcome is a mismatch of IP addresses between the MUOS terminals and the MUOS ground system. This would result in failed user communications unless the problem is caught and fixed by the provisioner prior to the provision being sent to the ground system and unit planner. In MOT&E-2, the SMDC/ARSTRAT provisioner was able to correct the errors before the test began for the limited number of radios used during the test. However, provisioners will be unable to make such corrections when there are thousands of MUOS radios deployed. The Navy should modify the MUOS PlanProvApp so that the provisioner can load a series of IP

[21] A static IP address is when a device has an IP address that never changes. In dynamic IP addressing the Dynamic Host Configuration Protocol assigns a different address every time a device connects to a network. These IP addresses are temporary, and can change over time.

addresses and the system can assign the IP addresses in the sequence loaded. The Navy should also update system documentation and training appropriately. USSTRATCOM should update JSMPS to provide the capability for provisioners to modify IP address assignments, and select/filter how JSMPS reads in MUOS terminal profile information.

The MUOS PlanProvApp allows the provisioner to select fixed IP addresses for P2P and P2N networks outside of the appropriate subnetworks without warning when allocating resources. If the provisioner does not catch the error this results in failed P2P and P2N services for deployed users. The Navy has been aware of this problem since the PRI-2 problem report submission in January 2015. The Navy should fix the erroneous IP address allocation outside IP subnetworks to avoid deployed user failed communications.

The MUOS lacks a long-term solution to resolve NIPRNet and SIPRNet website names and provide content back to users. The MOT&E-2 used temporary assets housed in a test laboratory in San Diego. However, long-term tactical Domain Name Service (DNS) capabilities are needed to support future MUOS to NIPR and SIPR requirements. A DNS enables the use of website names and e-mail addresses rather than requiring users to know specific numerical IP addresses. Without a DNS, users are unable to access NIPRNet and SIPRNet websites without direct knowledge of the specific server IP address. The Navy should work with the Defense Information Systems Agency to implement a SIPRNet and NIPRNet DNS capability for MUOS.

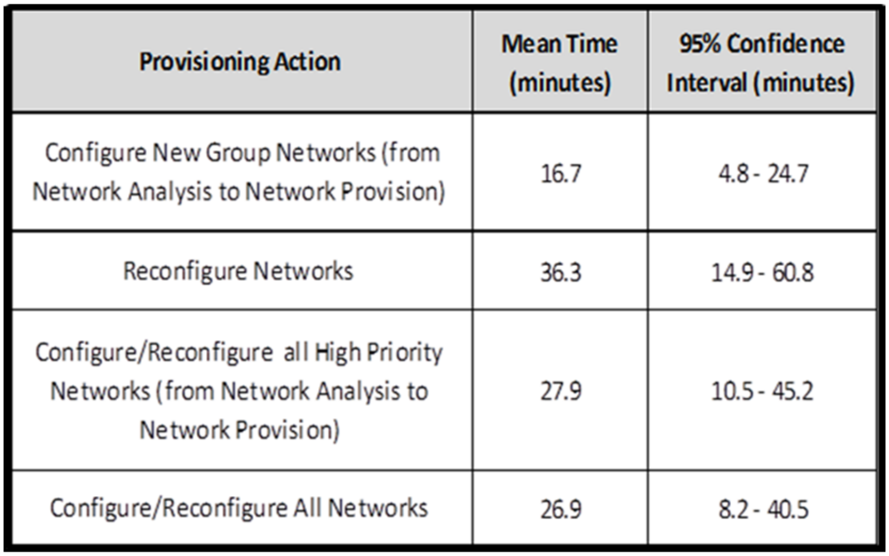
The MUOS waveform lacks a Dynamic Host Configuration Protocol (DHCP) capability that assigns unused IP addresses from MUOS radios to their attached computers used for processing data communications. Unit planners have to manually assign static IP addresses to connect the MUOS radios to IP devices such as SIPRNet or NIPRNet computers. If the connected devices are moved and paired with a different radio or a new device is connected to the radio. When this occurs, unit planners have to manually reconfigure the IP addresses to enable the radio to communicate with the connected device. This can be especially problematic when unit planners do not have authorization to reconfigure computers, such as those computers fielded through the Navy Marine Corps Intranet program. The Navy should implement a DHCP capability in the MUOS waveform to enable dynamic IP assignments for connected devices.

Group Network Provisioning (KPP)

MUOS does not meet the KPP threshold criterion to configure and reconfigure high-priority networks in 5 minutes, and routine networks in 15 minutes. The user definition of configuring and reconfiguring networks includes planning, allocating, and prioritizing accesses to resources. As discussed earlier, the group network provisioning process is a four-step process comprised of inputting the satellite access request (SAR) into MUOS, performing network analysis, approving the network, and provisioning the network.

The Navy asserts that the KPP only involves the final step in the group provisioning process – provisioning. This merely involves pressing the provision button in the MUOS PlanProvApp and waiting for the system to accept it and render a result. This completely ignores evaluating the plan against available resources and allocating the resources. Therefore, it does not meet the definition in the user requirements document. The mean time to provision high-priority users, using the Navy method, was 5.2 minutes (2.8 – 7.6 minutes at the 95 percent confidence level) against the 5-minute criterion.

Table 3-6. Group Mean Configuration Times



Provisioning Action	Mean Time (minutes)	95% Confidence Interval (minutes)
Configure New Group Networks (from Network Analysis to Network Provision)	16.7	4.8 - 24.7
Reconfigure Networks	36.3	14.9 - 60.8
Configure/Reconfigure all High Priority Networks (from Network Analysis to Network Provision)	27.9	10.5 - 45.2
Configure/Reconfigure All Networks	26.9	8.2 - 40.5

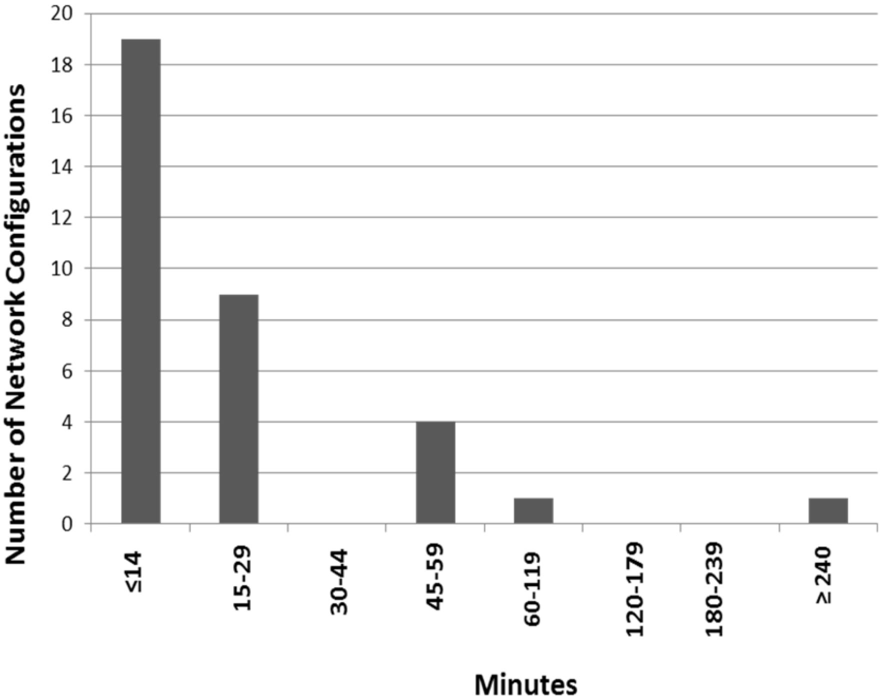


Figure 3-3. Distribution of High Priority Configurations and Reconfigurations

A measure that more accurately meets the user-defined requirement must include network analysis – a network cannot be provisioned without first performing analysis and determining if resources are available. As Table 3-6 displays, with network analysis included, the mean provisioning time for high-priority networks is 27.9 minutes (10.5 – 45.2 minutes at the

95 percent confidence interval). The RSSC-West resource planners performed a total of 54 configurations or reconfigurations during the test, 40 of which were high-priority. Five of the high priority group provisions failed and did not have associated times, and DOT&E discarded one of the group configuration times as an outlier because it took over six days to complete. Figure 3-3 shows the distribution of the remaining 37 high-priority configuration and reconfiguration times. Four high-priority network reconfigurations took 5 minutes or less. These were relatively simple changes, such as lowering the data rate of the network. No new network configurations took 5 minutes or less. Two high-priority network provisions took long times to complete; one network creation took 101 minutes, and one reconfiguration took 6 hours, 11 minutes.

The network analysis "engine" could often take 30 minutes or more to complete. On average, network analysis took 13 minutes, 45 seconds of the total provisioning time. The analysis sometimes failed to complete and required the planner to close the application and restart the process. The Navy was aware of the analysis engine timeouts and lock-ups from at least October 2014, when it performed an Independent Contractor Assessment developmental test event and briefed the results to the Navy's development contractors. The SMDC/ARSTRAT resource planners experienced the same problems in the Navy's June 2015 Technical Evaluation. The Navy should perform root cause analysis and correct the underlying problems causing the routine analysis engine failures. Additionally, the Navy should conduct loading testing and analysis to determine analysis engine performance based on the Capabilities Production Document's Communication Service Requirements and on multiple RSSCs analyzing networks simultaneously. The Navy should resolve any discovered performance constraints.

When network analysis does complete, the system renders a "Likelihood of Success" of high, medium, or low for the provisioned group network to the resource planner. There is no system feedback, documentation, or training provided that informs the planners how the system determines Likelihood of Success or what the planners can do to improve a network's likelihood of success. Since the Likelihood of Success has no context it has little meaning to the planner. What the planners do know is that the rendered Likelihood of Success is not necessarily accurate. There are problems with how the system determines Likelihood of Success. For example, Problem Report 297980, generated September 2015, shows that the analysis engine uses a hard-coded gain value rather than the range of possible values MUOS selects from. This could lead to user terminals being provisioned to a satellite beam carrier that they couldn't actually use, resulting in failed communications. The application also predicts capacity resource usage differently than the MUOS actual usage, leading to erroneous Likelihood of Success results. The Navy should fix the problems with how MUOS determines group network Likelihood of Success. The Navy should also either provide resource planners guidance on how group network Likelihood of Success is determined, to include recommending planning steps they can take to improve poor outcomes through automated means, or update the Interactive Electronic Technical Manuals (IETMs). There are a number of suitability problems with the planning and provisioning application discussed in Section Four of this report.

The system forces resource planners to perform network analysis on one group network at a time, serially. DOT&E observed that failures often occur when the planners queue two or more group networks in the system, even though the networks may be in different geographic regions using different MUOS resources. Because of this, the RSSC resource planners perform analyses one at a time for each request and in the order the requests are received. There is no mechanism to prioritize high-priority requests. The RSSC resource planners must be told by the user that the request is high-priority and have the priority approved by SMDC/ARSTRAT. Then they manually search the queue – which may contain hundreds of requests – to find the high-priority request and pull it out of queue to service it. The Navy should provide the resource planners an automated means to prioritize network provisioning.

Unless the problems are fixed, system performance can only get worse when there are thousands of group networks to analyze resources against and four RSSCs using the provisioning tool simultaneously. According to emerging doctrine at the Army's Cyber Center of Excellence, a brigade combat team may have as many as 65 group networks. When the Army completes its reorganization it will have 33 brigade combat teams, resulting in at least 2,200 active group networks.

As Table 3-7 shows, the RSSC-West resource planners were able to successfully create 83.3 percent (45 of 54) of all group network configurations and reconfigurations, with an 80.0 percent confidence interval of 71.1 to 90.9 percent. The resource planners were able to successfully complete high-priority group configurations 86.0 (37 of 43) percent of the time and successfully complete standard-priority group configurations 72.7 percent (8 of 11) of the time.

Table 3-7. Summary of Group Network Provisioning Results

Configuration Type	Attempts	Successes	Failures	Pass Rate Percentage	80% C.I. (Percent)
All Group Configurations/Reconfigurations					
New Group Network Configurations	24	22	2	91.7	73.9 - 97.4
Group Network Reconfigurations	30	23	7	76.7	58.9 - 88.1
All Group Configurations/Reconfigurations	**54**	**45**	**9**	**83.3**	**71.1 - 90.9**
Configurations/Reconfigurations by Priority					
High Priority	43	37	6	86.0	72.6 - 93.4
Standard Priority	11	8	3	72.7	42.8 - 90.1
All Group Configurations/Reconfigurations	**54**	**45**	**9**	**83.3**	**71.1 - 90.9**

C.I. – Confidence Interval

The RSSC resource planners successfully created new group networks 91.7 percent (22 of 24) of the time, with an 80.0 percent confidence interval of 73.9 to 97.0 percent. Group reconfigurations are changes to, and re-provisioning of, existing group networks. The RSSC planners were successful 76.7 percent (23 of 30) of the time performing reconfigurations, with an 80.0 percent confidence interval of 58.9 to 88.1 percent.

Two of the new group network configurations failed in the network analysis step because the MUOS PlanProvApp, which resource managers use to perform network analysis, never completed. The system remained in "analyzing results – status not available." When a configuration or reconfiguration fails, the resource planner has to exit the application and start the process over.

Two of the seven reconfigurations failed when the Home Location Register – Authentication (HLR-AuC) went down in the Northwest Switching Facility (SF). While the network managers received an alarm event, the RSSC planner wasn't notified by the network managers that the HLR-AuC was down and they wouldn't be able to provision. Given the problems at the NMS and the chain of events that transpired, it seems clear the NMS personnel were not aware of the consequences of the HLR-AuC failure.

The HLR-AuC is a central database that contains details of each MUOS terminal and authorizes the terminals to enter and use MUOS. It is a key component and single point of failure in the MUOS architecture. When it is not working, new users cannot register with the network, terminal rekeys cannot occur, and the provisioning of new networks or reconfiguration of existing networks cannot occur. Group networks that need no configuration changes or users added or deleted can continue to operate normally until a rekey event (weekly) or other change is required.

The first indication to the RSSC resource planners that there was a failure that prohibited group provisioning was when the two group reconfigurations failed on November 9, 2015. The Northwest HLR-AuC had actually failed on November 3, 2015, six days earlier. The MUOS network managers submitted a PRI-2 trouble ticket (#155437) requesting depot-level support with an operational impact statement of, "unknown but possible operational and crypto key management outage." The trouble ticket also requested documentation updates so they could identify and troubleshoot the problem in the future. Between the initial trouble ticket and resolution of the problem on November 9, 2015, the Network Managers submitted at least 16 more trouble tickets related to this problem. Besides the HLR-AuC failure, there were four other times during MOT&E-2 when system failures prevented the RSSC planners from provisioning groups.

- On October 19 – 20, 2015, the message brokering servers at the NMS required rebooting, resulting in an outage of at least 7 hours, 18 minutes.
- On October 30, 2015, the Certificate Revocation Lists expired, causing an outage of 4 hours until the network management facility (NMF) System Administrator could obtain new certificate revocation lists and load them into the system.
- On November 17, 2015, group provisioning failed across the entire system because the Operating System Support –Radio and Core (OSS-RC) was inaccessible. The OSS-RC functions as the NMF's operating system. It is designed to manage, configure, monitor, and troubleshoot the MUOS ground system networks. The NMF submitted a trouble ticket and on-site depot support took 4 hours, 2 minutes to resolve the problem.

Long provisioning outages continue to plague MUOS. Since MOT&E-2, the MUOS Program Manager has tracked provisioning outages. The MUOS provisioning capability has been down 99,420 minutes over that timeframe, the equivalent of 69 days from December 2015 to March 3, 2016. The Navy determined the provisioning availability was 55.7 percent in January, 0.0 percent in February, and 7.1 percent in March 2016. While availability is typically a suitability metric, poor availability has a direct and negative consequence on operational effectiveness. If provisioners can't access the system, then they are incapable of provisioning radios. If they cannot provision radios, then operational units cannot access the system and conduct mission communications when they need.

As discussed, there is no MUOS CONOPS, procedure, or system for the MUOS network managers or satellite controllers to notify the RSSC resource planners, Satellite Operational Manager, Satellite System Expert, provisioners, and deployed users of outages or system degradations and their operational effects. The Navy, in coordination with USSTRATCOM, should develop an outage notification system and tool to notify MUOS stakeholders of system outages and degradations with an assessment of the associated operational effects.

Terminal Provisioning

Soldiers in MOT&E-2 were able to successfully provision their terminals in 64.2 percent (61 of 95) of attempts, with a 95 percent confident interval between 42.3 and 68.4 percent. As Table 3-8 shows, when provisioning worked, soldiers took on average 26.4 minutes to complete the provisioning of their terminals. There is no user-defined time requirement levied on MUOS for provisioning. However, the provisioning time requirement of 11 minutes for the HMS Manpack terminal was not met.

Table 3-8. Summary of Terminal Provisioning Results

Location	Initial Provisioning Mean Time (minutes)	Operational Provisioning Mean Time (minutes)	Total Terminal Provisioning Mean Time (minutes)	Attempts to Provision	Provisioning Successes	Provisioning Failures	Provisioning Pass Rate Percentage [95% Confidence Interval]
Fort Bragg	9.4	15.8	25.2	40	20	20	50 [33.7 - 66.2]
Fort Drum	15.2	17.3	26.4	34	21	13	61.8 [38.3 - 81.9]
Joint Base Lewis McChord	9.3	17.9	27.6	21	20	1	95.2 [76.0 - 99.8]
AGGREGATE	**11.3**	**17.0**	**26.4**	**95**	**61**	**34**	**64.2** **[42.3 - 68.4]**

Terminal provisioning takes place at the unit locations and is the final step in preparing the terminals to communicate with MUOS. The MUOS user-defined requirement is that the system must provide initial network parameters via a digital storage device. MUOS met this user-defined requirement, but the requirement lacks operational significance. The Navy should explore trades with the other Services' terminal offices to reduce the overall terminal provisioning time and to increase terminal provisioning success rates.

Initial provisioning was performed at the unit level at Fort Bragg, Fort Drum, and Joint Base Lewis McChord (JBLM) by unit planners. Initial provisioning began by directly connecting the Simple Key Loader and Joint Enterprise Network Manager, and transferring the respective crypto-key material and MUOS profile information – including the group configuration data – to the MUOS terminal. Initial provisioning ended by powering on the terminal, performing a terminal self-test, and logging into MUOS. Operational provisioning involved the downloading of the remaining profile parameters from the MUOS ground system through the satellites. Depending on the planned configurations, the thousands of parameters can be downloaded via over-the-air file transfer (OTA-FT) from MUOS to the terminal.

All 34 of the provisioning failures that occurred across the three sites happened during operational provisioning, when the MUOS terminals attempted to download via OTA-FT. Initial provisioning took 11.3 minutes on average for the 95 attempts to provision. The 61 successful OTA-FTs took 17.0 minutes on average across the three sites. When provisioning failed, the soldiers started the terminal provision process over from initial provisioning. The testers stopped tracking time because the soldiers took time to troubleshoot, discussed how to proceed, and ultimately decided to start from the beginning because it could not be determined how the failures occurred. The provision re-attempt was often made after a long break – trying after troubleshooting or when the terminal could obtain a stronger satellite signal.

The testers observed a high number of provisioning failures at Fort Bragg (50.0 percent) and Fort Drum (38.2 percent) compared to JBLM (4.8 percent). These failures may have been due to "mobility events" where the terminals lost communications with the CONUS satellite and never recovered. The terminals at Forts Bragg and Drum were in the field of view of one satellite, and that satellite was in a degraded mode (see classified annex). The terminals at JBLM were in the field of view of two satellites and experienced far better success rates. MUOS earth coverage envisions that 35 percent of the MUOS footprint will provide a field of view to a single satellite, so failures may be a common occurrence in these areas. The Navy should further investigate the differences in terminal provisioning performances observed during the MOT&E, including terminals provisioning with a single satellite field of view and terminals provisioning in a two satellite field of view.

Spectrum Adaptive (SA)-Wideband Code Division Multiple Access (WCDMA) Communications

When available, MUOS provided SA-WCDMA voice communications to deployed users; however, during the majority of the testing there were limited or widespread communications outages that could result in failed operational missions. MUOS demonstrated that the SA-WCDMA communications provide better voice accuracy and quality than the legacy ultra high frequency (UHF) dedicated channels that MUOS provides as a secondary payload on each satellite.[22] MUOS demonstrated the ability to transfer data between users and with the DISN at rates up to 64 kbps.

Voice Communications

As discussed previously under the Test Adequacy section in this report, COTF conducted MOT&E-2 through execution of 952 mission scenarios, transmitting over 271 established group

[22] DOT&E determined that the UHF payload on MUOS provides better quality communications than a UHF Follow-On (UFO) satellite (*Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation Report*, January 2013).

networks with 4,609 individual terminal transmissions, to evaluate the diversity of factors that could affect performance of MUOS. The test team also conducted a comparative test of 341 Legacy UHF transmissions to compare the Legacy UHF performance with that of MUOS under the different terrain types. DOT&E used four metrics to evaluate the accuracy and quality of MUOS voice communications: Link Probability of Effective Communications, Voice (PECV); Message Accuracy; User Rating of Loudness and Clarity; and Group PECV. User Rating of Loudness and Clarity is a measure of quality of service while the other metrics are measures of accuracy.

Comparison of MUOS SA-WCDMA to Dedicated Legacy UHF

Table 3-9 displays the comparison of SA-WCDMA performance to legacy UHF performance over a single link. Functionally, a single link is P2P network topography, so there are no Group PECV results. MUOS SA-WCDMA performed better in message accuracy and user rating over legacy UHF.

The differences in SA-WCDMA message accuracy and user rating over legacy UHF results are statistically significant (p-values are less than 0.01).[23] The slight difference in performance between Link PECV for SA-WCDMA and legacy UHF is not significant. MUOS SA-WCDMA provides better message accuracy and quality of service than legacy UHF. There is no specified user criterion that compares MUOS SA-WCDMA performance to legacy UHF performance.

Table 3-9. SA-WCDMA and Legacy UHF Single Link Performance

Response Variable	SA-WCDMA [95% Confidence Interval]	Legacy [95% Confidence Interval]
Link PECV	**0.96** [0.956 - 0.97]	**0.95** [0.92 - 0.97]
Message Accuracy	**0.68** [0.67 - 0.69]	**0.47** [0.42 - 0.52]
User Rating	**0.93** [0.92 - 0.934]	**0.83** [0.79 - 0.87]

SA-WCDMA – Spectrum Adaptive-Wideband Code Division Multiple Access;
PECV – Probability of Effective Communications, Voice

Likewise, MUOS SA-WCDMA performance in group networks compares favorably to the legacy UHF communications. Table 3-10 shows the results for four group sizes that represent platoon through brigade combat team (BCT) networks.[24]

[23] P-values are the probability of obtaining a result equal to or more extreme than what was observed. A low p-value indicates a convincing statistical argument that there is a difference between the levels being tested (MUOS WCDMA and Legacy UHF). For this report, a p-value of 0.01 or less is considered "low."

[24] The test team collected group network performance data for group sizes ranging from 2 to 38 participants. DOT&E chose to report results based on Army echelon network sizes because they are operationally meaningful.

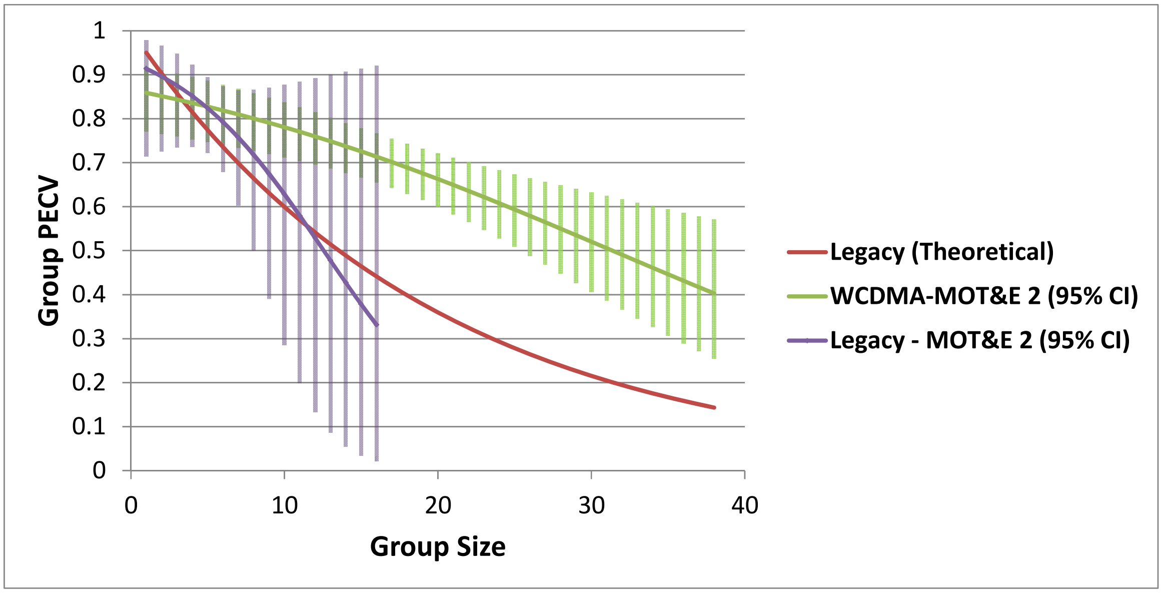
Table 3-10. SA-WCDMA and Legacy Group Communications Performance

Group Size (# of users)	Group PECV [95% Confidence Interval]			
	Sample Size	SA-WCDMA	Actual Legacy	Theoretical Legacy
Platoon (4)	271 (SA-WCDMA) 80 (Legacy)	**0.85** [0.75 - 0.93]	**0.88** [0.69 - 0.98]	**.82**
Company (13)		**0.74** [0.65 - 0.83]	**0.38** [0.08 - 0.93]	**.51**
Battalion (16)		**0.71** [0.61 - 0.79]		**.46**
Brigade (31)		**0.43** [0.38 - 0.66]		**.21**

SA-WCDMA – Spectrum Adaptive-Wideband Code Division Multiple Access; PECV – Probability of Effective Communications, Voice
Note: There are no data for legacy ultra high frequency (UHF) groups larger than 16.

COTF collected a small amount of legacy UHF data for groups larger than 8 participants and did not collect any legacy UHF data for groups larger than 16 participants, as indicated by the darkened grey box in Table 3-10. This prevented DOT&E from directly comparing MUOS Group PECV to legacy UHF network PECV for battalion and BCT command networks. Based on the available data, DOT&E was able to model legacy UHF group performance for the larger networks by projecting the probability of success for a single link (Link PECV for legacy UHF) to larger groups. The "Theoretical Legacy" column in Table 3-10 shows the results of this modeling.

Figure 3-4 displays the theoretical and actual performance curves for legacy UHF compared to actual SA-WCDMA Group PECV during MOT&E-2. The green line shown in the figure is the Group SA-WCDMA performance, the purple line is the actual legacy UHF group performance and the red line is the modeled UHF performance. The green and purple horizontal lines display the 95 percent confidence intervals and represent uncertainty with the results. Since there were fewer legacy UHF group calls made, the uncertainty for UHF is larger than the SA-WCDMA performance uncertainty. MUOS SA-WCDMA group service performs significantly better than the theoretical legacy UHF group networks.



PECV – Probability of Effective Communications, Voice; SA-WCDMA – Spectrum Adaptive-Wideband Code Division Multiple Access; MOT&E 2 – second Multi-Service Operational Test and Evaluation; CI – Confidence Interval; UHF – ultra high frequency

Figure 3-4. Comparison of Group SA-WCDMA to Legacy UHF Performance

MUOS Voice Communications Quality

DOT&E characterized MUOS Group and Link PECV performance based on Army operational unit group sizes and across different terrain types. Table 3-11 summarizes these results.

Table 3-11. Group and Link PECV by Group Size and Transmitter Terrain

Operational Group (Network Size)	Group PECV [95% Confidence Interval]			Link PECV [95% Confidence Interval]		
	Clear	Forest	Urban	Clear	Forest	Urban
Platoon (4)	**0.92** [0.74 - 0.98]	**0.59** [0.34 - 0.80]	**0.98** [0.88 - 0.99]	**0.99** [0.95 - 0.995]	**0.93** [0.82 - 0.97]	**0.995** [0.98 - 0.999]
Company (13)	**0.78** [0.61 - 0.89]	**0.64** [0.47 - 0.78]	**0.89** [0.74 - 0.96]	**0.97** [0.94 - 0.99]	**0.96** [0.91 - 0.98]	**0.99** [0.97 - 0.997]
Battalion (16)	**0.72** [0.54 - 0.84]	**0.66** [0.49 - 0.79]	**0.84** [0.67 - 0.93]	**0.97** [0.93 - 0.99]	**0.97** [0.92 - 0.99]	**0.99** [0.97 - 0.996]
Brigade (31)	**0.28** [0.09 - 0.60]	**0.74** [0.43 - 0.91]	**0.28** [0.12 - 0.54]	**0.92** [0.82 - 0.97]	**0.99** [0.96 - 0.996]	**0.97** [0.93 - 0.99]

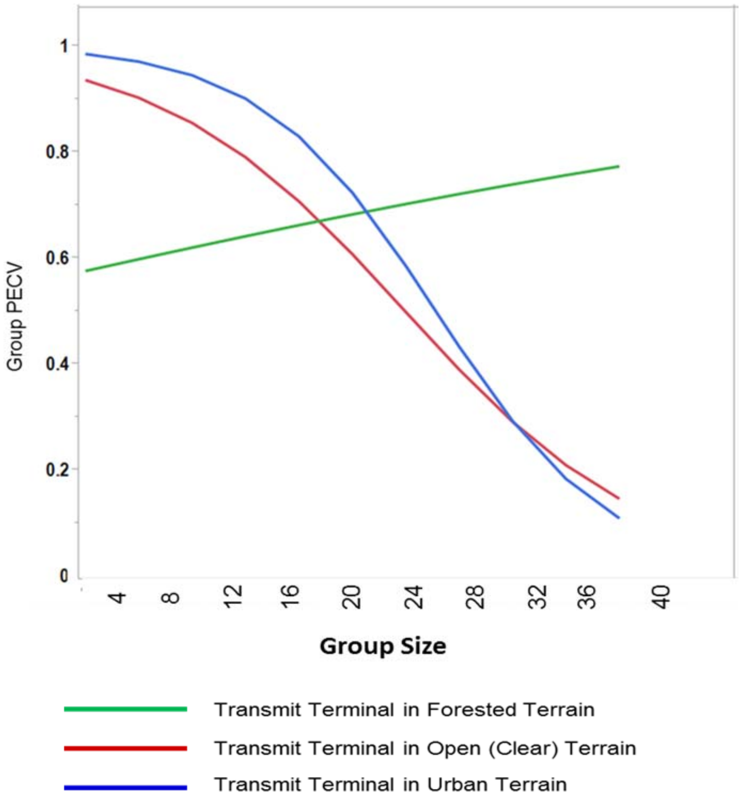
PECV – Probability of Effective Communications, Voice

A successful PECV transmission occurs when a transmitted voice message is correctly received and understood by the receiving terminal operator. There is no user-specified criterion for PECV. The user defined criteria for Group and P2P voice communication simply states that MUOS must provide netted (Group) and P2P (Link) voice services with the expectation that MUOS will do this in challenging terrain, including urban and forested terrain.

The numbers depicted under the Link PECV in Table 3-11 show the probability that the receiving terminal operator will correctly receive and understand a transmission. Similarly, the numbers under Group PECV show the likelihood that all members in a network received the message correctly. DOT&E evaluated 271 group communication transmissions and 4,609 individual link transmissions from MOT&E-2.

The MUOS SA-WCDMA communications performed as DOT&E expected in clear and urban terrain. Functionally, each group network is comprised of individual links, so as more members are added to groups, the likelihood that all members of a group will receive a transmission naturally grows worse.

However, when the transmitter initiates calls from forested terrain, where the MUOS signal is attenuated, the performance improves as the group size grows. For example, Group PECV in forested terrain for a company command network of 13 participants was 64 percent, while Group PECV in forested terrain for a BCT command network of 31 participants was 74 percent. So, while the transmitting terminal was in forested terrain, the receiving terminals were in combinations of open, forested and urban terrains. DOT&E observed similar results when evaluating message accuracy and user rating.



PECV – Probability of Effective Communications, Voice

Figure 3-5. Group Performance Improvement in Forested Terrain

This effect is clearly shown graphically in Figure 3-5. Group PECV with the transit terminal in forested terrain is depicted by the green line. Group PECVs with the transmit terminals in clear and urban terrain are depicted by the red and blue lines, respectively.

DOT&E believes this behavior is a cumulative effect of the open loop power control functions in MUOS. In open loop power control the transmitting terminal sets the output power for initial uplink and downlink transmissions. If the signal is attenuated, then the transmitter increases the power levels for all members in that group and all members benefit whether or not they are in challenging terrain.

The Navy increased the open loop power control stress margin just prior to MOT&E-2 in order to improve call performance. However, increasing the stress margin and boosting the signal consumes additional power and reduces overall capacity. While this had no negative effects for the relatively small number of terminals in the test event, it may have unintended operational effects when MUOS has to service the full communications requirements. The C-SSE has expressed concerns about the performance and planning constraints to future operations. The Navy, in coordination with USSTRATCOM, should model the power control parameter effects on call performance and system capacity when MUOS is at the full communications service requirements.

MUOS Voice Communications by Service Type

MUOS is able to support group, point-to-point (P2P), and point-to-network (P2N) networks. DOT&E found no significant performance difference between group, P2P, and P2N communications services that MUOS provides. The user-defined criterion is simply that MUOS must support broadcast (P2N), point-to-point (P2N) and netted topologies. COTF categorized MUOS calls to the Defense Switched Network (DSN) telephones as a P2N topology.

Table 3-12. Summary of MUOS Communication Services Results.

MUOS Communication Service	Sample Size	Link PECV [95% CI]	Message Accuracy [95% CI]	User Rating [95% CI]
Group	4414	**0.96** [0.956 - .967]	**0.68** [0.66 - 0.69]	**0.93** [0.92 - 0.94]
Point to Point	195	**0.98** [0.95 - 0.99]	**0.68** [0.61 - 0.74]	**0.92** [0.87 - 0.95]
Point to Net (MUOS to DSN)	113	**0.94** [0.88 - 0.97]	**0.73** [0.64 - 0.81]	**0.91** [0.84 - 0.95]

PECV – Probability of Effective Communications, Voice; CI – Confidence Interval; DSN – Defense Switched Network

Table 3-12 summarizes the MUOS communication service results. There are a large proportionate of group network samples compared to P2P and P2N samples. The Army intends to primarily use MUOS for beyond-line-of-sight group networks and therefore COTF made this a focal point for the MOT&E-2. DOT&E expected the similar results between group, P2P, and P2N networks. Functionally, there is no difference between a group service with two members communicating and a P2P service. The Navy's June 2015 Technical Evaluation had similar results.

MUOS Voice Encoding

MUOS supports speaker recognition voice services. The user-defined threshold criterion is that MUOS must support speaker recognition for selected circuits for important users, with a Mean Opinion Score (MOS) of 4x4, or better. The Navy implemented this capability through the use of voice encoders that turn analog voice transmissions into binary data. Conversational voice is lower fidelity and uses 2.4 kbps, compared to higher fidelity voice recognition that uses 9.6 kbps. Table 3-13 summarizes the MOT&E results for voice encoding type.

Table 3-13. Summary of MOT&E Voice Encoding Type Results

Voice Encoder	Sample Size	Link PECV [95% CI]	Message Accuracy [95% CI]	User Rating [95% CI]
Conversational	1555	**0.96** [0.95, 0.97]	**0.64** [0.61, 0.66]	**0.93** [0.91, 0.94]
Recognition	2907	**0.96** [0.95, 0.97]	**0.70** [0.69, 0.72]	**0.93** [0.92, 0.94]

PECV – Probability of Effective Communications, Voice; CI –Confidence Interval

DOT&E found that terminal operators could not tell the difference between the two different types of voice encoders used by MUOS. The user rating score of 0.93 for both conversational and recognition voice encoder means that 93 percent of operator responses rated the MUOS quality of service as 5x5 (loud and clear). There is no statistical difference between user rating scores or Link PECV scores between the two voice encoders. DOT&E found that only in the most granular response, message accuracy, is there a statistically significant difference in performance between the voice encoders. Using voice recognition consumes additional bandwidth and reduces the number of users that can access the system, with little benefit. The current default setting in MUOS is set at voice recognition (9.6 kbps), when conversational voice (2.4 kbps) would suffice for most missions. The Navy should make conversational voice (2.4 kbps) the MUOS default setting for provisioning voice communications, instead of the current default of voice recognition (9.6 kbps), so as not to waste satellite resources.

WCDMA Communications Path

SA-WCDMA communications can take six different paths through MUOS, depending on transmitter and receiver location. The user-defined threshold criterion is that MUOS must support communications between users located in different MUOS satellite footprints, as well as between and within different satellite beams of the same satellite. The possible communications paths between MUOS users are:

- Same Satellite/Same Satellite Beam/Same Radio Access Facility (RAF)
- Same Satellite/Same Satellite Beam/Different RAF
- Same Satellite/Different Satellite Beam/Same RAF

- Same Satellite/Different Satellite Beam/Different RAF
- Different Satellite/Different Satellite Beam/Same RAF
- Different Satellite/Different Satellite Beam/Different RAF

DOT&E found no significant statistical difference in performance when MUOS communications were routed through different spot beams on the same satellite, different satellites, or through different RAFs. The communication path is not a controllable factor during an operational test. MUOS chooses the routing path between users in such a way that balances user load across the system. COTF did not collect enough data to model one of the factor levels (Different Satellite/Different Satellite Beam/Same RAF). Table 3-14 summarizes the results of the other five communications paths.

Table 3-14. Summary of MUOS Communication Path Results

Communications Path	Sample Size	Link PECV [95% CI]	Message Accuracy [95% CI]	User Rating [95% CI]
Different Satellite, Different Beam, Different RAF	975	**0.96** [0.95 - 0.97]	**0.72** [0.69 - 0.75]	**0.92** [0.90 - 0.93]
Same Satellite, Different Beam, Different RAF	78	**0.94** [0.86 - 0.97]	**0.69** [0.58 - 0.79]	**0.92** [0.84 - 0.97]
Same Satellite, Different Beam, Same RAF	451	**0.97** [0.95 - 0.98]	**0.68** [0.64 - 0.72]	**0.93** [0.90 - 0.95]
Same Satellite Same Beam, Different RAF	72	**0.94** [0.86 - 0.98]	**0.68** [0.57 - 0.78]	**0.90** [0.81 - 0.95]
Same Satellite, Same Beam, Same RAF	2885	**0.97** [0.96 - 0.97]	**0.67** [0.65 - 0.68]	**0.94** [0.93 - 0.95]

PECV – Probability of Effective Communications, Voice; CI – Confidence Interval; RAF – Radio Access Facility

SA-WCDMA Voice Intelligibility

COTF tested voice intelligibility using two methods prescribed by the MUOS Capability Production Document: the Diagnostic Rhyme Test (DRT) and the MOS test.[25] The user-defined threshold requirement for DRT is that MUOS must support intelligible voice services, with a DRT of 75 percent or greater in an extremely noisy environment, and 92 percent or greater in a quiet, error-free environment. The threshold for MOS is that MUOS must support acceptable voice services with a MOS value of 3.1 or greater in a noisy environment, and 3.8 or greater in a

[25] Capability Production Document for Joint Satellite Communications (SATCOM) Mobile User Objective System (MUOS) Increment 1, January 15, 2008.

quiet, error-free environment. The user-defined noisy environment is described as being in or near a High Mobility Multipurpose Wheeled Vehicle (HMMWV).

DOT&E found that evaluating voice quality using a commercial telephony standard like DRT was not useful in evaluating MUOS. DRT like-sounding word pairs did not provide a mission context to determine whether MUOS provided communications of a high enough quality to convey mission-critical information.

Table 3-15 summarizes the DRT and MOS scores for noisy and quiet environments. DOT&E found no statistically significant difference between MUOS communications in noisy and quiet environments using DRT data. COTF conducted modified MOS testing using the scales previously discussed in this report. DOT&E found no statistically significant difference between quiet and noisy environments for voice volume and voice clarity.

Table 3-15. Diagnostic Rhyme Test and Modified Mean Opinion Score Results

Ambient Noise	Diagnostic Rhyme Test (DRT)		Mean Opinion Score (MOS)		
	Samples	Score [95% CI]	Samples	Volume [95% CI]	Clarity [95% CI]
Quiet	12	**0.85** [0.83 – 0.87]	2535	**4.89** [4.86 – 4.91]	**4.87** [4.84 – 4.89]
Noisy	33	**0.88** [0.84 – 0.92]	1848	**4.87** [4.83 – 4.90]	**4.82** [4.79 – 4.86]

CI – Confidence Interval

Communications-on-the-Move (COTM)

The MUOS and AN/PRC-155 radios demonstrated the ability to provide COTM to users. COTF tested the ability of MUOS to provide COTM by using AN/PRC-155 Manpack in vehicle-on-the-move and soldier-on-the-move configurations. Due to the available configurations, COTF could only test these radios at speeds limited to 40 miles per hour and below. Table 3-16 summarizes the group size performance results based upon transmit speed. The differences in performance based on transmit speeds are not statistically significant.

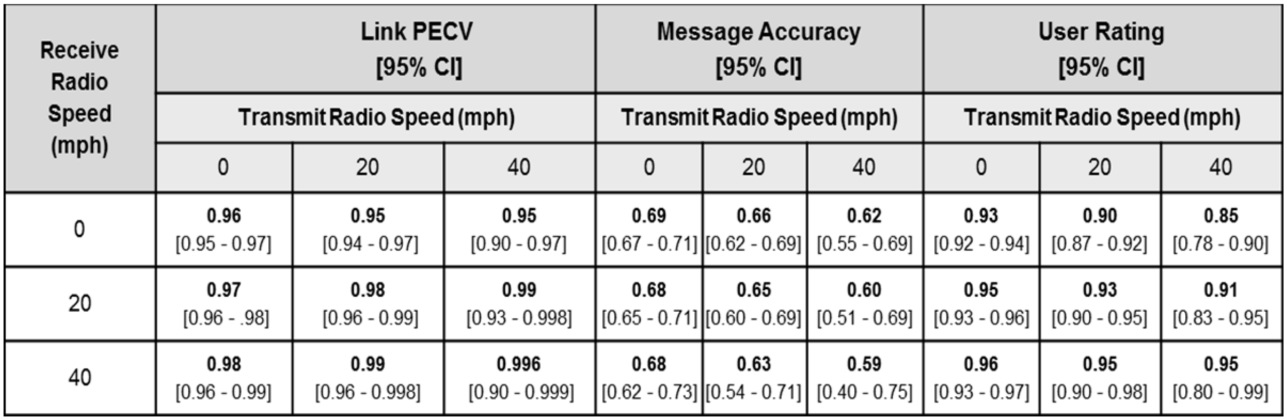
Table 3-16. Summary of Group Size and Transmit Speed Results

Operational Unit (Group Size)	Group PECV [95% Confidence interval]		
	Transmit Radio Speed (miles per hour)		
	0	20	40
Platoon (4)	**0.81** [0.62 - 0.92]	**0.96** [0.76 - 0.99]	**0.99** [0.70 - 0.999]
Company (13)	**0.70** [0.57 - 0.81]	**0.81** [0.60 - 0.92]	**0.88** [0.50 - 0.98]
Battalion (16)	**0.65** [0.53 - 0.76]	**0.71** [0.50 - 0.85]	**0.75** [0.34 - 0.95]
Brigade (31)	**0.40** [0.19 - 0.65]	**0.14** [0.02 - 0.59]	**0.04** [0.00 - 0.75]

PECV – Probability of Effective Communications, Voice

Table 3-17 below, summarizes the results of Link PECV, message accuracy and user rating based on receive speed. DOT&E analysis determined that receive speed has a statistically significant effect on user rating of quality. However, environmental noise may be a contributing and confounded factor with receive speed because data are collected in HMMWVs, where the noise increases as speed increases.

Table 3-17. Summary of Receive Speed Results



Receive Radio Speed (mph)	Link PECV [95% CI]			Message Accuracy [95% CI]			User Rating [95% CI]		
	Transmit Radio Speed (mph)			Transmit Radio Speed (mph)			Transmit Radio Speed (mph)		
	0	20	40	0	20	40	0	20	40
0	**0.96** [0.95 - 0.97]	**0.95** [0.94 - 0.97]	**0.95** [0.90 - 0.97]	**0.69** [0.67 - 0.71]	**0.66** [0.62 - 0.69]	**0.62** [0.55 - 0.69]	**0.93** [0.92 - 0.94]	**0.90** [0.87 - 0.92]	**0.85** [0.78 - 0.90]
20	**0.97** [0.96 - .98]	**0.98** [0.96 - 0.99]	**0.99** [0.93 - 0.998]	**0.68** [0.65 - 0.71]	**0.65** [0.60 - 0.69]	**0.60** [0.51 - 0.69]	**0.95** [0.93 - 0.96]	**0.93** [0.90 - 0.95]	**0.91** [0.83 - 0.95]
40	**0.98** [0.96 - 0.99]	**0.99** [0.96 - 0.998]	**0.996** [0.90 - 0.999]	**0.68** [0.62 - 0.73]	**0.63** [0.54 - 0.71]	**0.59** [0.40 - 0.75]	**0.96** [0.93 - 0.97]	**0.95** [0.90 - 0.98]	**0.95** [0.80 - 0.99]

PECV – Probability of Effective Communications, Voice; CI – Confidence Interval; mph – Miles Per Hour

Mobility

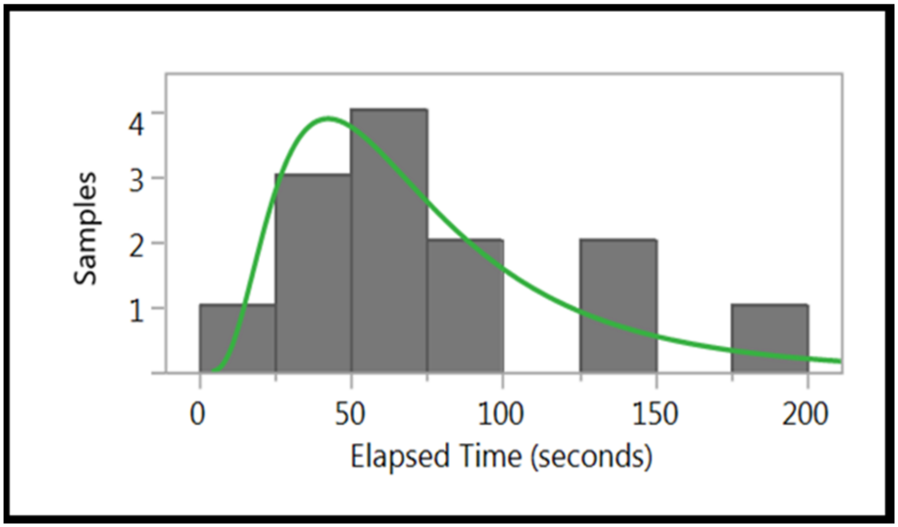
MUOS does not provide the capability for a transparent transfer of communication services as a user transitions between satellite coverage areas and between satellite beams. Terrestrial cellular service handles users moving between cells seamlessly. MUOS does not. MUOS breaks the connection between users when the system determines a transition to a new cell is needed, and then reconnects the users. While the mobility event is occurring the user has a complete loss of communications.

Table 3-18. Duration of Mobility Events During MOT&E-2

Starting Satellite	Starting Satellite Beam Carrier	Ending Satellite	Ending Satellite Beam Carrier	Elapsed Time (seconds)
Pacific	207	CONUS	12	38
Pacific	207	CONUS	30	28
Pacific	207	CONUS	32	23
Pacific	206	CONUS	30	187
Pacific	207	CONUS	13	72
Pacific	46	CONUS	21	98
Pacific	207	CONUS	13	96
Pacific	207	CONUS	31	52
Pacific	207	CONUS	32	50
Pacific	207	CONUS	12	30
Pacific	206	CONUS	13	68
Pacific	207	CONUS	126	125
CONUS	126	Pacific	207	145

CONUS – Continental United States

The AN/PRC-155 Manpack terminal notifies users when one of these mobility events is occurring. Table 3-18 shows that the mean time for a mobility event experience during the MOT&E-2 was 78 seconds. Figure 3-6 displays the lognormal parametric best fit of the distribution times – the 50th percentile value is 64 seconds, while the 10th percentile is 28 seconds and the 90th percentile is 145 seconds. The Navy should explore and implement system improvements so users can transition between satellites and beams seamlessly rather than have communication outages.



Note: Green line displays the lognormal parametric fit

Figure 3-6. Lognormal Distribution of Mobility Event Duration

DOT&E attended the training for the AN/PRC-155 radios and observed that MUOS mobility events are not part of the training for radio operators. The Services should train operators that MUOS breaks the connection and re-establishes it in the new cell, as well as train them on the duration of the outage.

Data Communications

MUOS demonstrated the ability to transfer data between users and with the Defense Information Systems Network (DISN) at data rates up to 64 kbps over the 3 data transport modes of burst, flow, and streaming. Table 3-19 summarizes the data transmission results. There is no specified user threshold criterion for data accuracy or quality. Overall, MUOS demonstrated a probability of successful data transmission of 96 percent, 94.8 – 97.0 percent at the 95 percent confidence level.

DOT&E found that data rate and transmission method had no statistically significant effect on performance of data transfers. MUOS communications service type did have an effect on the performance of MUOS data communications, but this difference may be due to the way point-to-network (P2N) works. The soldiers employed the Army's Command Post of the Future (CPOF) to conduct P2N chat. This network would fail upon initiation or not at all, accounting for a low number of failures. If the chat failed upon login, then no attempts could be made to chat and the testing was postponed until the testers resolved the problem with the CPOF server. In these cases, DOT&E attributed the failure to the CPOF server and did not charge failures to MUOS.

Table 3-19. Summary of Data Transmission Results

MUOS Communication Service Type	Transmission Success [95% Confidence Interval]		
	Transport Type		
	Burst	Flow	Stream
Point-to-Point	**0.92** [0.64 - 0.99]	**0.92** [0.79 - 0.97]	**0.98** [0.89 - 0.997]
Point-to-Network	**0.9999** [0.98 - 1.0]	**0.9998** [0.69 - 1.0]	**0.996** [0.52 - 0.999]
Defense Information Systems Network	**0.90** [0.71 - 0.97]	**0.80** [0.69 - 0.88]	**0.92** [0.81 - 0.97]

Network Management

Network management is a broad range of functions including activities, methods, procedures, and the use of tools to administrate, operate, and reliably maintain computer and communications networks. MUOS network management is based upon the commercial Fault, Configuration, Accounting, Performance, and Security (FCAPS) model.[26] MUOS is complex and operates differently than legacy UHF. Most, if not all, of the MUOS network managers do not fully understand how the system operates. The system was designed by engineers to be run by engineers. The Navy has not prepared the MUOS network managers to be able to manage the system, and what steps the Navy has taken to help the network managers have been haphazard. The MUOS network managers are not able to effectively manage the MUOS network because:

- The system provides fault alert events that are cryptic, prioritized inconsistently across the system, and often excessive.
- The system provides network managers with component status, but there is no means to monitor call status resulting in extended outages.
- The system provides the network managers no means to monitor interconnectivity between sites.
- Additionally, there are numerous suitability issues – discussed in Section Four of this report – that contribute to ineffective operations, including:
  - A high number of unresolved, long-standing high-priority problems
  - Incomplete and inaccurate technical manuals
  - Unsatisfactory training
  - Poor availability
  - Long repair times

[26] FCAPS consists of Fault, Configuration, Accounting, Performance, and Security Management domains.

- A high dependency on depot support

Fault Management

By design, fault management is the focus of MUOS network management. The MUOS fault management system is ineffective because it provides the network managers fault alarm events that are cryptic, inconsistently prioritized, and often excessive. The tool MUOS uses for identifying faults is IBM's Tivoli Netcool (Netcool) application. MUOS has a Netcool instantiation for the For Official Use Only (FOUO) enclave, and another Netcool instantiation for the Secret enclave. The Netcool screens scroll at a variable velocity depending upon how many fault alert events they receive. Sometimes network managers miss the faults, because faults happen often and the system scrolls the problems off the display before network managers notice them.

Figure 3-7 is a screenshot of the FOUO fault management screen – taken during MOT&E-2 on November 18, 2015 – that helps to illustrate the problems. Alert events displayed by the fault management system are representations of Simple Network Management Protocol (SNMP) traps (e.g., "rip2-ers1-nw-rfa is not reachable").[27] The traps are not in plain language and are typically not meaningful to the network managers.

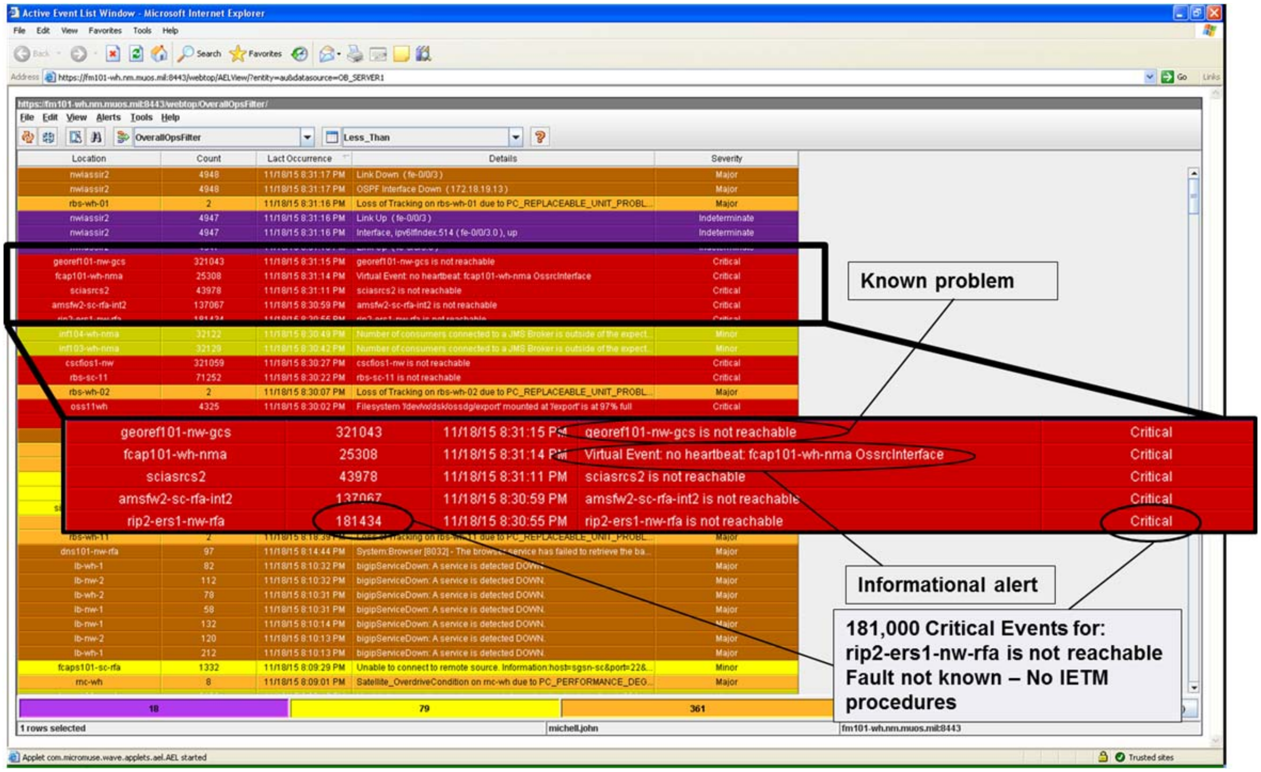
The network managers were overwhelmed by the sheer number of alarm events the SNMP traps sent. The MUOS Program Manager recognized this and applied filtering of alarm events to triage alarm events. The filtering effort is incomplete and arbitrary. The system filters alarm events as Critical, Major, Intermediate, or Minor. The system filters alarm events independently and differently between the FOUO enclave and Secret enclave. A fault that is "critical" on one enclave display may be shown as "informational" on the other enclave display, causing network managers confusion over what actions they should take. An informational alarm event means the network managers do not need to take any specific restorative action.

Alarm events, including critical ones, can display many thousands of times. Figure 3-7 shows "rip2-ers1-nw-rfa is not reachable" as a critical alarm, indicated by the red color and severity listed as critical. Figure 3-7 also shows that this alarm event occurred 181,434 times, raising doubts about its displayed severity. Compounding this problem is that the provided technical manuals often contradict the displayed severity. For example, Figure 3-7 shows the critical alert, "Virtual event: no heartbeat: fcap101-101-wh-nma-OSSRC interface." This alarm event would seem to be actually critical: It references the main server for fault, configuration, administration, and performance management (FCAP101), and also references the Operating System Support – Radio and Core (OSS-RC) server that serves as the primary operating system for the Network Management Segment (NMS). However, when the network managers followed the troubleshooting chart in the Interactive Electronic Technical Manual (IETM) for this event,

[27] Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks, and for modifying that information to change device behavior. Traps enable a component to notify the management station of significant events by way of an unsolicited SNMP message.

the troubleshooting flow chart told them that the fault was "informational only" and to take no action.

There are other problems with alarm events and the IETM. Faults that MUOS identifies as critical are missing from the IETM. Critical faults that are documented do not always have descriptions of the operational effect in the IETM. Critical faults that are documented do not always have methods to resolve the fault. For example, testers asked the network managers to show what corrective action the network managers should take for critical alarm event "rip2-ers1-nw-rfa is not reachable" in Figure 3-7. The network managers showed the testers that there was no procedure in the IETM to resolve this fault.


Active Event List Window - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://fm101-wh.nm.muos.mil:8443/webtop/AELView/?entity=au&datasource=OB_SERVER1
Go Links
https://fm101-wh.nm.muos.mil:8443/webtop/OverallOpsFilter/
File Edit View Alerts Tools Help
OverallOpsFilter
Less_Than

Location	Count	Lact Occurrence	Details	Severity
nwiassir2	4948	11/18/15 8:31:17 PM	Link Down (fe-0/0/3)	Major
nwiassir2	4948	11/18/15 8:31:17 PM	OSPF Interface Down (172.18.19.13)	Major
rbs-wh-01	2	11/18/15 8:31:16 PM	Loss of Tracking on rbs-wh-01 due to PC_REPLACEABLE_UNIT_PROBL...	Major
nwiassir2	4947	11/18/15 8:31:16 PM	Link Up (fe-0/0/3)	Indeterminate
nwiassir2	4947	11/18/15 8:31:16 PM	Interface, ipv6IfIndex.514 (fe-0/0/3.0), up	Indeterminate
georef101-nw-gcs	321043	11/18/15 8:31:15 PM	georef101-nw-gcs is not reachable	Critical
fcap101-wh-nma	25308	11/18/15 8:31:14 PM	Virtual Event: no heartbeat: fcap101-wh-nma OssrcInterface	Critical
sciasrcs2	43978	11/18/15 8:31:11 PM	sciasrcs2 is not reachable	Critical
amsfw2-sc-rfa-int2	137067	11/18/15 8:30:59 PM	amsfw2-sc-rfa-int2 is not reachable	Critical
inf104-wh-nma	32122	11/18/15 8:30:49 PM	Number of consumers connected to a JMS Broker is outside of the expect...	Minor
inf103-wh-nma	32129	11/18/15 8:30:42 PM	Number of consumers connected to a JMS Broker is outside of the expect...	Minor
cscfios1-nw	321059	11/18/15 8:30:27 PM	cscfios1-nw is not reachable	Critical
rbs-sc-11	71252	11/18/15 8:30:22 PM	rbs-sc-11 is not reachable	Critical
rbs-wh-02	2	11/18/15 8:30:07 PM	Loss of Tracking on rbs-wh-02 due to PC_REPLACEABLE_UNIT_PROBL...	Major
oss11wh	4325	11/18/15 8:30:02 PM	Filesystem '/dev/vx/dsk/ossdg/export' mounted at '/export' is at 97% full	Critical
rbs-wh-11	2	11/18/15 8:18:39 PM	Loss of Tracking on rbs-wh-11 due to PC_REPLACEABLE_UNIT_PROBL...	Major
dns101-nw-rfa	97	11/18/15 8:14:44 PM	System:Browser [8032] - The browser service has failed to retrieve the ba...	Major
lb-wh-1	82	11/18/15 8:10:32 PM	bigipServiceDown: A service is detected DOWN.	Major
lb-nw-2	112	11/18/15 8:10:32 PM	bigipServiceDown: A service is detected DOWN.	Major
lb-wh-2	78	11/18/15 8:10:31 PM	bigipServiceDown: A service is detected DOWN.	Major
lb-nw-1	58	11/18/15 8:10:31 PM	bigipServiceDown: A service is detected DOWN.	Major
lb-nw-1	132	11/18/15 8:10:14 PM	bigipServiceDown: A service is detected DOWN.	Major
lb-nw-2	120	11/18/15 8:10:13 PM	bigipServiceDown: A service is detected DOWN.	Major
lb-wh-1	212	11/18/15 8:10:13 PM	bigipServiceDown: A service is detected DOWN.	Major
fcaps101-sc-rfa	1332	11/18/15 8:09:29 PM	Unable to connect to remote source. Information:host=sgsn-sc&port=22&...	Minor
mc-wh	8	11/18/15 8:09:01 PM	Satellite_OverdriveCondition on mc-wh due to PC_PERFORMANCE_DEG...	Major

georef101-nw-gcs	321043	11/18/15 8:31:15 PM	georef101-nw-gcs is not reachable	Critical
fcap101-wh-nma	25308	11/18/15 8:31:14 PM	Virtual Event: no heartbeat: fcap101-wh-nma OssrcInterface	Critical
sciasrcs2	43978	11/18/15 8:31:11 PM	sciasrcs2 is not reachable	Critical
amsfw2-sc-rfa-int2	137067	11/18/15 8:30:59 PM	amsfw2-sc-rfa-int2 is not reachable	Critical
rip2-ers1-nw-rfa	181434	11/18/15 8:30:55 PM	rip2-ers1-nw-rfa is not reachable	Critical

Known problem

Informational alert

181,000 Critical Events for:
rip2-ers1-nw-rfa is not reachable
Fault not known – No IETM procedures

18
79
361
1 rows selected
michell.john
fm101-wh.nm.muos.mil:8443
Applet com.micromuse.wave.applets.ael.AEL started
Trusted sites

Figure 3-7. Screenshot of the FOUO Enclave Fault Management Screen

The network managers have become desensitized to critical alerts and sometimes ignore them because there are hundreds of known issues with open problem change requests (PCRs), trouble tickets, or other problems that the Navy is slow to resolve. Figure 3-7 shows critical alarm "georef101-nw-gcs is not reachable." This fault alarm is related to the geolocation capability that was deferred from MOT&E-2 because the functionality is still under development and not ready to be operationally tested. The Navy should:

- Improve network management alert filtering at the NMS to make the alerts descriptive, relevant, timely, and actionable.
- Filter and prioritize alert event notifications consistently across the FOUO and Secret network management enclaves.

- Update the IETM to ensure there is consistency between the NMS displayed fault severity and the fault severity contained in the IETM.
- Update the IETM to include all alert events, including the methods to correct the faults and their potential operational effects.

Spectrum Adaptive (SA)-Wideband Code Division Multiple Access (WCDMA) Call Status Monitoring

MUOS does not provide a proactive means to monitor SA-WCDMA communication failures, resulting in potentially extended outages for deployed users. In other words, MUOS network managers cannot tell whether the cells are working or not working. The MUOS network managers cannot assess, take corrective action on, or report on SA-WCDMA satellite beam carrier availability. Key systems associated with SA-WCDMA call services – such as the radio base stations (RBSs) that handle the SA-WCDMA traffic and signaling in the radio access facilities (RAFs) – do not provide fault information to the fault management system.[28] There is also a known problem, submitted in August 2015 (PCR# 297843), where the OSS-RC does not propagate radio network controller (RNC) alert events to the fault management system. An RNC manages the RBSs in a RAF.

SMDC/ARSTRAT and Regional SATCOM Support Center (RSSC) – West (Colorado) planners perform provisioning, network configurations, and monitor call records. The MUOS network managers manage the MUOS ground system infrastructure, but are generally not aware of user communications status over the MUOS network. The MUOS network managers are often unaware of communication outages until a user submits a trouble ticket. The first notification is typically by the user submitting a trouble ticket to the Space and Naval Warfare Systems Command help desk, which is not familiar with MUOS. The SMDC/ARSTRAT C-SSE or RSSC-West resource planners are not in the reporting chain unless notified separately by the user or NMS. They cannot assess, report, or react to the operational user community. As recommended previously, the Navy and USSTRATCOM should jointly develop a MUOS outage notification tool to notify the C-SSE, provisioners, and deployed users of system degradations, outages, carrier frequency problems, and their potential operational effects.

During MOT&E-2, the depot contractor performed “enhanced situational awareness” by conducting automated MUOS calls from its factories in Scottsdale, Arizona, and Taunton, Massachusetts, overnight. The Navy told the testers this was required to “tune” MUOS, rather than to monitor satellite beam carrier (SBC) outages. Besides the outages related to rekeying events, there were at least four other outages during testing that the MUOS NMS was not aware of until the depot contractor submitted trouble tickets:

[28] There are two banks of six RBSs in each RAF; a bank of six RBSs serve a single satellite in providing communications from the MUOS ground segment through the satellite to the user. A single RBS provides communications over several of the 16 beams provided by each satellite.

- On October 26, one-half of the capacity on the Pacific satellite and the Wahiawa RAF was unavailable. The outage lasted approximately 2 days, starting the afternoon of October 24 and ending almost 49 hours later on October 26.
- On November 12, RBS #12 at the Wahiawa RAF was out of synchronization, and calls could not be made through cells 259, 379, 307, and 267 on Pacific Satellite Beams 1, 2, 7, and 16, covering the areas of Japan, Korea, and the Western Pacific.
- On November 18, radios were not able to join groups on CONUS satellite beams 2 (cell 137) and 8 (Cell 185) through the Wahiawa RAF.
- On November 18, there was a group service interruption on 25 percent of the Pacific satellite for approximately 15.5 hours.

There may have been more SBC outages that were not discovered. The depot contractor’s automated calling was of limited scope and not across the entire MUOS constellation. The automated calling consumes communication resources. While this did not negatively affect MOT&E-2, DOT&E questions whether this is operationally viable for the long-term solution when operational users saturate the system and resources are limited. USSTRATCOM should review the automated calling performed by the depot contractor and determine if this is a viable operational solution when MUOS enters into full operations.

Site Interconnectivity Monitoring

MUOS does not provide network managers with a tool to monitor the connections between the different ground sites. Without active monitoring of DISN interconnectivity, NMS personnel cannot determine if there is latency in the circuits. Degradations can go unchecked, leading to longer reaction times when there is a loss of connectivity. The network management personnel have developed a rudimentary tool to ping the border gateway routers at the ground facilities.[29] The MUOS network managers submitted a high-priority trouble ticket (#155669) on November 6, 2015, requesting that the MUOS Program Manager provide a real-time monitoring tool. The Navy should develop and provide the NMS a tool to directly and actively monitor DISN interconnections between MUOS sites without operator intervention.

Communications Security

NMS Cryptographic Key Loading

Using the current processes, the MUOS NMS security personnel will not be able to keep up with the demand for keys given a full operational population of terminals. As discussed previously, the loading of cryptographic keys is an orchestrated process between the MUOS ground system and the MUOS terminal. During terminal provisioning, the Operational Planning Authority (OPA) at Peterson AFB, Colorado, assigns an unused cryptographic key-pair to each terminal via the seed profile. The actual keying materiel is populated in the terminal via

[29] Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network.

over-the-air file transfer (OTA-FT) upon power-up and registration. Each terminal requires a key-pair of Advanced Encryption Standard (AES) cover key and over-the-air rekey (OTAR) keys.

The Naval Computer and Telecommunications Area Master Station – Pacific (NCTAMS-PAC) Communication Security (COMSEC) Custodian generates the AES cover key and OTAR keys using the Electronic Key Management System (EKMS) key processor. The MUOS NMS security manager must manually transfer each terminal's pair of AES cover key and OTAR key from the EKMS Local Management Device/Key Processor to the MUOS Key Management System through a process that requires the transfer of a single key-pair at a time. This is a detailed and labor-intensive process that is unforgiving. The process requires a two-person team to navigate. If mistakes are made, then the keys can become unusable – requiring NCTAMS-PAC to obtain more keys from the National Security Agency. The previous NMS security manager inadvertently destroyed keys trying to transfer them to MUOS, and quit his job because the process was too stressful.

The MUOS security manager loads 25 pairs of keys at a time into a simple key loader and transfers them to MUOS as his teammate reads the instructions and tracks the checklist. Transferring the 25 key-pairs in an observation by COTF took 48 minutes. In a second observation by DOT&E, the process took 1 hour, 14 minutes.

The security manager estimates that NMS can transfer 85 pairs of keys a day, based on current manning levels. The NMS personnel will need to transfer 250 key-pairs a day to meet demand and not result in delays to the terminal users in provisioning or rekeying their terminals. NCTAMS-PAC estimates this will be a problem by FY18, given the expected terminal fieldings. The IETM shows procedures for loading many key-pairs simultaneously into the MUOS Key Management System (KMS) via compact disk, which could significantly speed up the process, but those procedures are greyed out without explanation. The Navy should develop a technical solution and procedures to perform bulk loading of MUOS AES keys into the MUOS Key Management System. If a technical solution cannot be developed, then the Navy should review staffing levels and adjust them appropriately to ensure military operations are not impaired due to delays in loading sufficient numbers of operational keys.

Over-the-Air Rekeying and Compromised Terminal Operations

MUOS was able to conduct routine OTARs but cannot reliably conduct compromised terminal operations. The reliability problems could result in global communications outages for an entire branch of Service or all of Special Operations until the problem is resolved and the MUOS ground system broadcasts a new group cover key (GCK).

The MUOS network managers conduct two types of OTAR operations – routine and compromised terminal operations. Routine OTARs occur on a weekly basis and update the group cover key for all members of a group. The NMS conducts compromised terminal operations on demand to remove a compromised terminal from the MUOS network. To achieve this, all terminals in a group are rekeyed except the terminal that was compromised.

Table 3-20. Summary of Over-the-Air Rekey Operations

Over the Air Rekey (OTAR) Operation	Attempts	Successes	Pass Rate Percentage	95% Confidence Interval
Routine (weekly)	15	15	100	81.7*
Compromised Terminal OTARs	4	2	50	6.7 - 93.3
Total OTARs	**19**	**17**	**89.5**	**66.7 - 98.7**

* Lower Confidence Bound

As Table 3-20 summarizes, the MUOS NMS successfully conducted 89.5 percent of all OTAR operations, with a 95.0 percent confidence interval from 66.7 to 98.7 percent. The MUOS NMS successfully conducted 100.0 percent (15 of 15) of routine OTARS, with a 95.0 percent lower confidence bound of 81.7 percent. Successful rekeys took between 2 and 3 minutes to complete; one outlier took 8 minutes to complete. DOT&E observed a minor problem when 9 of the 15 routine rekey events were as "Group Compromise Recovery Events" in the OTA-FT update report, when the system should have listed these as "Group Rekey Events."

Compromised terminal operations were more problematic. Two of four compromised terminal operations succeeded, with a 95.0 percent confidence interval between 6.7 and 93.3 percent. The wide range of uncertainty is a result of the small sample size. COTF did not conduct additional compromised terminal OTAR operations because failed OTARs led to long outages that were disruptive to the test. MUOS failed to conduct OTARs on two occasions due to system reliability problems that are not specific to compromised terminal operations:

- On November 9, 2015, the system failed during "Sending GCK Rekey Broadcast Package." The COTF test director submitted a PRI-1 Trouble Ticket (#155778) to restore communications. NMS network managers determined the root cause of the failed rekey was due to an RNC fault at the Wahiawa RAF. Further investigation by the network managers verified the keys were received by the Group Manager at each of the RAFs, updating the ground system, but the keys were not broadcasted to the terminals as scheduled. Because the system requires all four RAFs to broadcast the rekey simultaneously, and since none of the RAFs broadcasted the rekey, the GCKs between the terminals and the ground system were mismatched, resulting in loss of all group communications.
- On November 17, 2015, the NMS Security Manager performed a pre-OTAR check that failed due to the RNC in the Australian RAF failing. A secondary and redundant board in the RNC should have taken over but it did not. NMS network managers tried to troubleshoot but there was no documentation, instructions, or guidance available. The network managers submitted a trouble ticket (#156159) for depot support. Depot support intervened and attributed the problem to a failure of the

> FCAPS server to push the valid certificate revocation list file to the RNCs. The system could not rekey for 6 hours, 2 minutes until depot-level support rebooted the OSS-RC server (which restarted processes on the FCAPS server).

The outages could result in serious and wide-ranging consequences in live operational missions. As discussed preciously, there are only eight possible GCKs available in the system. The concept of operations is still being developed by SMDC/ARSTRAT, but the current concept is that the Army, Navy, Air Force, Marine Corps, Special Operations, and Coast Guard will each have a unique GCK, with some spares remaining for contingencies. A failure such as the one experienced on November 9, 2015, regardless of the type of rekey operation, could result in global communications outages for an entire branch of Service, all of Special Operations, or the entire Coast Guard until the problem was resolved and the MUOS ground system broadcasts new GCKs.

Additionally, once the NMS network managers initiate the process to perform an OTAR, they have no means to stop it – even if they determine ahead of time that the rekey will result in widespread outages. The Navy knew of the rekey problem going into MOT&E-2. The developmental testers had observed this problem in during testing in May 2014, January 2015, April 2015, and again in the June 2015 Technical Evaluation. To mitigate outages from reliability problems, the security managers perform certificate revocation list updates daily – rather than every six days as specified in the manuals – diverting resources from other system responsibilities. This does not eliminate problem, but it potentially gives the NMS some advance warning in order to resolve problems before they cause communication outages. The Navy should resolve the reliability problems with rekey operations that can result in communication outages on a wide-ranging scale. The Navy should also develop the capability to abort rekeys when it is clear a rekey event will result in communication outages. USSTRATCOM should reconsider its emerging GCK concept, considering the potential for catastrophic outages for failed rekey events.

Terminal Profile and Cryptographic Key Portability

The current MUOS profile and cryptographic key procedures do not allow profile and crypto-key portability, and hence do not support the standard operational concepts for tactical radios. As Table 3-21 shows, all services will be affected to varying degrees by the lack of MUOS profile and crypto-key portability.

The MUOS ground system selects AES cover keys and OTAR keys for exclusive use with each individual profile. The system replaces (rekeys) the AES cover key over-the-air to the terminal radio at the end of the one-year expiration period. There is currently no other method of obtaining the replacement cover key.

Table 3-21. Assessment of Service Profile and Key Portability Requirement

Service/Platform	Platform	Profile Portability Required	Anticipated Frequency
Army	Manpack	Yes	Frequent
	Aviation	Yes	Not Often
Navy	Maritime	No	Not Often
	Aviation	Yes	Frequent
	Manpack	Yes	Frequent
Marine Corps	Manpack	Yes	Frequent
	Aviation	Yes	Frequent
Air Force	Aviation	Yes	Frequent
	Manpack	Yes	Frequent
Coast Guard	Maritime	Yes	Not Often
	Aviation	Yes	Frequent
	Manpack	Yes	Frequent

If a terminal operator zeroizes a terminal for any reason (accident, maintenance, CONOPS) after a rekey of the cover key (i.e., after one year), then the user must request a new profile. If the user tries to refill the terminal with the original (or pre-expiration) cover key, it will fail to authenticate, and the ground system will not resend the new cover key. The user must request and receive a new profile, which changes the terminal phone number. Any group networks that terminal participates in would need to be reconfigured, and associated terminals would need to be updated.

At the end of a mission, the Army envisions that users will zeroize tactical MUOS terminals and store them as unclassified Controlled Cryptographic Items, as they do now for all tactical combat net radios today. Additionally, when users turn terminals into maintenance terminals they normally zeroize the radio, since maintainers do not typically have security clearances or secure storage necessary to handle the classified terminals.

Under such scenarios, the only way to bring a terminal back into operations is to request a new profile. This is a time-consuming process and requires ready access to SIPRNET, which may not be possible in all operational locations. When obtaining a new profile, the user receives a new phone number which is not known to the rest of the force. The Navy should work with the other Services and NSA to develop a materiel solution, policies, and procedures for profile and cryptographic key portability to support the users' CONOPS.

Cybersecurity

COTF, with Naval Information Operations Command (NIOC) support, conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) from November 9 – 20, 2015, from the MUOS Satellite Control Segment (SCS) in Point Mugu, California, and the NMF, SF, and RAF at Wahiawa, Hawaii. After allowing time for the MUOS Program Manager to fix or mitigate vulnerabilities, COTF and NIOC followed up with a cybersecurity Adversarial Assessment at the SCS and NMS from April 4 – 8, 2016. The results of the cybersecurity testing can be found in the classified annex to this report. The Navy should fix or mitigate the cybersecurity recommendations in the classified annex to this report.

.

Section Four
Operational Suitability

MUOS is not operationally suitable. The ground system lacks the stability and maturity to enter into and sustain global operations. MUOS does not provide communications that deployed users can rely on when the system is in widespread use or at full capacity. MUOS performed poorly in almost every area of operational suitability. The cumulative effects of these failures could have grave operational consequences to deployed forces.

MUOS does not meet the user-defined threshold for operational availability. The Network Management Segment (NMS) was operational available 6.3 percent of the time, against a 95.0 percent threshold criterion. The Ground Transport Segment (GTS) was operationally available 87 percent of the time, against a 99 percent threshold requirement. There were large, contiguous blocks of test time during which a subset of MUOS users/operators would have experienced an outage. There was no time after hour 36 of the month-long test that the NMS did not experience an operational mission failure. The ground system availability problems were known to the MUOS Program Manager at least as early as the Technical Evaluation in June 2015. While the program never published availability metrics outside of the program office, the Technical Evaluation report states that, "Collective observations of system downtime resulted in Ground Segment availability for GTS and NMS not met."

MUOS does not meet threshold requirements for segment mean repair times. The MUOS threshold segment repair time is 45 minutes (0.75 hours). MUOS demonstrated repair times in terms of hours, even with depot maintainers on-site, in violation of their published logistic support plans. The median repair time for NMS based on 37 repair actions was 89 hours. NMS mean repair time was 1,058 hours. DOT&E believes a median repair time is a better statistical estimate for skewed distributions. The median repair time for the GTS was 185 hours, Satellite Control Segment (SCS) was 100 hours, and Ground Infrastructure Segment (GIS) was 114 hours.

Long repair times are driven in part by the MUOS organizational-level personnel having a high dependency on depot support to maintain operations. The MUOS Program Manager deployed contractor depot maintainers on-site during the test to minimize depot maintainer reaction time and in recognition of the complex MUOS system's lack of stability. The MUOS operators generated 128 unique trouble tickets, when duplicate trouble tickets were removed, 73 percent of which requested depot support. The depot maintainers had to visit the Wahiawa, Hawaii, site 90 times during the 20 test days.

Ground system problem change requests (PCRs) remained uncorrected for long periods and seldom contained operational effect statements. PCR submitters sometimes incorrectly prioritized severity levels because they did not view the system operationally. There are over 900 ground system software PCRs open, with over 240 categorized as priority (PRI)-2 by the Navy. DOT&E performed an independent assessment of the 242 open PRI-2 PCRs, provided on March 3, 2016, and assessed that at least 151 of them will negatively affect MUOS operations.

The MUOS Program Manager lacks an executable plan to resolve known problems. DOT&E calculated the mean age of open PRI-2 PCRs to be 526 days.

The SCS controllers indicated general satisfaction with the classroom training, but 80 percent disagreed that it prepared them for the tasks they need to perform. The system satellite controllers, planners and provisioners, and network managers were dissatisfied with the provided training, documentation, and system usability. The system documentation is immature, missing information, and cannot be accessed by all the personnel who need to access it. Network managers, satellite controllers, and planners all expressed dissatisfaction with the documentation. The majority of NMS personnel are dissatisfied with the usability of the system.

Availability

Table 4-1 shows that MUOS does not meet the user-defined threshold for operational availability. DOT&E did not calculate confidence intervals because there were not enough separate downtimes. Either the Operational Mission Failures (OMFs) overlapped or there were too few OMFs in a particular segment.

Table 4-1. Operational Availability of the MUOS Ground Segments.

MUOS Ground System	Threshold Criterion	Measured Availability
Ground Transport Segment	**0.99**	**0.87**
Network Management Segment	**0.95**	**0.06**
Satellite Control Segment	**0.99**	**1.00**
Ground Infrastructure Segment	**0.99**	**0.94**

OMFs often occurred for a subset of MUOS users or operators, but not necessarily for all. In these cases an OMF was counted against the segment as a whole. This results in OMFs overlapping one another when availability is calculated. So, there are large contiguous blocks of test time during which a subset of MUOS users/operators would have experienced an outage. There was no time after hour 36 of the test that the NMS did not experience an OMF.

Some of the OMFs had not been resolved at the time this report was written. Because there was no identifiable end to the outage DOT&E did not include these failures in the calculations for operational availability. Therefore, it is likely that the operational availability is actually worse than the calculations show.

The availability problems were known to the MUOS Program Manager at least as early as the Technical Evaluation in June 2015. While the program never published availability metrics outside of the Program Office, its Technical Evaluation report states, “Collective observations of system downtime resulted in Ground Segment availability for GTS and NMS not met.” The MUOS Program Manager is now tracking communication service availability through the MUOS satellites by frequency carrier. In March 2016, communications service availability through the Continental United States (CONUS) satellite ranged between 19.1 and 25.6 percent, depending on the frequency carrier, due to continuing ground system problems. The Pacific and Atlantic satellite services fared better, with availability ranging between 76.2 and 96.9 percent.

Reliability

MUOS has no user-specified reliability requirements.[30] Table 4-2 summarizes the demonstrated Mean Time Between Operational Mission Failure (MTBOMF) of the MUOS Segments during the second Multi-Service Operational Test and Evaluation (MOT&E-2).

Table 4-2. Mean Time Between Operational Mission Failure (MTBOMF)

MUOS Ground System	Operational Mission Failures	Test Time (hours)	MTBOMF (hours) [95% Confidence Interval]
Ground Transport Segment	**6**	1,728	**263** [81 - 916]
Network Management Segment	**12**	576	**46** [21 - 103]
Satellite Control Segment	**0**	576	Unknown*
Ground Infrastructure Segment	**2**	576	**393.3** [31 – 15,468]

* Since there were no failures during testing DOT&E cannot calculate a point estimate

The MUOS NMS demonstrated an MTBOMF of 46 hours. The SCS did not experience an operational mission failure during MOT&E-2; therefore DOT&E cannot calculate a MTBOMF for this segment. Based on the approved test plan, DOT&E defines an OMF as a failure that:

- Prevents a user from communicating,
- Prevents an operator from commanding the satellites, and/or
- Prevents a planner from provisioning a user to communicate.

Mean Time Between Failure (MTBF) is a measure of the average operating time between any failures of the system, excluding scheduled maintenance. There is no user-defined threshold requirement for MTBF. Table 4-3 summarizes MUOS Ground System results from MOT&E-2. The NMS experienced 49 failures over a 30-day test event for an MTBF point estimate of 16 hours between failures – illustrating the instability of the ground system.

[30] The reliability requirements specified in the 2008 MUOS Capability Production Document are actually availability requirements.

Table 4-3. MUOS Demonstrated Mean Time Between Failure (MTBF)

MUOS Ground System	Failures	Test Time (hours)	MTBF (hours) [95% Confidence Interval]
Ground Transport Segment	**36**	**1,728**	**37** [23 - 61]
Network Management Segment	**49**	**576**	**16** [10 - 23]
Satellite Control Segment	**9**	**576**	**142** [51 - 414]
Ground Infrastructure Segment	**6**	**576**	**94** [29 - 344]

Maintainability

MUOS does not meet threshold requirements for segment repair times. The MUOS threshold segment repair time is 45 minutes (0.75 hours). MUOS demonstrated repair times in terms of hours, even with the depot maintainers on-site. Table 4-4 summarizes the MUOS segments' demonstrated repair times for problems that the Navy resolved.

Table 4-4. Summary of Resolved MUOS Ground System

MUOS Ground System (Closed Trouble Tickets)	Maintenance Actions	Required Mean Time To Repair (hours)	Mean Time To Repair (hours) [95% CI]	Median Time To Repair (hours) [95% CI]
Ground Transport Segment	23	**0.75**	**896** [279 – 2,875]	**185** [90 – 383]
Network Management Segment	37	**0.75**	**1,058** [161 – 6,944]	**89** [25 – 325]
Satellite Control Segment	2	**0.75**	**259** [48 – 1,401]	**100** [30 – 335]
Ground Infrastructure Segment	6	**0.75**	**865** [53 – 14,196]	**114** [23 – 572]

CI – Confidence Interval

There were 234 trouble tickets generated by the test participants during the 30-day MOT&E-2. DOT&E counted 128 trouble tickets after eliminating duplicate entries for the same problem, tickets relating to non-operational parts of MUOS (such as the Sicily, Italy, Radio Access Facility [RAF]), and tickets requesting capability upgrades. The Navy claims that, as of March 2016, system operators or depot-level maintainers resolved 68 of the MOT&E-2 trouble tickets, leaving 60 still open and unresolved. However, this does not mean the 68 problems were actually fixed. Sometimes a trouble ticket is resolved by merely transforming it into a PCR, by attributing the trouble ticket to an open PCR, or by performing a work-around procedure. The Navy was not able to resolve all failures during MOT&E-2. If the failure was resolved outside of the test, then DOT&E included the time in calculations of maintainability.

The long repair times are driven in part by the MUOS organizational-level personnel having a high dependency on depot support to maintain operations. The Navy's User's Logistics Support Summary for MUOS, dated June 2015, specifies a two-tiered maintenance approach. The Naval Computer and Telecommunications Area Master Station – Pacific (NCTAMS-PAC) performs organizational maintenance and depot maintenance at a contractor depot (Scottsdale, Arizona) for complex repairs of defective items. Depot maintenance would also include remote troubleshooting and analysis support, as well as the dispatch of additional maintenance resources to ground sites for extended repair efforts.

This was not the maintenance concept the Navy used during MOT&E-2. The MUOS Program Manager deployed contractor depot maintainers to Wahiawa in order to minimize depot maintainer reaction time and in recognition of the complex MUOS system's lack of stability. The depot maintainers are located in a trailer adjacent to the Wahiawa Network Management Facility (NMF), Switching Facility (SF), and RAF. Additionally, as discussed in the training section of this report, the program has done a poor job in preparing the NCTAMS-PAC personnel for assuming their responsibilities as MUOS network managers. The MUOS Program Manager has stated that the Navy is revising the maintenance concept to include on-site depot-level maintainers.

Figure 4-1 graphs the daily visits from depot maintainers to the NMS. The Naval Command Operational Test and Evaluation Force (COTF) controlled the depot maintainers' access and required them to log in and out for each visit.

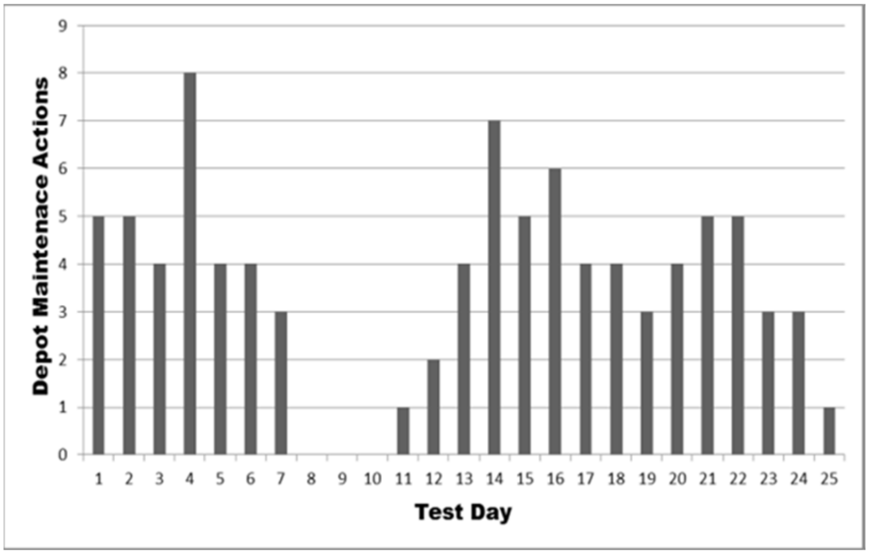


Figure 4-1. Depot Maintenance Support by Test Day.

The NCTAMS-PAC personnel typically requested depot maintainer support through a trouble ticket. While this induced some additional repair time, DOT&E believes this was negligible since the testers allowed organizational maintainers to call and request depot support and then follow the called request with an actual trouble ticket. On October 22, 2015 (test day four), depot maintainers visited the NMF eight times to try to resolve the latent call detail records (CDRs), collect system logs, and remove automated scripts that keep the system call performance from degrading. The Navy decided to downgrade the auto-scripting from a depot-level task to an organizational-level task, although it never completed this during MOT&E-2.

The Navy's high reliance on depot maintenance contributes to the poor maintainability numbers. DOT&E observed that the organizational-level personnel are reluctant to perform maintenance actions with the depot maintainers in such close proximity. Of the trouble tickets that organizational personnel submitted during MOT&E-2, 73 percent (93 of 128) requested depot-level support. The allocation of maintenance actions appears weighted strongly towards depot maintenance. DOT&E observed that the MUOS RAF maintainers submitted a trouble ticket for depot maintainers to troubleshoot a power supply for the air condition controllers that they had already determined to be bad, but were reluctant to take further action on without approval of the depot maintainers. Overreliance on depot maintainers is a disservice to the organizational-level maintainers and network managers because they miss valuable opportunities to learn how to maintain and manage MUOS before there are large populations of users depending upon their abilities.

There is further evidence of inappropriate maintenance allocations based on server and database maintenance. This is normally an organizational maintenance task, but for MUOS it is allocated to depot. There is no database preventive maintenance taking place to defragment and groom databases and disk drives.

Table 4-5. Observations of Server Status During MOT&E-2

System	Purpose	Percent of Hard Drive Full	Operational Effect
Operations Support System for Radio and Core Server	NMF Operating System	97	- Unable to provision terminals - Unable to monitor failures - CDR backlogs
Tivoli Storage Manager Server	Backup and Recovery Operations	98	- Loss of ability to recover data
Australian RAF Earth Terminal 2 Interface/Signal Processor	Timing and Waveform Processing	99	- MUOS Call Failures
Security Information and Event Manager – Server 103	Cybersecurity Monitoring	93	- Unable to record security events
Security Information and Event Manager – Server 104	Cybersecurity Monitoring	90	- Unable to record security events

RAF – Radio Access Facility; NMF – Network Management Facility; CDR – Call Detail Record

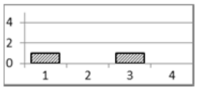
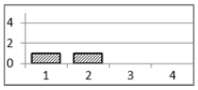
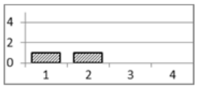
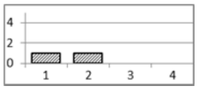
Table 4-5 shows DOT&E observations of select server status during MOT&E-2. Critical servers were operating at near full capacity – such as the Operating System Support – Radio and Core (OSS-RC), which performs as the NMS operating system. These high rates of capacity can affect MUOS system stability and result in MUOS ground system and user communication outages. The preventive maintenance procedures to groom the servers and databases were in the Interactive Electronic Technical Manual (IETM), but the depot maintainers removed this information from the organizational-level procedures in the latest update. The quantity and magnitude of the maintainability problems will escalate as MUOS is required to service the expected operational population of over 10,000 radios. The Navy should review the allocation of required maintenance actions and allocate maintenance actions to the lowest possible level.

Maintenance Surveys

The Navy surveyed maintainers at the SCS and NMS. Table 4-6 summarizes the responses from the SCS maintainers. The SCS maintainers were satisfied with the maintainability of the system. DOT&E considered a rating of 3 or above as a negative response. Comments by the respondents fell into two areas:

- MUOS software products delivered outside the structured SCS delivery process often fail to install in accordance with provided instructions, or fail to produce the desired outcome (i.e., missing or incorrect files).
- The fault isolation procedures in the IETM do not cover all the faults seen by satellite operators.

Table 4-6. Summary of Satellite Control Segment Maintainer Responses

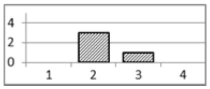
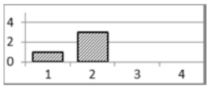
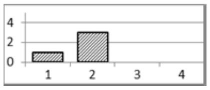
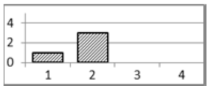
Survey Topic	Mode	Ratings ≥ 3	Distribution
System components were easy to access	1, 3	1 of 2	
Tools and equipment to perform tasks were available	1, 2	0 of 2	
Parts to perform tasks were available	1, 2	0 of 2	
Procedures were easy to follow	1, 2	0 of 2	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

Table 4-7 shows that organizational maintainers at the NMS were satisfied with the maintainability of the system. However, DOT&E cautions that this satisfaction may be the predicated on readily available depot support. Although they expressed overall satisfaction, the organizational maintainers complained that:

- The IETM is confusing and you may not find information you need in a section. The hyperlinks do not always take you to the right place in the IETM.
- Maintainers need to clear the logs of certain systems to prevent system failure. If this is not performed on a regular basis, the system may crash or become unresponsive. This is not included in the routine maintenance procedures.

Table 4-7. Summary of Network Management Segment Maintainer Responses

Survey Topic	Mode	Ratings ≥ 3	Distribution
System components were easy to access	2	1 of 4	
Tools and equipment to perform tasks were available	2	0 of 4	
Parts to perform tasks were available	2	0 of 4	
Procedures were easy to follow	2	0 of 4	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

The Navy should update SCS and NMS maintainer documentation to correct inaccuracies, add missing troubleshooting procedures, and give added detail for in-depth understanding of the purpose behind the procedures. The Navy should test software installations and develop appropriate procedures prior to delivering them to the operational SCS.

Supportability

Switchover

MUOS successfully demonstrated the capability to perform switchovers. Table 4-8 shows that MUOS was able to complete 80 percent (4 of 5) of switchover attempts during the MOT&E. The NMS and SCS were able to successfully perform switchovers on all four attempts – three times at the Northwest RAF, and once at the Australian RAF.

Table 4-8. Summary of Switchovers during MOT&E-2

Date	Radio Access Facility	Beginning – Ending Earth Terminal (ET)	MUOS Satellite	Attempts	Successes
October 19	Northwest	ET2 – ET3	CONUS	1	1
November 10	Northwest	ET3 – ET2	CONUS	1	1
November 12	Northwest	ET1 – ET3	ATLANTIC	2	1
November 13	Australia	ET2 – ET3	PACIFIC	1	1
			Aggregate	5	4

CONUS – Continental United States

The initial attempt on November 12, 2015, to perform a switchover from the Northwest RAF's ET1 to ET3 failed when the network managers received an OSS-RC fault preventing the switchover from completing. The network managers could not find the fault indication information in the IETM and submitted a trouble ticket requesting depot support, and an IETM update. Depot support resolved the problem the next day and created a PCR to update the documentation.

Ground System Problem Change Requests (PCRs)

Ground system PCRs remain uncorrected for long periods; seldom contain operational effect statements; and submitters sometimes incorrectly prioritize severity levels because they do not view the system operationally. In September 2015, the Navy briefed the test community that there were 243 open, PRI-2 system deficiencies, called PCRs, in preparation for MOT&E-2. These PCRs were from a category called "ground system software" PCRs, and they do not represent the full set of PCRs on MUOS. The Program Manager assessed 35 of these PRI-2 deficiencies as having an "operational impact." A PRI-2 PCR, by definition, adversely affects the accomplishment of an essential capability and there is no known work-around solution.[31] It is not clear how a deficiency can adversely affect an essential capability but not have a negative operational impact.

On March 3, 2016, DOT&E requested from the Navy an updated list of the backlog of high-priority ground system PCRs (PRI-2 PCRs and higher) open on MUOS. The MUOS program provided DOT&E with a revised list of 242 open PRI-2 PCRs. The Navy resolved 11 of the 35 pre-MOT&E deficiencies with operational impact and discovered 11 new deficiencies with operational impact. The March 3, 2016, list of operational impact PCRs included at least six PRI-2 PCRs opened before September 2015 that the Program Manager previously did not consider to have an operational impact. DOT&E reviewed the March 3, 2016,

[31] Institute of Electrical and Electronics Engineers Standard 12207

list of PRI-2 PCRs and assesses that at least 151 of the deficiencies will negatively affect MUOS operations. The MUOS ground system software has 993 open PCRs, if all priority levels are considered, including lower PRI-3, PRI-4, or PRI-5 problems.

The operational impact assessments are not based on what would be required of MUOS as a fully operational system. The operational impact section of high-priority PCRs is often not completed or left completely blank. The assessment of operational impact by the PCR submitter is often based on current Spectrum Adaptive (SA)-Wideband Code Division Multiple Access (WCDMA) usage that is sporadic as it supports test events and demonstrations. Therefore, the PCR priorities are sometimes lower than they should be. The Navy should reassess PCR priorities with the user community in light of true operational effects, then prioritize and correct the problems accordingly. DOT&E does not believe that there are no PRI-1 PCRs among the 933 open ground system software PCRs. The four cases below are a small sampling of the PCRs the Navy categorized as PRI-2.

- PCR #294982 – The Radio Network Controller (RNC)-to-Radio Cover Group interface has problems that can result in a loss of 64 carriers (one-half the capacity on two satellites) that requires operator intervention and an RNC reboot. However, as previously discussed, the RNC does not always alert the operator – resulting in extended outages.
- PCR #296491 – The RNC uses an incorrect cell identifier for group cover key, resulting in multiple satellite beam carriers across multiple beams and satellites being unable to support group network services.
- PCR #294982 – Over-the-Air (OTA) Provisioning servers are unavailable, resulting in OTA-File Transfer (FT) failing for all users.
- PCR #299599 – The OSS-RC server sometimes pushes invalid certificate revocation list files to the RNCs. The operational impact statement says this may cause group provisioning to fail. This PCR was written during MOT&E-2. MOT&E-2 results clearly show this problem undoubtedly causes group rekey failures which can result in widespread outages.

The MUOS Program Manager lacks an executable plan to resolve known problems. DOT&E, in reviewing the data set that was provided, found that the mean age of open PRI-2 PCRs is 526 days. The oldest is 1,307 days, and the newest is 39 days. The MUOS program experiences high-priority problems as fast as it resolves them. At the end of March 2016, the program had 993 ground system software PCRs: 256 PRI-2, 622 PRI-3, and 155 PRI-4 and below. This total does not include information assurance, technical refresh activities, or work-in-progress PCRs – combined, these categories would add an additional 2,029 PCRs. Figure 4-2 shows that the software PCR backlog has been essentially in steady state since at least June 2015. The steady state indicates that MUOS is not maturing as an operationally viable system.

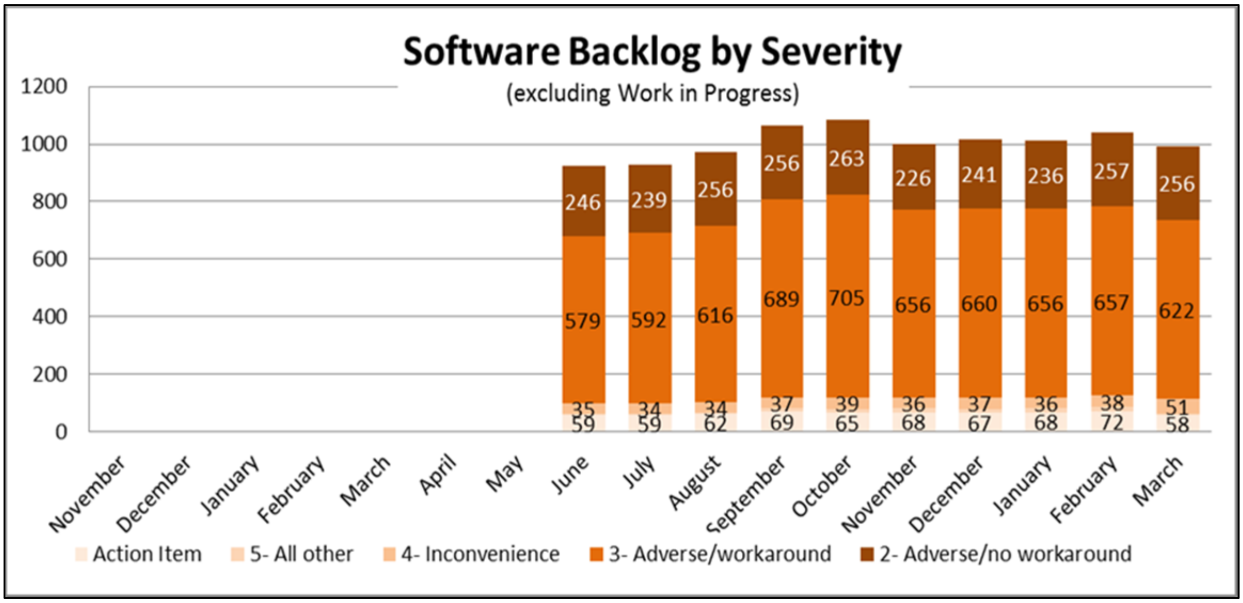


Figure 4-2 Ground System Problem Change Request Backlog by Month

If all categories of Ground System PCRs are considered, then the PCR backlog is continuing to grow. In November 2013, the overall PCR backlog was 1,872; in June 2015 it was 2,262; and in March 2016 the backlog was 3,012. The Navy needs to increase efforts to resolve problems with MUOS. The Navy should develop and adequately fund an executable plan to resolve the large number of high-priority PCRs and trouble tickets before the next operational test.

Manning

MUOS does meet the manpower threshold criterion that the number of network management operations personnel must be the same as or less than that used to support the UHF Follow-On (UFO) system. However, this requirement is senseless in light of the fact that the legacy UHF capability did not retire – nor will it retire soon – and MUOS SA-WCDMA is significantly more complex than legacy UHF. The Navy personnel who manage legacy UHF still manage UHF legacy operations. The MUOS SA-WCDMA is a new, additive, capability that is very complex to operate and maintain. The Navy plans for 30 personnel to manage the Wahiawa Ground System: 24 government and contractor operators (system administrators, security managers, network managers), 4 military and contractor maintainers, and 2 training contractors. During MOT&E-2, NCTAMS-PAC manned Wahiawa Ground System at 57 percent (17 of the 30 personnel), leaving one or two personnel to manage MUOS on the night shifts. The Navy is trying to build up the staff but suffers from turnover as qualified personnel leave for higher-paying opportunities. While manning was not a critical problem during MOT&E-2, it will be a critical problem when the system becomes operational. The Navy should determine the root causes of contractor staffing turnover and modify policies as necessary.

MUOS Trouble Ticketing and Help Desk Operations

Trouble Tickets

The 128 trouble tickets written during MOT&E-2 are consistent with MUOS norms. As Figure 4-3 shows, the number of trouble tickets continue to grow at a rate at least as fast as the MUOS Program Manager can close them. Some percentage of the trouble tickets will be converted to PCRs. As of February 29, 2016, there were 550 open trouble tickets. As of March 30, 2016, that number had grown to 576 open trouble tickets.

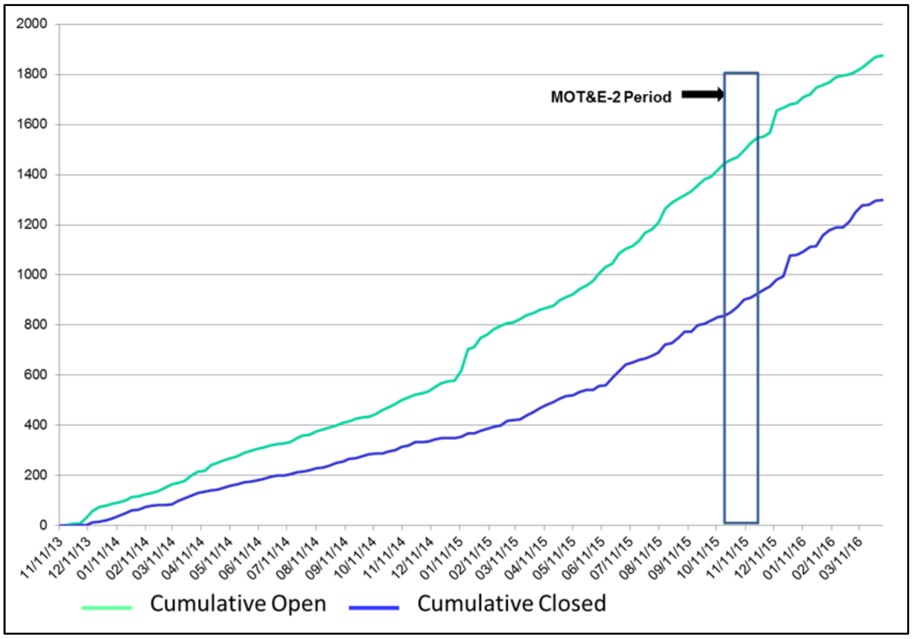


Figure 4-3. Cumulative Open and Closed Trouble Tickets

As stated previously, DOT&E counted 128 trouble tickets after eliminating duplicate entries for the same problem and eliminating tickets relating to non-operational parts of MUOS. Trouble tickets submitted by the MUOS operators and by the Space and Naval Warfare Systems Command (SPAWAR) Help Desk are sometimes categorized at a lower priority than they should be. The MUOS personnel, including the developing contractor, are not following the criteria for prioritizing a problem as a PRI-1 problem, the highest priority, per the MUOS User's Logistic Support Summary, dated June 2015.

During MOT&E-2, the MUOS personnel submitted only one PRI-1 trouble ticket when, on November 5, 2015, the Sicily, Italy, RAF lost connectivity and became isolated from the rest of MUOS. The MUOS Program Office later downgraded this to a PRI-2 problem. The Army test units submitted the only other PRI-1 trouble ticket when, on October 30, 2015, a total loss of communications occurred at Joint Base Lewis McChord (JBLM). Based on the Navy's criteria, DOT&E believes there should have been more PRI-1 trouble tickets. Below is a small sample of trouble tickets which DOT&E believes should have been characterized as PRI-1 during MOT&E-2:

- On October 26, General Dynamics submitted a PRI-2 trouble ticket (#154968) when it determined through automated calling that there was loss of F3/F4 frequencies (50 percent of communications) on the Pacific satellite through Wahiawa RAF.
- On October 30, the NMS personnel submitted PRI-3 trouble ticket (#155205) for a problem that prevented provisioning and rekeying.
- On November 13, the NMS personnel submitted a PRI-2 trouble ticket for the failure of a SIPR circuit that MUOS relies upon for inter-site interconnectivity and for the downloading of certificate revocation lists that could result in widespread communication failures.

Help Desk Operations

Help desk personnel are unfamiliar with MUOS. The Navy gave MUOS help desk support responsibilities to the SPAWAR consolidated Help Desk in August 2015, just two months prior to MOT&E-2. The recent addition of Help Desk support meant that the help desk personnel were not familiar with MUOS at the time of MOT&E-2. The inexperienced help desk personnel failed to recognize the importance of problems, inappropriately prioritized problems, and even assigned problems to the wrong system.

For example, on October 30, the JBLM MUOS radio operators notified the SPAWAR Help Desk of a MUOS communication outage that affected all of JBLM. The help desk initially responded that the "MUOS person" was not there and asked if the radio operators could call back later. The Army personnel explained the importance of the problem and the help desk replied that they should call the RAF directly. The RAFs are unmanned, so the Army inferred that the help desk meant the NMF. On the Army's third try the help desk agreed to write a trouble ticket. The help desk personnel incorrectly assigned the problem as a PRI-4 trouble ticket and incorrectly assigned it to the Joint Enterprise Network Manager. The Navy should retrain the MUOS operators, developing contractors, users, and help desk personnel on how to initially prioritize problems. The Navy should provide additional training to the SPAWAR Help Desk personnel on how to handle and assign MUOS help desk calls.

Configuration Control

During root cause investigation of the CDR latency problem discussed previously, DOT&E discovered that the servers that process CDRs were in "debug" mode. Debug mode increases processing overhead and is not considered an operational configuration. More troubling was that the Navy, including the depot maintainers, did not have a clear picture of what servers and systems in MUOS were operating in debug mode. The Navy should perform a configuration audit of the ground system to determine what systems are in debug mode and bring debug operations under configuration control.

Training

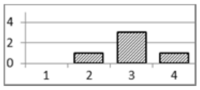
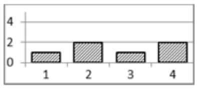
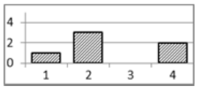
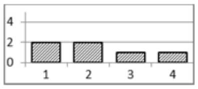
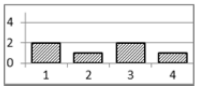
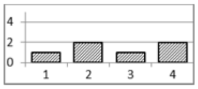
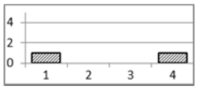
The Navy-provided classroom, on-the-job training (OJT), and simulation training do not prepare the satellite controllers and network management personnel to perform their assigned duties. The classroom prepared resource planners and provisioners for their duties, but trainees found the material difficult to understand and the Navy did not provide the planners and provisioners with OJT or web-based sustainment training as required by the MUOS Lifecycle Support Plan.

The MUOS Program Manager provided training to maintainers and operators in three areas: Satellite Control, Communications Planning, and Network Management. COTF surveyed the SCS operators and maintainers at Point Mugu, California; the communications planners at Regional Satellite Communications (SATCOM) Support Center (RSSC) – West; Army Space and Missile Defense Command/Army Strategic Forces Command (SMDC/ARSTRAT) provisioners at Peterson Air Force Base, Colorado; and the NMS operators and maintainers in Wahiawa, Hawaii.

Satellite Control Segment

SCS Training consisted of classroom training, computer-based training, and OJT. Table 4-9 summarizes the respondents' mixed opinions about the classroom training. More than half of the responses (20 of 37) indicated satisfaction with the training.

Table 4-9. Summary of Satellite Control Segment Classroom Training Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Training was received for the tasks to perform	3	4 of 5	
Training was organized well	2, 4	3 of 6	
Training materials were easy to understand	2	2 of 6	
Trainee had opportunity for hands-on learning with actual equipment	1, 2	2 of 6	
Training was relevant to the tasks	1, 3	3 of 6	
Training prepared trainee for assigned duties	2, 4	3 of 6	
Maintenance - Training was received to perform tasks	1, 4	1 of 2	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

Of the satellite controllers who responded, 80 percent (4 of 5) disagreed that the received training for the tasks they needed to perform. Two-thirds (4 of 6) of the respondents felt the training was easy to understand.

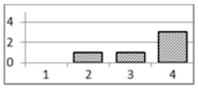
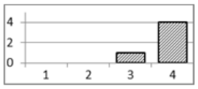
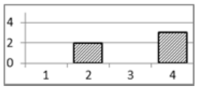
The MUOS Program Manager provides computer-based training at the SCS using a system called the Test and Training Simulator (TTS). The TTS is supposed to mimic the operations of the satellite control system. Table 4-10 shows that 80 percent (4 of 5) of responses indicated that the TTS was unsatisfactory. All (5 of 5) of the respondents either somewhat disagreed or strongly disagreed that the TTS was relevant to the tasks they need to perform. Most (3 of 5) strongly disagreed that the TTS prepared them for their assigned duties.

Respondents provided additional comments as part of the surveys. DOT&E noted two common themes in the comments:

- The TTS does not match the current configuration of MUOS.
- The TTS does not include the Orbit Analysis Subsystem, which is important to the performance of satellite controller duties.

The Navy should improve the SCS TTS, to include adding Orbit Analysis Subsystem capability, to make the TTS relevant and effective in training satellite controllers to perform their assigned duties.

Table 4-10. Summary of Satellite Control Segment Computer Based Training Results

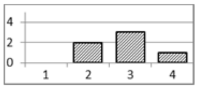
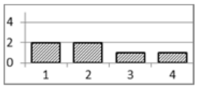
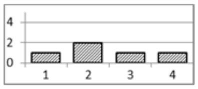
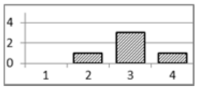
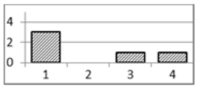
Survey Topic	Mode	Ratings ≥ 3	Distribution
Test and Training Simulator (TTS) was an effective training aid for satellite operations	4	4 of 5	
TTS was relevant to the tasks	4	5 of 5	
TTS prepared operator for assigned duties	4	3 of 5	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

More than half (15 of 27) of all satellite controller responses indicated that OJT was unsatisfactory (see Table 4-11). Eighty percent (4 of 5) of respondents disagreed that OJT prepared them for their assigned duties. Most (4 of 6) of the respondents did not think OJT was well-organized. Most (3 of 5) thought they needed more training. DOT&E noted three common themes in the comments:

- Satellite control engineers are not being trained by Subject Matter Experts. This limits in depth discussions during training.
- OJT does not cover all of the procedures operators are called on to perform.
- Too much time was spent troubleshooting erroneous procedures versus training.

Table 4-11. Summary of Satellite Control Segment On-the-Job Training Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Training was organized well	3	4 of 6	
Trainee had opportunity for hands-on learning with actual equipment	1, 2	2 of 6	
Training was relevant to the tasks	2	2 of 5	
Training prepared trainee for assigned duties	3	4 of 5	
Additional training is needed	1	2 of 5*	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

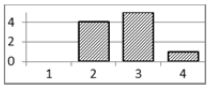
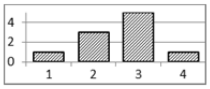
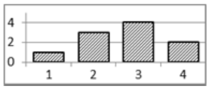
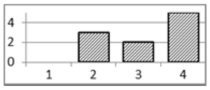
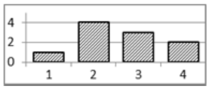
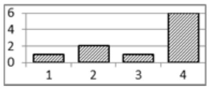
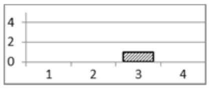
* This question asks about an undesired outcome, unlike most questions, which ask about desired outcomes. Ratings ≥ 3 indicates satisfaction in this case.

Network Management Segment

NMS training consisted of classroom and OJT training. As Table 4-12 summarizes, the 10 respondents were mostly dissatisfied with classroom training. Half of all respondents were dissatisfied with every aspect of Network Management classroom training. Seventy percent (7 of 10) of the respondents disagreed or strongly disagreed that the training prepared them for their assigned duties. DOT&E noted two common themes in the survey comments:

- Respondents desired more classroom training.
- Troubleshooting and failure resolution were not covered sufficiently in training.

Table 4-12. Summary of Network Management Segment Classroom Training Survey Results

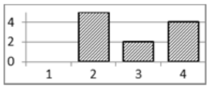
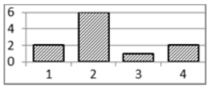
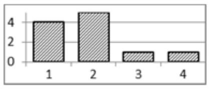
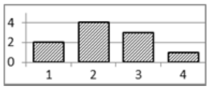
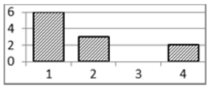
Survey Topic	Mode	Ratings ≥ 3	Distribution
Training was received for the tasks to perform	3	6 of 10	
Training was organized well	3	6 of 10	
Training materials were easy to understand	3	6 of 10	
Trainee had opportunity for hands-on learning with actual equipment	4	7 of 10	
Training was relevant to the tasks	2	5 of 10	
Training prepared the trainee for assigned duties	4	7 of 10	
Maintenance - Training was received to perform tasks	N/A	1 of 1	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

The last row of Table 4-13 shows that 82 percent (9 of 11) of respondents indicated that additional NMS OJT is needed. While most of the respondents thought the provided training was relevant (9 of 11), they did not think is was particularly well organized (6 of 11). On a positive note, 73 percent (8 of 11) of respondents felt the training provided them hands-on training, which is a weakness in many system training programs. DOT&E noted two common themes in respondent comments on the surveys:

- Respondents desired more standardization of the OJT.
- Respondents desired training that explains the purpose behind the procedures. This is a common weakness of the training across the MUOS program. The training focuses on the process of pressing buttons instead of teaching the students why they are taking a particular action and how the system responds. One system administrator told DOT&E, "I learned to do tasks but I do not know why I am doing them."

Table 4-13. Summary of Network Management Segment On-the-Job Training Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Training was organized well	2	6 of 11	
Trainee had opportunity for hands-on learning with actual equipment	2	3 of 11	
Training was relevant to the tasks	2	2 of 11	
Training prepared trainee for assigned duties	2	4 of 10	
Additional training is needed	1	2 of 11*	

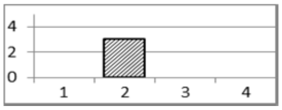
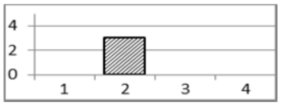
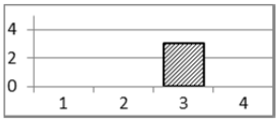
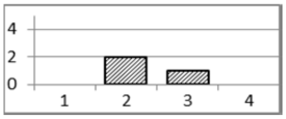
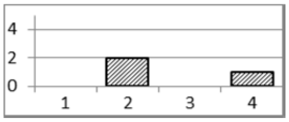
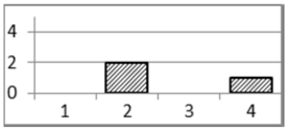
4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)
* This question asks about an undesired outcome, unlike most questions, which ask about desired outcomes. Ratings ≥ 3 indicates satisfaction in this case.

Planning and Provisioning

The Navy provided SMDC/ARSTRAT and RSSC-West planning and provisioning training, consisting solely of classroom training. Table 4-14 summarizes the results of the planning and provisioning training survey results. Two-thirds of responses (12 of the 18) indicated that planners at SMDC/ARSTRAT and RSSC-West found the training satisfactory.

Although all respondents rated the training as overall satisfactory in the survey, they wrote negative comments about the provided training. All respondents found the training material difficult to understand. Training did not provide enough hands-on experience – training was conducted on the live system and trainers were reluctant to allow more than one trainee to build communications services in the MUOS Planning and Provisioning Application (PlanProvApp). The IETMs were not always presented or followed during hands-on exercises. Most importantly, the Navy has not provided the OJT and web-based sustainment training as required by the MUOS Lifecycle Support Plan.

Table 4-14. Summary of Planning and Provisioning Training Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Training was received for the tasks to perform	2	0 of 3	
Training was organized well	2	0 of 3	
Training materials were easy to understand	3	3 of 3	
Trainee had opportunity for hands-on learning with actual equipment	2	1 of 3	
Training was relevant to the tasks	2	1 of 3	
Training prepared trainee for assigned duties	2	1 of 3	

4 point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

The Navy should improve the training and provide SCS, NMS, SMDC/ARSTRAT, and RSSC personnel with additional training, with an emphasis on developing an in-depth understanding of the purpose behind the actions rather than simply "pushing buttons." The Navy should provide the planning and provisioning OJT and web-based sustainment training as required by the MUOS Lifecycle Support Plan.

Documentation

The system documentation is immature, in constant revision, and cannot be accessed by all the personnel who need to access it. The provided documentation is inaccurate, incomplete and does not work on DOD standard internet browser configurations. There is no transition plan in place to prepare the SMDC/ARSTRAT personnel to assume Satellite Operational Manager responsibilities.

Trouble Tickets

During MOT&E-2, 38 percent (55 of 146) of trouble tickets submitted by the network managers, satellite controllers, and communications planners included documentation support. The MUOS personnel submitted 27 trouble tickets requesting that the Navy correct errors in the documentation, and an additional 28 trouble tickets requesting that the Navy provide missing information on the identification and troubleshooting of displayed faults.

Interactive Electronic Technical Manual (IETM) Compatibility

The MUOS-provided IETM is not compatible with Microsoft Internet Explorer version 11 (IEv11) or other approved browsers and cannot be accessed by personnel outside the MUOS boundary. This includes users such as the RSSCs, USSTRATCOM, and SMDC/ARSTRAT. The Navy-Marine Corps Intranet (NMCI) – which the SCS and NMS access – is moving to IEv11 in early 2016, exacerbating the incompatibility problem. As a workaround, the MUOS Program provided the RSSC and SMDC/ARSTRAT planners non-network-connected laptops. This created a loss of functionality, such as failed hypertext links and the inability to view embedded Portable Document Format (PDF) documents. The Navy should provide IETMs that work on DOD standard internet browser environments.

Transition to Operations

There is no transition plan in place to prepare USSTRATCOM to assume Satellite Operational Manager responsibilities, or to prepare the SMDC/ARSTRAT personnel to assume Consolidated – SATCOM System Expert (C-SSE) responsibilities. The documentation for performance management, system monitoring and situational awareness only informs the operator what buttons to push. The Navy has not provided the C-SSE with documentation that describes the system parameters that can be varied, how to manage communications performance, and how changes in communications performance affect system capacity. The Navy, in coordination with STRATCOM and SMDC/ARSTRAT, should develop a plan to transition operational control of MUOS from the developer to the Satellite Operational Managers and C-SSE. The transition plan should document, at a minimum, lessons learned, system defaults, required knowledge, and performance management processes.

User Surveys

The MUOS program office is responsible for providing the IETMs for the operators, maintainers, and planners at SCS, NMS, RSSC, and SMDC/ARSTRAT. COTF surveyed the operators, maintainers, and communications planners concerning the system documentation.

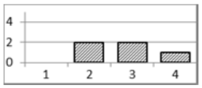
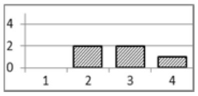
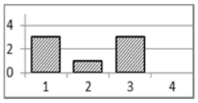
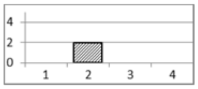
Satellite Control Segment

COTF surveyed the SCS operators and maintainers at the Naval Satellite Operations Center (NAVSOC) on the acceptability of the satellite Telemetry, Tracking, and Commanding (TT&C) documentation. Table 4-15 summarizes the results of the SCS documentation survey. The majority of SCS operators' survey responses (11 of 19) indicated they are dissatisfied with the documentation. DOT&E noted two common themes in the comments:

- The satellite TT&C IETM lacks adequate warnings and cautionary notes.
- Fault isolation procedures in the IETM do not cover all of the faults that are seen by operators.

The Navy should update the satellite control IETM to include adequate satellite control warnings and cautionary notes. Additionally, the Navy should update the satellite control IETM to include comprehensive fault isolation procedures.

Table 4-15. Summary of Satellite Control Segment Documentation Survey Results

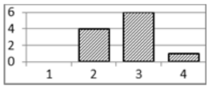
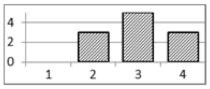
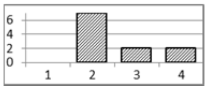
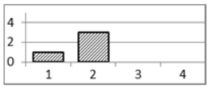
Survey Topic	Mode	Ratings ≥ 3	Distribution
Documentation was available to perform the tasks	2, 3	3 of 5	
IETM task procedures were easy to follow	2, 3	3 of 5	
IETM was a useful reference for safety information (e.g., Notes, Cautions, and Warnings)	1, 3	3 of 7	
Maintenance - Documentation was available to perform tasks	2	2 of 2	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)
IETM – Interactive Electronic Technical Manual

Network Management Segment

Table 4-16 summarizes the NMS documentation survey results. Of the responding NMS operators, 58 percent (19 of 33) indicated dissatisfaction with the documentation. NMS maintainers were satisfied with the documentation.

Table 4-16. Summary of Network Management Segment Documentation Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Documentation was available to perform the tasks	3	7 of 11	
IETM task procedures were easy to follow	3	8 of 11	
IETM was a useful reference for safety information (e.g., Notes, Cautions, and Warnings)	2	4 of 11	
Maintenance - Documentation was available to perform tasks	1, 2	0 of 4	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)
IETM – Interactive Electronic Technical Manual

DOT&E noted four common themes in the survey comments about the IETM:

- It lacks procedures for recurring alarms.
- It needs information about the operational effect of each type of failure.
- It is cumbersome and difficult to navigate, especially when being used for troubleshooting.
- It lacks troubleshooting and correction procedures in the event that a procedure produces erroneous results or the systems behave outside of normal parameters.

These comments are consistent with DOT&E observations during MOT&E-2. The Navy should create a comprehensive list of the failures, faults, and alarms seen at all ground segment sites and update the IETMs with descriptions of the alarms, the operational effects of the failures, and procedures for operators and maintainers to follow.

Planning and Provisioning

The SMDC/ARSTRAT and RSSC planners and provisioners were dissatisfied with the IETM. The lack of compatibility may have contributed to this perception. The SMDC/ARSTRAT and RSSC provisioners and planners thought the IETM procedures were difficult to follow. DOT&E noted three common themes in the survey comments:

- The IETMs did not work with standard DOD operating systems and applications and the RSSC operators had difficulty getting the IETMs into a secure environment.
- The IETMs do not address how to make changes to existing group services.
- The IETM describes how to click buttons but does not contain enough information for the operator to understand why the tasks are being performed or for the planners to understand why to select one parameter input over another.

The Navy should update the technical manuals to provide theory of operation, what the selectable range of each value is, and explanations for why an operation manager, provisioner, or network manager would select one value over another.

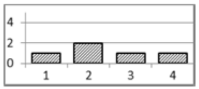
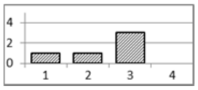
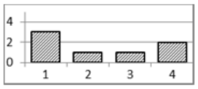
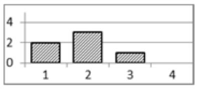
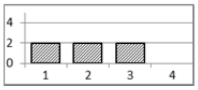
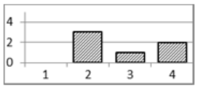
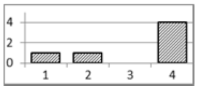
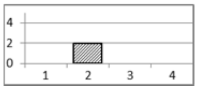
Usability

MUOS is operated via computer workstations at the SCS and NMS, and via web portal at the RSSC and SMDC/ARSTRAT. COTF surveyed operators and maintainers about the usability of the various components of the MUOS.

Satellite Control Segment

Table 4-17 summarizes the responses from MUOS satellite controllers on the usability of MUOS. The results show that 63 percent (26 of 41) of satellite controller survey responses indicate satellite controllers are satisfied with the usability of the system.

Table 4-17. Summary of the Satellite Control Segment Usability Results

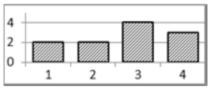
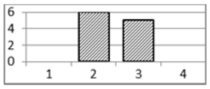
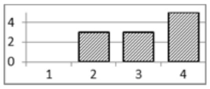
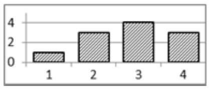
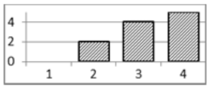
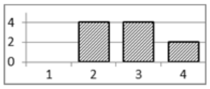
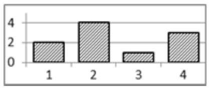
Survey Topic	Mode	Ratings ≥ 3	Distribution
Satellite Control Segment consoles support monitoring task execution	2	2 of 5	
Tasks were difficult to perform	3	3 of 5*	
System alerts notified personnel of a condition requiring immediate action	1	3 of 7	
Information on graphical user interfaces is clearly displayed	2	1 of 6	
Automated features of the system facilitated ease of operations	1, 2, 3	2 of 6	
Operator workstations caused fatigue	2	3 of 6*	
Operator workstations caused eye strain	4	4 of 6*	
Maintenance tasks were easy to perform	2	0 of 2	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)
* This question asks about an undesired outcome, unlike most questions, which ask about desired outcomes. Ratings tions sks are being performed or s case.

Network Management Segment

Table 4-18 summarizes the survey results of the NMS personnel located in Wahiawa, Hawaii. Of the NMS respondents, 71 percent (46 of 65) indicated dissatisfaction with the usability of the system. Consistent with the findings previously discussed in this report, the network managers did not believe the system supported their ability to monitor the system (7 of 11); thought system alerts were not adequate to initiate action (8 of 11); thought displayed information was useful (7 of 11); and thought automated action facilitated ease of operations (9 of 11). Additional comments were also consistent with DOT&E observations. The network managers thought that the failure notification system is too cryptic to be useful and that they have no way to monitor the status of SA-WCDMA communications. The Navy should work with the MUOS network managers to provide them with the information they need to fully understand faults and alarms given by the system.

Table 4-18. Summary of Network Management Segment Usability Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Network Management Segment consoles support monitoring task execution	3	7 of 11	
Tasks were difficult to perform	2	5 of 11*	
System alerts notified personnel of a condition requiring immediate action	4	8 of 11	
Information on graphical user interfaces is clearly displayed	3	7 of 11	
Automated features of the system facilitated ease of operations	4	9 of 11	
Operator workstations caused fatigue	2	6 of 10*	
Operator workstations caused eye strain	2	4 of 10*	

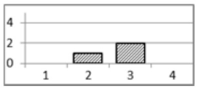
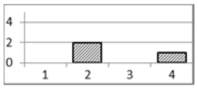
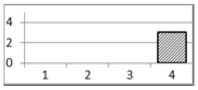
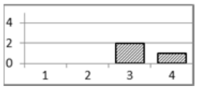
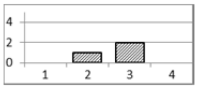
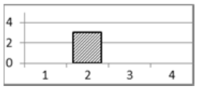
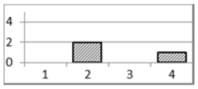
4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

* This question asks about an undesired outcome, unlike most questions, which ask about desired outcomes. Ratings ≥ 3 indicates satisfaction in this case.

Planning, Provisioning & Situational Awareness

Table 4-19 summarizes the results of the usability survey COTF gave to the SMDC/ARSTRAT and RSSC planning and provisioners. In 57 percent (12 of 21) of the responses to survey questions, planners and provisioners indicate they are dissatisfied with the usability of the PlanProvApp and the Situational Awareness application and reports. Over half (5 of 9) of the favorable responses were ergonomic-related questions of whether the system caused eyestrain and fatigue.

Table 4-19. Summary of Planning and Provisioning Usability Survey Results

Survey Topic	Mode	Ratings ≥ 3	Distribution
Network Management Segment consoles support monitoring task execution	3	2 of 3	
Tasks were difficult to perform	2	1 of 3*	
System alerts notified personnel of a condition requiring immediate action	4	3 of 3	
Information on graphical user interfaces is clearly displayed	3	3 of 3	
Automated features of the system facilitated ease of operations	3	2 of 3	
Operator workstations caused fatigue	2	0 of 3*	
Operator workstations caused eye strain	2	1 of 3*	

4-point scale (1=strongly agree, 2=somewhat agree, 3=somewhat disagree, 4=strongly disagree)

* This question asks about an undesired outcome, unlike most questions, which ask about desired outcomes. Ratings ic-related questions of whether the syst

The planners and provisioners had numerous comments on the PlanProvApp and the Situational Awareness application. DOT&E observations of the provisioners and planners performing their work validated their concerns.

Planning and Provisioning

There is no electronic interface between USSTRATCOM's Joint Integrated Satellite Communications Tool (JIST) and MUOS. Planners must manually cut and paste information in satellite access requests (SARs), field-by-field, from JIST into the MUOS and from MUOS back into JIST to create satellite access authorizations (SAAs). The Navy should develop the capability to electronically import JIST SAR data into the MUOS PlanProvApp and auto-populate the SAR fields. USSTRATCOM should develop the capability in JIST to electronically import MUOS PlanProvApp SAA output data into JIST and auto-populate the SAA fields.

PlanProvApp does not provide any indications to the operator of what is considered when determining the "Likelihood of Success" or how the planner could improve the outcome. When conducting network analysis, the system returns with a Likelihood of Success of low, medium, or high for the network that the RSSC provisioner is planning. The IETM does not provide any amplifying information. The Navy should provide an automated means, or update the IETM, to give RSSC operators guidance on how the Likelihood of Success is determined and outline what planning steps operators can take to improve a network that has a low likelihood of success.

The network analysis Likelihood of Success and provisioning Audit Status appear contradictory at times, and there is no documentation or explanation of how each status is deduced. When the system provisions a group network, it provides an analysis on the likelihood of success and an audit status in different windows within the application. The analysis engine may render a "High Likelihood of Success" but the audit status may show that the "Provision Failed." This seems contradictory to the planners and provisioners, and there is no automated guidance or information in the IETM. The Navy should also update the PlanProvApp to provide feedback to planners on why the system renders a network failing provisioning audit and what steps they should take to rectify the failure.

Network analysis and system audits have no indications of progress or even whether the system is still working. The planners have to assume the system is working and continue to wait, or assume that the system is not working and cancel the process and restart. This contributes to inefficient processing of group SARs. The Navy should provide the planners and provisioners a progress indicator so they can tell whether the plan is working or has failed.

Network audits are presented to the planner from the oldest on top to the most recent at bottom, in reverse order of how it should be presented. This forces the planner to scroll through hundreds to thousands of audit statuses to view the most recent audit. The Navy should order the audit status in the PlanProvApp from newest to oldest, instead of oldest to newest as it currently is.

The MUOS-generated SAA is missing necessary information. The MUOS PlanProvApp SAA does not include the following necessary information:

- Type of voice communications access authorized (conversational versus recognition)
- Authorized data rate, based on the type of access

The Navy should update the PlanProvApp to provide type of voice communications type (recognition, conversational) and authorized data rate (2.4, 9.6, 32, 64kbps) based on type of access authorized in the SAA report.

MUOS does not permit selecting Confidential as a security level, resulting in under- or over-classification of plans. The Navy should update the MUOS PlanProvApp to have a selectable Confidential classification, so SARs are not under- or over-classified.

SMDC/ARSTRAT and RSSC operational managers are unable to consistently delete frequency profiles for group networks that are no longer needed. The "zombie networks" remain in deleting status and may reduce system capacity. The Navy should fix the problem with zombie networks that cannot be deleted and consume capability.

USSTRATCOM's JIST defaults to 9.6 kbps for voice communications instead of the more efficient 2.4 kbps, thereby potentially wasting satellite bandwidth. Voice quality is excellent on both 2.4 kbps and 9.6 kbps. Provisioning at 2.4 kbps enables 1,976 accesses per beam while 9.6 kbps enables 494 accesses. USSTRATCOM should update JIST to default to

2.4 kbps voice rather than 9.6 kbps voice for standard access requests so that satellite resources are not overprovisioned.

JIST's SAR and SAA screens and printouts lack classification markings. USSTRATCOM should fix JIST to provide proper classification markings for SAR and SAA screens and printouts.

Situational Awareness

Reports often are not representative of user activity or system status. The information downloaded by network planners from the NMS is inaccurate. At times the system completely fails to render results or will return an erroneous result of "no items found." The problems are shared by the planners and provisioners as well as the Wahiawa network managers – all of whom share the same applications. The Navy should fix the problems with MUOS situational awareness inaccuracies, failed renderings, and missing information.

The Situational Awareness application is slow to react and has tangible wait times for screens to refresh. When the screens do render information, there is a latency of at least 3 – 4 hours from data creation to report availability. When selected, the screens are supposed to refresh automatically to keep current information rendered to the operators. The screens do not refresh automatically when selected. The Navy should fix the problems with the slow and unresponsive Situational Awareness screens, outdated information of the screens, and the inability to perform auto-refreshes.

MUOS provides a capability to export reports to Microsoft Excel for further analysis or archiving. When the RSSC resource planners download the reports to Excel, there are no column titles and the report loses context once downloaded. When downloading the reports, the downloading process often times out, renders page errors, or returns with a "no items found" error. The Navy should fix the problems with downloading situational awareness and performance reports to Excel, including but not limited to missing column headings, system time outs, page errors, and "no items found" errors.

The NMS Situational Awareness application does not contain the information (data rates, services, min/max power, type of access) that planners and provisioners need to perform their mission. The Navy should add operationally relevant information to the Situational Awareness screens and reports.

Safety

The SCS, NMS, RSSC, and SMDC/ARSRAT are operated under controlled environmental conditions with operators at computer workstations or in equipment rooms with racks of electronic equipment. No safety problems were noted during operational testing.

Section Five
Recommendations

The Navy and U.S. Strategic Command (USSTRATCOM) should take the following actions to make MUOS operationally effective and operationally suitable. The Naval Command Operational Test and Evaluation Force (COTF) should verify the corrections in the Follow-on Operational Test and Evaluation (FOT&E).

Operational Effectiveness

The Navy should:

- Restore funding to sustain the MUOS Performance Model so the government can perform independent performance and capacity trades.
- Train the Consolidated Satellite Communications (SATCOM) System Expert (C-SSE) and transfer the responsibility for beam carrier management per the established MUOS documentation.
- Fix the problem with MUOS being unable to process satellite access requests (SARs) with multiple group networks.
- Perform root cause analysis and fix the problems preventing fixed assigned group networks.
- Perform root cause analysis and correct the problems with the Global System View.
- Perform root cause analysis and correct the problems with latent and inaccurate call detail records.
- Fix the problems with inaccurate, incomplete, and missing situational awareness and performance webpage views, reports, and graphs.
- Work with the Defense Information Systems Agency to implement a generic discovery server for the MUOS For Official Use Only (FOUO) and Top Secret enclaves to resolve Internet Protocol (IP) addresses and enable dynamic IP addressing.
- Modify the MUOS Planning and Provisioning Application (PlanProvApp) so the provisioner can load a series of IP addresses and so the system assigns the IP addresses in the sequence loaded. The Navy should also update system documentation and training appropriately.
- Fix the erroneous IP address allocation outside IP subnetworks to avoid deployed user failed communications.
- Work with the Defense Information Systems Agency to implement a SIPRNet and NIPRNet Domain Name Server capability for MUOS.
- Implement a Dynamic Host Configuration Protocol capability in the MUOS waveform to enable dynamic IP assignments for connected devices.

- Perform root cause analysis and correct the underlying problems causing the routine analysis engine failures.
- Conduct loading testing and analysis to determine analysis engine performance based on the Capabilities Production Document's Communication Service Requirements and on multiple Regional SATCOM Support Centers (RSSCs) analyzing networks simultaneously. Resolve any discovered performance constraints.
- Provide the resource planners an automated means to prioritize network provisioning to plan high priority networks before lower priority networks.
- Jointly develop with USSTRATCOM, a MUOS outage notification tool to notify the C-SSE, provisioners, and deployed users of system degradations, outages, carrier frequency problems, and their potential operational effects.
- Explore and implement a plan for the other Services' terminal offices to reduce the overall terminal provisioning time and to increase terminal provisioning success rates.
- Further investigate the differences in terminal provisioning performances observed during the second Multi-Service Operational Test and Evaluation (MOT&E-2) – including terminals provisioning with a single-satellite field of view and terminals provisioning in a two-satellite field of view – and correct any identified problems.
- Model, in coordination with USSTRATCOM, the power control parameter effects on call performance and system capacity when MUOS is at the full communications service requirements.
- Make the MUOS default setting for provisioning voice communications as conversational voice (2.4 kbps) instead of the current default of voice recognition (9.6 kbps), to conserve satellite resources.
- Explore and implement system improvements so users can transition between satellites and beams seamlessly rather than have communication outages.
- Improve network management alert filtering at the Network Management Segment (NMS) to make the alerts descriptive, relevant, timely, and actionable.
- Filter and prioritize alert event notifications consistently across the FOUO and Secret network management enclaves.
- Develop and provide the NMS a tool to directly and actively monitor Defense Information Systems Network interconnections between MUOS sites without operator intervention.
- Develop a technical solution and procedures to perform bulk loading of MUOS Advanced Encryption Standard keys into the MUOS Key Management System. If a technical solution cannot be developed, then the Navy should review staffing levels and adjust them appropriately to ensure military operations are not impaired due to delays in loading sufficient numbers of operational keys.

- Fix the reliability problems with rekey operations that can result in communications outages on a wide-ranging scale.
- Develop the capability to abort rekeys when it is clear that a rekey event will result in communication outages.
- Investigate and implement a means to disable a compromised terminal without requiring a rekey of all other networked terminals.
- Work with the other Services and the National Security Agency to develop a materiel solution, policies, and procedures for profile and cryptographic key portability to support users' concept of operations.
- Fix the known problems with how MUOS determines a group network "Likelihood of Success" that can result in provisioning networks that will fail.
- Fix or mitigate the cybersecurity recommendations in the classified annex to this report.

USSTRATCOM should:

- Update the Joint SATCOM Mission Planning System (JSMPS) to provide the capability for provisioners to be able to modify IP address assignments and select/filter how JSMPS reads in MUOS terminal profile information.
- Jointly develop with the Navy, a MUOS outage notification tool to notify the C-SSE, provisioners, and deployed users of system degradations, outages, carrier frequency problems, and their potential operational effects.
- Review the automated calling performed by the depot contractor and determine if this is a viable solution when MUOS enters into full operations.
- Reconsider its emerging group cover key concept, considering the potential for catastrophic outages for failed rekey events.

Suitability

The Navy should:

- Update the Interactive Electronic Technical Manual (IETM) to ensure there is consistency between the NMS displayed fault severity and the fault severity contained in the IETM.
- Update the IETM to include all alert events, as well as the methods to correct the faults and their potential operational effects.
- Review the allocation of required maintenance actions and allocate maintenance actions to the lowest possible level.
- Update Satellite Control Segment (SCS) and NMS maintainer documentation to correct inaccuracies – to include missing troubleshooting procedures – and provide added detail for in-depth understanding of the purpose behind the procedures.

- Reassess problem change request (PCR) priorities with the user community in light of true operational effects, and prioritize and correct the problems accordingly.
- Develop and adequately fund an executable plan to resolve the large number of high-priority PCRs and trouble tickets before the next operational test.
- Test software installations and develop appropriate procedures prior to delivering them to the operational SCS.
- Determine the root causes of contractor staffing turnover and modify policies as necessary.
- Retrain the MUOS operators, developing contractors, users, and help desk personnel on how to initially prioritize problems.
- Provide additional training to the Space and Naval Warfare Systems Command's help desk personnel on how to handle and assign MUOS help desk calls.
- Perform a configuration audit to determine what systems are in debug mode and bring debug operations under configuration control.
- Improve the SCS simulator, including adding Orbit Analysis Subsystem capability, to make the Test and Training Simulator relevant and effective in training satellite controllers to perform their assigned duties.
- Update the satellite control IETM to include adequate satellite control warnings and cautionary notes and to include comprehensive fault isolation procedures.
- Create a comprehensive list of the failures, faults, and alarms seen at all ground segment sites and update the IETMs with descriptions of the alarms, the operational effects of the failures, and procedures for operators and maintainers to follow.
- Update the technical manuals to provide theory of operation, what the selectable range of each value is, and explanations for why an operation manager, provisioner, or network manager would select one value over another.
- Work with the MUOS network managers to provide them with the information they need to fully understand faults and alarms given by the system.
- Update the PlanProvApp to provide feedback to planners on why the system renders a "network failing" provisioning audit and to tell the planners what steps they should take to rectify the failure.
- Reorder the audit status in the PlanProvApp from newest to oldest, instead of oldest to newest as it is currently is.
- Provide an automated means, or update the IETM, to provide RSSC planners guidance on how the "Likelihood of Success" is determined and what planning steps they can take to improve a network that has a low likelihood of success of working.

- Update the PlanProvApp to provide the voice communications type (recognition, conversational) and authorized data rate (2.4, 9.6, 32, 64kbps) based on type of access authorized in the SAA report.
- Fix the problem with "zombie networks" that cannot be deleted and consume capability.
- Fix the problems with MUOS situational awareness inaccuracies, failed renderings, and missing information.
- Fix the problems with the slow and unresponsive situational awareness screens, outdated information of the screens, and the inability to perform auto-refreshes.
- Fix the problems with downloading situational awareness and performance reports to Microsoft Excel, including but not limited to missing column headings, system time outs, page errors, and "no items found" errors.
- Add operationally relevant information such as data rates, services, minimum/maximum power, and type of access to the situational awareness screens and reports.
- Develop the capability to electronically import Joint Integrated SATCOM Tool (JIST) SAR data into the MUOS PlanProvApp and auto-populate the SAR fields.
- Provide the planners and provisioners a progress indicator so they can tell whether the plan is working or failed.
- Update the MUOS PlanProvApp to have a selectable Confidential classification, so SARs are not under- or over-classified
- Improve training and provide SCS, NMS, RSSC, and SMDC/ARSTRAT personnel additional training with an emphasis on developing an in-depth understanding of the purpose behind the actions rather than simply "pushing buttons."
- Provide the planning and provisioning personnel on-the-job-training and web-based sustainment training as required by the MUOS Lifecycle Support Plan.
- Provide IETMs that work on DOD standard internet browser environments.

USSTRATCOM should:

- Develop the capability in JIST to electronically import MUOS PlanProvApp SAA output data into JIST and auto-populate the SAA fields.
- Update JIST to default to 2.4 kbps voice rather than 9.6 kbps voice for standard access requests so that satellite resources are not overprovisioned.
- Fix JIST to provide proper classification markings for SAR and SAA screens and printouts.

DIRECTOR OPERATIONAL TEST & EVALUATION

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA