ALASKA LAND MOBILE RADIO EXECUTIVE COUNCIL
(A Federal, State and Municipal Partnership)

MEMORANDUM FOR ALMR Executive Council **April 12, 2013**

FROM: DOD Executive Co-Chair

SUBJECT: April 18, 2013, ALMR Executive Council Meeting Agenda

TO: See Distribution

1. Call to Order. Colonel Scott Moser, Department of Defense (DOD) Co-Chair will call the meeting to order at 1:30 p.m. The roll will be taken. (5 min)

2. Opening Statements and Other Announcements. (5 min)

3. Approval of Previous Meeting Minutes. Review of the draft ALMR Executive Council minutes from the March meeting. (5 min) (Atch 1)

> **Motion: Approve March 21, 2013, Executive Council meeting minutes, as written.**

4. Old Business. (30 Min)

a. State of Alaska (SOA) Tower at Donnelly Dome. Mr. Woodall previously advised the council due to the length of time that had passed the package had to be re-accomplished. He stated it had already been sent to Pacific Air Force (PACAF) and from there it would go to Air Force Realty. Colonel Moser advised he would check on the status.

b. Operations Management Office (OMO) Contract. Mr. Woodall previously briefed the council that the DOD was now outside of the contract completion window and could no longer pursue a sole source contract. He stated the DOD was looking at extending the current contract anywhere from one to three months, but the difficulty with doing this is the different pricing based on the new cost share. He advised the council the State may also not be able to extend their contract with the FY14 cost increases included because cost would increase by over 20 percent, but he was still waiting on the State to make that determination.

c. Service Level Agreement (SLA) change. At the March meeting, Mr. Del Smith, Operations Manager, briefed that the User Council had recently approved the new System Key Management Procedure with the most up-to-date processes required for System security. He advised these new procedures make some language in Appendix C to the SLA obsolete. Mr. Smith stated the OMO prepared a change to SLA Appendix C (Atch 2) to correct this, which would cover the affected pages and would be marked accordingly.

5. **User Council Update.** (Major Matt Leveque, Chair) (5 Min)

6. **Operations Management Office.** (Mr. Del Smith) (10 Min)

   a. March System metrics (Atch 3)

   b. 7.13 Migration status update

   c. Clear site status

   d. State of Alaska audit

7. **New Business.** (15 Min)

8. **Next Meeting.** The next meeting is scheduled for May 16, 2013, 1:30 p.m. at the Department of Public Safety Training/Conference Room, 5700 E Tudor Road. (5 Min)

9. **Adjourn Meeting.** (5 Min)

Scott E. Moser

SCOTT E. MOSER, Colonel, ALCOM/J6
Department of Defense Alaska Co-Chair
ALMR Executive Council

3 Attachments:
1. Draft March Meeting Minutes
2. Revised Service Level Agreement Appendix C
3. March System Metrics

Distribution:
ALCOM/J60, Colonel Scott Moser
SOA DPS, Commissioner Joseph Masters
AFEA, ASAC Darrin Jones
AML, Chief Jeff Tucker
MOA, Lt Ken Spadafora
User Council, Major Matt Leveque
OMO, Mr. Del Smith
ALCOM/J64, Mr. Timothy Woodall
SOA ETS, Mr. Jim Kohler
SOA ETS, Mr. Adam Paulick
MOA, Mr. Trygve Erickson
MOA, Mr. Jason Beach

ALASKA LAND MOBILE RADIO EXECUTIVE COUNCIL
(A Federal, State and Municipal Partnership)

MEMORANDUM FOR ALMR Executive Council **April XX, 2013**

FROM: DOD Executive Co-Chair

SUBJECT: March 21, 2013, ALMR Executive Council Meeting Minutes

TO: See Distribution

Executive Council Members Present:

Colonel Scott Moser	Department of Defense (DOD) - Alaskan Command
Commissioner Joe Masters	State of Alaska (SOA) - Department of Public Safety
Assistant Special Agent in Charge Darrin Jones	Alaska Federal Executive Association (AFEA) - Federal Bureau of Investigations
Chief Jeff Tucker	Alaska Municipal League (AML) - North Star Volunteer Fire Department (via teleconference)
Lt Ken Spadafora	Municipality of Anchorage (MOA) - Office of Emergency Management

ALMR Support Team Members and Guests Present:

Major Matt Leveque	User Council Chairman - Alaska State Troopers (via teleconference)
Mr. Del Smith	Operations Manager, ALMR
Mr. Adam Paulick	Acting Director, Enterprise Technology Services (ETS)
Mr. Jim Kohler	ETS Telecommunications Special Projects Administrator (via teleconference)
Mr. Tim Woodall	Department of Defense QA/QC
Mr. Bruce Richter	Office of Emergency Communications Region X Coordinator

Ms. Sherry Shafer	Operations Management Office (via teleconference)
Ms. Sharon White	Enterprise Technology Services (via teleconference)

1. Call to Order. Colonel Scott Moser, Department of Defense (DOD) Co-Chair, called the meeting to order at 1:36 p.m.

2. Opening Statements and Other Announcements. None.

3. Approval of Previous Meeting Minutes. Colonel Moser asked the Executive Council if they had reviewed the February meeting minutes and if they had any requested changes. Hearing no changes, Colonel Moser requested a motion be made.

> **Motion: Approve February 21, 2013, Executive Council meeting minutes, as written.**

The motion was made by Assistant Special Agent in Charge (ASAC) Jones to accept the minutes with the proposed change and seconded by Commissioner Joe Masters. There were no objections. **The motion was carried and approved.**

4. Old Business.

a. State of Alaska (SOA) tower at Donnelly Dome. Colonel Moser asked Mr. Tim Woodall to provide the update on this issue. Mr. Woodall advised the council due to the length of time that had passed the package had to be re-accomplished. He stated it had already been sent to Pacific Air Force (PACAF) and from there it would go to Air Force Realty.

Colonel Moser advised he would contact PACAF tomorrow and check on the status.

Mr. Woodall briefed that the Alaskan Command (ALCOM) had asked for approval to move forward without the paperwork, but were not approved to do so.

b. Operations Management Office (OMO) FY14 contract. Mr. Woodall advised the council that the DOD was now outside of the contract completion window and could no longer pursue a sole source contract at this time. He stated DOD was looking at extending the current contract anywhere from one to three months but the difficulty with doing this is the different pricing based on the new cost share. Mr. Woodall briefed he had been in contact with Ms. Karen Morgan, Wostmann & Associates Inc., and she was going to provide him with the pricing. He ~~also~~ advised the council the State ~~also~~ may also not be able to extend their contract with the FY14 cost increases included because cost would increase by over 20 percent. ~~–~~He stated he is waiting on the State to make that determination. Mr. Woodall stated the final issue with the extension was that the current contract allocation of 50 percent was not projected with the services, only the 12 percent based on the new cost share, which may result in a funding shortage.

5. User Council Update.

Major Matt Leveque briefed the council that the State had uploaded their State and Local Implementation Grant Program (SLIGP) application ~~to request grant funds from~~to FirstNet. He explained that FirstNet is ~~supposed to be able~~charged with developing and deploying a ~~to provide future~~ public safety long-term evolution (LTE) ~~interoperability~~ interoperable data network across the United States.

Major Leveque advised that if accepted, the grant program ~~this~~ will ~~let~~enable Alaska to tell the National Telecommunications and Information Administration (NTIA) and FirstNet what networks Alaska has currently and how we think FirstNet should deploy the LTE network in ~~it should look like in~~ Alaska. Another objective of the SLIGP is to another objective of the SLIGP is to enhance Statewide Interoperability Governance Bodies (SIGB). He explained that currently the state's SGIB is ~~has~~ the Alaska ~~Interoperability~~ Interoperable Communications Committee (AKICC) which is kind of an orphan at the moment. Major Leveque advised that ~~Commissioner Masters allowed AKICC to coalesce with~~ Division of Homeland Security and Emergency Management has agreed to transfer the Statewide Interoperability Coordinator (SWIC) functions to DPS. Combining that responsibility with ~~and~~ the State 911 Coordinator, who is already within DPS may allow for greater coordination.~~and he believes this will allow for better coordination in the future.~~

Commissioner Masters stated a lot of the responsibility for pulling these functions together had fallen on Major Leveque and requested he address the perception that FirstNet will take over voice communications.

Major Leveque advised the council this is absolutely not the case. ~~He stated modern I-phones® would be able to operate on it but this system is designed at this time for data only for public safety.~~ He explained that while LTE can support voice communications, FirstNet was intended to be a data network, first and foremost. Secondly, LTE doesn't currently offer 'mission critical' voice reliability and experts say that it could be many years before that capability is reached. Major Leveque briefed ~~the problem is figuring out how to integrate it into the current public safety systems. He stated that there is probably eight to ten years before that will happen and~~ that we will need to maintain ~~our~~ ALMR system~~s~~ for the foreseeable future.

Commissioner Masters emphasized that it was important for council members to head off any discussions this would be a replacement for ALMR.

Mr. Smith advised the council he was at the International Wireless Communications Expo (IWCE) the previous week and there had been a lot of presentations regarding LTE. He briefed the council there would be an article in the April edition of the *Insider* newsletter to cover the point that it would not replace ALMR. Mr. Smith pointed out that currently the ALMR System has 83 sites to cover the current footprint. He stated with the LTE system, you would probably need a 100 more sites in between.

Colonel Moser asked if the idea was that this would be a state-owned system.

Major Leveque stated no; at this point the expectation is that while states will have significant roles in controlling system access and availability, FirstNet is the organization that will own the network(s) across all 56 states and territories. In addition, there was no business plan developed yet so there is no way to estimate what it might cost for agencies to participate once the network was established in Alaska. ~~He advised what it might look like is similar to our current system but leveraging commercial systems to support it, such as ALMR plus utilities.~~ There are expectations that FirstNet will attempt to leverage existing infrastructure, including that owned by cities, utilities, commercial carriers and the state, but that those might be difficult agreements to negotiate due to first responders' needs to preempt all (or most) non first responders during major emergencies. ~~Major Leveque briefed he sees this as problematic for public safety being on commercial carriers.~~

Colonel Moser briefed the council there were cases he recalled where commercial carriers had solicited the DOD, but were turned down. He stated they don't understand the complexities of public safety networks.

Major Leveque briefed that the future costs are unknown but it had been sold to Congress highlighting the function of streaming video.

ASAC Jones stated the Federal Bureau of Investigation had paid significantly more for something like it and it was not economically feasible.

Mr. Smith stated he could not foresee Verizon putting sites where it was not economical.

6. Operations Management Office.

a. System Metrics. Mr. Del Smith presented the February System metrics to the council. He stated they were about where they would normally be expected for this time of year.

b. Kenai and Kasilof sites. Mr. Smith advised the council that both the Kenai and Kasilof sites had capacity upgrades the previous week. Kenai received two new channels and Kasilof received one new channel. Mr. Smith briefed that both sites saw zero busies over the weekend immediately following the upgrade but he was anxious to see the metrics after a week's time.

c. Clear site. Mr. Smith advised the council that the Clear AFS personnel's radios were prohibited from accessing the Clear site and the effect of increased traffic on the other sites in the area was being monitored.

d. 7.13 Migration. Mr. Smith briefed the council that the project teams and the OMO are soon to start meeting via teleconference every Tuesday with Motorola® and the system cutover is expected to occur August 5 - 20.

Colonel Moser asked when the migration was expected to be finished.

Mr. Woodall explained that the migration would be completed by the end of August but after that there would still be an Acceptance Test Procedure to do, as well as an information assurance scan which takes approximately two weeks. He advised the current Motorola® contract runs into October but this could not and would not occur; everything had to be finalized prior to the end of the current Federal fiscal year.

Mr. Smith advised he had been in touch with the dispatch centers finding out what they intended to do during outages. He stated he also understood Motorola® was up to do some pre-testing with the Anchorage Wide Area Radio Network (AWARN) and they had been unable to get past 7.5, although AWARN has the latest equipment installed. Mr. Smith briefed the council that all the project teams are working together to mitigate the impacts to the users to the greatest extent possible.

Mr. Woodall stated the one thing that everyone cannot predict is the number and length of the outages.

e. Service Level Agreement (SLA) change. Mr. Smith briefed the council that recently the User Council had approved the new System Key Management Procedure and the language in the new procedure is the most up-to-date processes required for System security. However, he advised that these new procedures make a section of one of the SLA attachments obsolete. Mr. Smith stated the OMO proposes to do a change as a SLA attachment to correct this, which would cover only those affected pages and they would be marked accordingly. He advised the front cover would also be annotated to reflect the change, the same as it was when the service response times were changed by the State for their sites. Mr. Smith stated it was not a substantial change requiring a new SLA be signed.

Colonel Moser asked if those individuals doing the work had seen the new procedure.

Mr. Smith briefed that the new procedure had been sent out and also posted to the web site. He advised there is no timeline to change the SLA, but it is currently in conflict.

Colonel Moser asked the other council members to review the changes and be prepared to vote at the next meeting.

7. <u>New Business</u>.

a. System Change Requests (CRs). Mr. Smith advised the council members there were a number of CRs for approval and with the council's permission; he would get signatures after the end of the meeting. There were no objections to this request.

b. State Budget. Mr. Jim Kohler requested to provide a short overview of where the State budget process was at. He stated at the last meeting the House Finance Sub-committee had hacked out significant dollars from the budget; however, the House Finance Committee had returned the $500K back in general funds to cover municipal contributions toward the cost share. Mr. Kohler briefed the House Finance Committee let the Department of Administration increment request for $600K reduction by the Finance sub-committee stand.. He stated the Senate Finance Sub-committee was much friendlier toward the budget as a whole and he was very optimistic the Senate budget version would have full funding included. Mr. Kohler advised it should be released next week after the Senate passes their version. He stated, as a whole, it looks a lot better than a month ago.

Commissioner Masters advised there was a lot of participation by key stakeholders including the Department of Administration, the Department of Transportation, the Department of Public Safety and the Alaska Municipal League, which was in sharp contrast to the years prior.

c. State Legislative Audit. Mr. Smith advised the council that the OMO was still dealing with the State audit providing information and documents as they were requested. He stated auditors had requested all the information be provided by April 3

8. Next Meeting. Colonel Moser briefed the next meeting is scheduled for April 18, 2013, 1:30 p.m. at the Department of Public Safety Training/Conference Room, 5700 E Tudor Road.

9. Adjourn Meeting. Colonel Moser asked if there were any other items for discussion. Hearing none, he sought a motion to adjourn.

Motion: Adjourn the March monthly Executive Council meeting.

The motion was made by ASAC Jones and seconded by Commissioner Masters. There were no objections. **The motion was carried and approved.**

The meeting adjourned at 2:14 p.m.

SCOTT E. MOSER, Colonel, ALCOM/J6
Department of Defense Alaska Co-Chair
ALMR Executive Council

Distribution:
ALCOM/J60, Colonel Scott Moser
SOA DPS, Commissioner Joseph Masters
AFEA, ASAC Darrin Jones
AML, Chief Jeff Tucker
MOA, Lt Ken Spadafora
User Council, Major Matt Leveque
OMO, Mr. Del Smith
SOA ETS, Mr. Adam Paulick
ALCOM/J64, Mr. Timothy Woodall
SOA ETS, Mr. Jim Kohler
MOA, Mr. Trygve Erickson

Appendix C
Operations and Maintenance Processes and Procedures

These processes/procedures include specific tasks/activities with associated responsibilities identified for site owners, users, System infrastructure operations, the Executive and User Councils.

The certification/training requirements of the staff performing the tasks/activities within these procedures/processes must be identified. These processes/procedures must be followed and sustained. Any changes, considered or required, must be managed by the included Change Management Process.

1.0 Asset Management Process

1.1 The asset management process will be utilized to effectively track and manage System assets that are utilized for operations and support, including active and spare System equipment.

1.2 Users and the System Management Team will track and manage installs, moves, additions, deletions, and changes to System equipment. Updates will be made within 48 hours of a change in status or location of the asset.

1.3 The System Management Team will utilize a database to provide a tracking mechanism for user System assets. System equipment items to be tracked include the following:

1.3.1 User ownership

1.3.2 Model/part number

1.3.3 Serial number

1.3.4 User asset number

1.3.5 RF frequency (if applicable)

1.3.6. Software and firmware version

1.3.7 Equipment location

1.3.8 Site/area assignment (for spares)

2.0 Call Management Process

The Technical Support Team problem ticket system will be used by all support team levels (where approval and technical access has been granted) to record and track all problem reports, inquiries or other types of calls received for support. This provides the Technical Support Team with the ability to provide metrics with regard to this SLA.

3.0 Change Management Process

The Change Management Process will be used by all Technical Support Teams, where approval and technical access has been granted, to record and track all change requests or actions required for support. This provides the Technical Support Team with the ability to provide status with regard to System changes for this SLA.

3.1 Add/Change/Delete Procedures.

Each agency authorized to have subscriber radios on the System will, at some point, need to begin operating on the System, make modifications to their subscriber database or modify the talk groups. The following procedure establishes the Add/Change/Delete process that will be required for all users that operate on the System.

3.2 Adding New Units for Existing Agencies.

If a user already operates radios on the System and needs to add a new serial number with a new alias, the following procedure will be adhered to:

3.2.1 Using the Customer Programming Software (CPS), the user will read the radio and email the information or bring a copy of the codeplug into the System Management Office (SMO). Contact the communications service provider for a copy of the CPS to accomplish this step. If all of the radios are of the exact same model, users do not need more than one codeplug. If there is more than one type of radio, users will need a codeplug from each type.

3.2.2 Along with the codeplug, fill out the Add/Change/Delete form at para 14.0. Provide the SMO with a complete listing of serial numbers and aliases attributed to each serial number. An Excel spreadsheet may be attached to the form, but the form must be filled out for tracking purposes.

3.2.3 The SMO will modify the codeplug and ship it back to the designated Communications Service Provider. Also, send the SMO will send the user a document with all of the assigned System ID numbers. This information is required to clone radios.

3.2.4 Use the codeplug to clone radios using the information provided by the SMO. This step will require the use of an Advance Systems Key (ASK). Please refer to the Membership Agreement under paras 3.7.2.1 – 3.7.2.5 for more information.

3.2.5 Once all of radios are cloned, test each function of the radio. If there are any problems/questions, please contact the SMO.

3.3. Reporting Lost or Stolen Radios.

As soon as it is known a radio on the System has been lost or stolen it must reported to the SMO. Provide to the SMO with the Serial Number/ID number of the missing radio. If the loss or theft of a particular radio is of an urgent nature it can be reported after normal business hours.

Using the Network Management Terminal, the identified radio will be disabled. When this radio is powered on by anyone, the radio will completely go dead and all functions will be inoperative. If the radio is found, please contact the SMO and they can reinitiate the radio. For the security of the overall System, it can not be over emphasized to maintain positive control of all of your System assets.

3.4. Changing an Existing ALMR Radio.

The processes discussed above are changes to a radio. Therefore, the Add/Change/Delete Form must be filled out. Cloning a radio does not require anything to be done in the Network Manager Terminal.

3.5. When Change Forms are Required.

3.5.1 Issued a spare radio and required to change the alias/serial number/ID number of a radio.

3.5.2 Upon personnel change and require the changing of an alias/serial number/ID number of a radio.

3.5.3 Changes to some features.

3.5.4 Possess a cloned a radio and discovered multiple radios with the same information.

3.6 Changing a Radio.

Changing information in a radio requires that the radio itself be modified and similar information be changed in the Network Management System. If this procedure is not followed, it is likely the radio will become inoperative after the changes have been made to the radio. To ensure the database is current, the following procedure must be adhered to:

3.6.1 Using the radio programming software, make the desired changes.

3.6.2 Fill out the required areas on the Add/Change/Delete form and email/send the form to the SMO.

3.6.3. If the change is required immediately, follow-up with a phone call. Normally changes can be made within 24 hours of receiving the Add/Change/Delete form. Users will be notified by the SMO when the change is complete.

NOTE: Users with access to a Network Manager Terminal are authorized to make changes on radios within their fleet. The Add/Change/Delete form must still be filled out and sent into the System Manager's office.

3.7 Deleting a Radio.

3.7.1 If a radio is deemed to be lost or damaged beyond economical repair, the decision may be made to delete the radio from the inventory. To keep the inventory accurate, it will be necessary to fill out the Add/Change/Delete form so the radio and ID number can be deleted from the Network Management System.

3.7.2 Fill out the Add/Change/Delete form with all pertinent information. Add the status or reason for this deletion in the information area.

3.7.3. Advanced System Keys. The System Management Office (SMO), as the primary System Key holder, is responsible for managing all System Key technology. The ASK/System Key, and the management of these devices, is established in the Membership Agreement signed by each user.

3.7.3.1 The SMO will:

- Maintain and manage the Master System Key for all manufactures of equipment approved to operate on the ALMR System.
- Program the physical System Key for requesting agencies with the necessary parameters, once the proper hardware is provided by the agency.
- Authorize the use of, or issue, the software System Keys, for those manufacturers who do not provide a physical System Key, to authorized self-maintained member agency's technicians and/or to manufacturer-authorized service vendors that maintain equipment for ALMR agencies, as they become available, and upon request.
  NOTE: Some manufacturers charge a fee for their Software System Key. When purchasing subscriber units, ensure you are aware whether or not the manufacture charges for the initial key or update keys.
- Will destroy the software System Keys they manage, as they become obsolete.

3.7.3.2 Agencies will:

- Be responsible for acquiring/purchasing the proper programming software, hardware (iButton and iButton readers, or equivalent security device), and

licenses necessary to program the subscribers they utilize, which utilize physical System Keys.

- Not distribute, disclose to, or permit any unauthorized party to view, read, print, extract, copy, archive, edit, create, clone, transfer, tamper with, or otherwise compromise the security of any codeplug programming file, System Key file, System IDs, encryption key file, template, or talkgroup information for any agency on ALMR, for any reason.
- Immediately notify the ALMR Help Desk of a security breach in the event they learn that any party has improperly or fraudulently obtained any radio codeplug file, System Key, System ID, encryption key, template, or talkgroup information.
- Be responsible for the cost of all reprogramming necessary to overcome said breach and subject to sanctions, including loss of programming authorization, if determined to be at fault.
- Destroy manufacturer System software keys as they become obsolete, or when directed to do so by the OMO or SMO.
- Be prepared to replace all System Key hardware, which will be programmed to expire every three years.
- Provide an audit report for software System Keys to the SMO every three years showing location and who has access.
- Program only those subscriber ID(s) for their own agency or agencies they provide subscriber maintenance for and program only those shared talkgroups for which there is an approved Talkgroup Sharing Agreement on file with the OMO
- Program all subscriber units to allow "Radio Inhibit" from the System Network Management Terminal
- Program all subscriber units for write-protect file access only, if the equipment supports the write protect function
- Archive the file from the radio prior to shipping any radio to the vendor for repair (**NOTE: Radios may be sent with the programming intact. It is <u>not</u> recommended to ship radios to any vendor with encryption keys intact.**)
- Verify radios for correct codeplug information and that they are write-protected, if capable, when returned from vendor repair.
- Maintain current and accurate records of all programming performed; codeplugs and subscriber units are subject to audit by the SMO

3.7.3.3 Vendors will:

- Be responsible for acquiring/purchasing the proper programming software, hardware (iButton and iButton readers, or equivalent security device), and licenses necessary to program the subscribers they support, which utilize physical System Keys.
- Not distribute, disclose to, or permit any unauthorized party to view, read, print, extract, copy, archive, edit, create, clone, transfer, tamper with, or otherwise compromise the security of any codeplug programming file, System Key file,

System IDs, encryption key file, template, or talkgroup information for any agency on ALMR, for any reason.

- Immediately notify the ALMR Help Desk of a security breach in the event they learn that any party has improperly or fraudulently obtained any radio codeplug file, System Key, System ID, encryption key, template, or talkgroup information.
- Be responsible for the cost of all reprogramming necessary to overcome said breach, and subject to sanctions, including loss of programming authorization, if determined to be at fault.
- Destroy manufacturer System software keys as they become obsolete, or when directed to do so by the OMO or SMO
- Be prepared to replace all System Key hardware, which will be programmed to expire every three years.
- Provide an audit report for software System Keys to the SMO every three years showing location and who has access.
- Program only subscriber ID(s) for agencies they provide subscriber maintenance for and program only those shared talkgroups for which there is an approved Talkgroup Sharing Agreement on file with the OMO.
- Program all subscriber units to allow "Radio Inhibit" from the System Network Management Terminal.
- Program all subscriber units for write-protect file access only, if the equipment supports write-protect function
- Verify for correct codeplug information and that they are write-protected before returning to the agency.
- Maintain current and accurate records of all programming performed; codeplugs and subscriber units are subject to audit by the SMO

3.8 Some users have access to a System Management Terminal. With this terminal, they will be authorized to make some changes, such as adding/deleting of certain information for certain location/agencies. Even though they may have the ability to make these changes, this does not negate the requirement to inform the SMO of any changes. Talk groups will not be added without the approval of the SMO and may require additional coordination. Any addition of serial numbers may require modification of the ASK permissions. This process must be followed, even though the user is making the requested changes themselves.

3.9 The System does not manage or control the use of Encryption Keys. Agencies that have, or require the use of, a KMF for OTAR must establish their own internal procedures to ensure any asset changes, such as adding/deleting of radios, are kept current in the KMF database.

3.10 Security and overall management of total System assets requires that all users understand and follow these procedures.

4.0 Configuration Management Process

The Technical Support Team configuration management processes will be used by all support team levels, where approval and technical access has been granted, to record and track all change requests or actions required for the network, infrastructure, consoles, radio sites, connectivity bandwidth, construction, permitting, liabilities, etc. This provides the Technical Support Team with the ability to provide status with regard to System configurations for this SLA.

NOTE: Configuration management must comply with the national consensus standard as defined within the commercial standard ANSI/EIA-649.

5.0 Customer Support Plan (CSP)

The System is a shared system between DOD, SOA, and other federal and local government agencies. The purpose of the CSP is to describe the services, processes and procedures to be delivered in support of the System, and additional areas of the System including microwave network transport and encryption equipment.

6.0 Disaster Recovery Planning

Natural Disasters include, but are not limited to, earthquakes, tsunamis, volcano eruptions, etc. During a disaster activity, usage of the System is expected to be high. The following are areas of expected increase for operations:

6.1 Scheduling of personnel. During this time, the System Management Team will go on a higher level of total System monitoring, closely assessing the effected area for loading and service issues.

6.2 Activate Network Monitoring Office/System Service Center (NMO/SSC) to Higher Monitoring. The NMO/SSC will be notified of the disaster. They will be staffed with appropriate personnel to assist in monitoring and resolving issues throughout the emergency.

6.3 Other Support Personnel. Contract support personnel such as ProComm and North Slope will be activated to assist with issues, as necessary. Additionally, management and technical personnel from DOD/SOA DOA/Enterprise Technology Service (ETS)/SATS will be included in System management and restoration during the disaster.

7.0 Help Desk

7.1 Call Taking, Tracking, and Dispatching.

7.1.1 The System infrastructure support process includes Help Desk Technical Support, call taking/tracking and dispatch operations. To provide support to the

System, Dispatch Operations is available 7 days/week, 24 hours/day (including holidays) to provide a central point of contact for all System service requests. Users and System Management Team personnel can contact the Help Desk to request service, request information, or inquire on an open case via telephone at 1-888-334-2567 outside the Anchorage area or 334-2567 within Anchorage.

7.1.2 The Help Desk will dispatch appropriate factory trained and authorized service personnel and provide call management by tracking the progress of all System infrastructure service issues to completion. The Help Desk will utilize the Customer Support Plan for information in regard to the System infrastructure equipment that includes performance history, location and site access requirements, and the site contacts. Upon notification by a user or System Management Team personnel in the field or via remote network monitoring detected issues, the Help Desk will open a case to track service activities reported. The Help Desk will notify users or System Management Team personnel by email or pager of the events occurring during the existence of the issue.

7.1.3 To provide call taking/tracking, and dispatching, the Help Desk will:

7.1.3.1 Be continuously available 24 hrs/day, 365 days/year to receive phone calls from Users for service requests, information requests, or to report and update current cases.

7.1.3.2 Remotely access the System via remote network capabilities to immediately respond to critical (Severity Level I and II) issues.

7.1.3.3 Manage and report responses, on behalf of the System and user or vendor activities, performed for remote and on-site equipment restoral efforts.

7.1.3.4 Create a case, as necessary, when service and information requests are received.

7.1.3.5 Gather information to perform the following:

7.1.3.5.1 Characterize the issue

7.1.3.5.2 Determine a plan of action

7.1.3.5.3 Assign and track the case to resolution.

7.1.3.5.4 Dispatch an ST to the equipment site, as required

7.1.3.5.5. Ensure the required personnel have access to User information, as necessary.

7.1.3.5.6 Maintain contact with the on-site ST(s) until System restoral occurs, and the case is closed.

7.1.3.5.7 Verify with the System Management Team that restoration is complete, or System is functional.

7.1.3.5.8 Escalate the case to the appropriate party upon expiration of a response time.

7.1.3.5.9 Close the case upon receiving notification from the servicer, User or vendor, indicating the case is resolved.

7.1.3.5.10 Notify user of case status, as required by the Customer Support Plan at the following case levels

7.1.3.5.10.1 Open and closed; or

7.1.3.5.10.2 Open, assigned to the servicer, arrival of the servicer on site, deferred or delayed, closed.

7.1.3.5.10.3 Provide case activity reports, when requested.

7.1.3.5.11 Continuously track and manage case activity from open to close through an automated case tracking process.

7.2 Infrastructure Technical Help Desk Support.

The System infrastructure support process also provides Technical Help Desk Support services in situations where the user, System Management Team or on-site ST needs additional assistance or information to address an issue or affect System restoral.

7.2.1 Technical Help Desk Support. Technical Help Desk Support services provide centralized remote telephone support for System infrastructure technical issues that require a high level of communications systems expertise or troubleshooting. The Technical Help Desk Support team is staffed with technologists who specialize in the diagnosis and resolution of System performance issues. This must include expertise in current System technologies such as ASTRO 25™.

7.2.2 Provided Services. Technical Help Desk Support provides for the following to be provided to the users and System Management Team(s):

7.2.2.1 Respond to requests for Technical Help Desk Support for System issues including restoration of failed systems and diagnosis of operation problems or issues.

7.2.2.2 Advise caller of procedure for determining any additional requirements for issue characterization, restoration, including providing a known fix for issue resolution when available.

7.2.2.3 Attempt remote access to System for remote diagnostics, when possible.

7.2.2.4 Maintain communication with the servicer or user in the field until close of the case, as needed.

7.2.2.5 Coordinate technical resolutions with agreed upon third-party vendors, as needed.

7.2.2.6 Escalate and manage support issues, including systemic issues, to the appropriate vendor/contractor engineering and product groups, as required.

7.2.2.7 Escalate the case to the appropriate party upon expiration of a response time.

7.2.2.8 Provide configuration change support and work flow changes to systems that have dial in/remote access capability.

7.2.2.9 Determine, in its sole discretion, when a case requires more than the Technical Help Desk Support services and notify the user of an alternate course of action.

7.3 Issue Reporting Procedure Description.

The SmartZone System is comprised of thousands of Users operating on multiple sites that utilize different mediums of connectivity. The Issue Reporting Procedure is for all System users, administrators and service providers. It is the intent of this procedure for all System participants to have a consistent process to enable them to call one number to report all System issues. Additionally, this will allow the System Management Team the ability to capture, track and report all issues. While this process is designed to deal primarily with System infrastructure, it will accept all calls dealing with possible communications service issues relating to the System.

7.3.1 System infrastructure:

7.3.1.1 RF sites

7.3.1.2 Network management systems and subsystems

7.3.1.3 KMF/OTAR subsystems

7.3.1.4 Bulk encryption

7.3.1.5 Microwave backbone

7.3.1.6 Telephone interconnect systems (T1 where the System is the data user)

7.3.1.7 Bi-directional amplifiers (BDAs)

7.3.1.8 MOSCAD systems

7.3.1.9 Motobridge™ Gateway Units

7.3.1.10 Transportable/deployable systems (not currently part of this CSP)

7.3.1.10.1 If the user issue with the subscriber is related to the System, use the Issue Reporting Procedure.

7.3.1.10.2 In many cases, a dispatch console will not be covered under the System Wrap-Around Warranty Service. Call if you feel it is a System problem. The on-call System Technician will evaluate your concern and coordinate a solution.

7.3.1.10.3 Each user will be asked to provide a primary and an alternate contact name. The user will, if possible, route all System service calls through these contact individuals.

NOTE: Subscriber units such as mobiles and portables, consoles and logging recorders are not considered Infrastructure and are normally maintained by the user's selected radio service provider. This does not mean that this procedure cannot be used in an emergency.

7.3.2 System On-Call Procedures for Normal and After Normal Business Hours.

7.3.2.1 Call 1-888-334-2567 outside of the Anchorage area or 334-2567 within Anchorage

7.3.2.1.1 Push Prompt #1

7.3.2.1.2 Push Prompt #2 to reach vendor/contractor System Support Center (SSC)

7.3.2.2 The SSC will ask for a Site ID:

7.3.2.2.1 The user will provide: SZ0142

7.3.2.2.2 The SSC will ask other questions to better identify user's location

7.3.2.2.3 The user will convey the issue and contact information to the SSC

7.3.2.2.4 The SSC will assign a case number

7.3.2.2.5 User records the case number

7.3.2.3 SSC will page an on-call technician who then calls the user

7.3.2.4 The on-call technician will work through the user's issue, involving other agencies if necessary

7.3.2.5 The user will be called when the issue is resolved

8.0 Inventory Property Books

Inventory management involves the management of communication assets. Management of inventory records for fiduciary, financial, or audit purposes is the responsibility of each user for their respective asset inventory. The System Management Team will track and manage modifications to data records, as they are communicated. This includes providing information to each user and can include information such as warranty expiration events, changes in equipment location, or effective status (i.e. no longer functioning, unable to repair, lost/stolen/damaged, etc.)

8.1 Spares

Users currently own and utilize a complement of field spare boards and modules in support of the equipment sites. The vendor/contractor shall supplement the System field spares through an advanced replacement process to minimize equipment outages at System sites. System spares are maintained for the various locations as specified in Tables 8-1, 8-2, 8-3, and 8-4.

Table 8-1 Tudor Road Master Site System Spares

1	HP Procurve, Model J4900A
1	HP Procurve, Model J4813A
1	MOSCAD Power Supply
1	CEB Board
1	CEB Board – BIM
1	CEB Board – Timer
1	CEB Board – AMI
1	CEB Board
1	CEB Board
1	Type 1 Transector
1	S2500 10Base-T
1	S2500 T1/E1 CSU/DSU MOD
1	Logitech Access Keyboard
1	HP DL360 G3 Hardware Kit
1	Head Set Jacks for CIE
1	Clipper Twin Foot Switch for CIE
1	Motorola Transportable, Model F2804A
1	Motorola Router Model ST2500A – S2500
1	Motorola Router Model ST2500B – S2500
1	Motorola Router ST4000B, Model ESPL-370
1	Motorola Router ST5500B, Model ESPL-360
1	Motorola PSC 9600, Model T6782
1	Motorola PSC 9600, Model T6784A
1	Transector Surge Suppression, Model MPS 32 T1
1	T1/E1 Interface
1	T1/E1 Interface
1	MOSCAD Motorola NFM XC RTU

Table 8-2 Ted Stevens Anchorage International Airport BDA

1	BDA Crossband Coupler, Model 80-05-06
1	BDA Crossband Coupler, Model 80-05-07
1	BDA Power Supply Model 3-15503
1	BDA Preamp Model 3-11423
1	BDA Preamp Model 3-11792
1	BDA AC-DC Converter Model 3-5969
1	Wilmore AC-DC Converter Mdl 1654-48-120-60-U

Table 8-3 Whittier BDA

1	VHF Head End BDA 10/5W
1	LNA VHF 70-500MHz with Relay
1	Power Amp 10W 100-250MHz 1.5 MHz BW
1	24V 17A PSU 400W (XP)
1	¼ W O-30DB Switched Attenuator
1	Attn Switch Remote D Type 60DB
1	Control Monitor Board RS485 Protocol
1	VHF Inline BDA 10/5W
1	LNA VHF 70-500 MHz with Relay
1	Power Amp 10W 100-250MHz SMA Connection
1	24F 17A PSU 400W (XP BCC)
1	¼ W 0-30 Switched Attenuator
1	Attn Switched Remote D Type 30DB
1	Control Monitor Board RS485 Protocol

Table 8-4 Site Spares

1	265W AC Power Supply
1	600W DC Power Supply 24 VDC
1	600W DC Power Supply 48/60 VDC
1	VHF Range 2 Receiver
1	VHF 125W Power Amp
1	Internal UHSO
1	Procurve Switch
1	NFM XC RTU
1	CSU/DSU Daughter Board
1	WAN Router
1	VHF Range 2 Exciter
1	Epic III Control Module
1	33.6 Modem
1	48 VDC Power Supply
1	CDRW Drive
1	Distribution Panel
1	PBA Plug-In Breaker 30 Amp
1	PBA Plug in Breaker 50 Amp
1	Power Supply
1	Wilmore Inverter

NOTE: All spares are currently owned by/reserved for the Department of Defense.

9.0 Metric Reporting Procedures/Processes

The Operations Manager will report on System operations and issues. Issues requiring action shall be prioritized and addressed by the Operations Manager, as prioritized and directed by the User Council.

9.1 The Operations Manager

C9.1.1 The Operations Manager will provide to the User Council System performance reports that are based on past and current System data. Written status reports of ongoing projects or technical solutions shall be submitted to the User Council monthly, or as required.

9.1.2 The data will be presented graphically in order to make it easily understandable. The focus will be on both performance and fault management.

9.1.3 The Operations Manager will provide trend analysis of the report data to highlight trends and actions that the User Council should consider initiating for the System to improve availability, reliability and serviceability of the network. Reports can be configured to indicate certain pre-designated parameters as directed by the User Council to prevent unauthorized access to System information. The information should include, but be limited to:

9.1.3.1 Baseline metrics to measure the “healthy” operation of the System (this is predicated on monitoring of the System to obtain the appropriate data)

9.1.3.2 Equipment, site, site link or other failure trends

9.1.3.3 Early identification of System performance degradation

9.1.3.4 Service-level performance information

9.1.4 The Operations Manager will also utilize this information to make recommendations to the User Council for improving network operations and improving cost-effective, proactive approaches to System maintenance and support.

9.1.5 The Operations Manager will be available to attend applicable meetings with the User Council or other meetings relating to System operations and performance.

10.0 Preventive Maintenance Inspection

10.1 Original Equipment Manufacturer (OEM)

10.1.1. On an annual basis, an OEM certified technician shall perform operational tests and alignments on the System infrastructure network equipment to optimize and ensure the equipment meets OEM specifications.

10.1.2 The technician shall remove any oil, dust and/or foreign substances from the equipment, clean filters if applicable, and measure, record, align and adjust the following applicable equipment parameters to the frequency and modulation outlined in the rule and regulations of the FCC.

10.1.3 A preventative maintenance schedule will be coordinated with the site owner, DOD/SOA DOA, and approved on a yearly basis. Modifications to the schedule must also be coordinated and approved within 90 days of the scheduled preventative maintenance audit and inspection being performed.

10.1.4. The government (DOD/SOA DOA), at its pleasure, can provide a representative to audit/observe the preventative maintenance audit and inspection. Where special conveyance is required to get to the site to perform this activity, vendor/contractor shall provide the conveyance of DOD/SOA DOA on the same conveyance used by the vendor/contractor.

10.1.5. Preventive maintenance activities will be documented and available for review, as required.

11.0 System Security

11.1 Strategy

11.1.1 The security strategy for the System is predicated on protecting the radio network infrastructure. The ASTRO 25™ has built-in security countermeasures. However, security also involves physical site and connected networks security.

11.1.2 The fundamental security strategy for protecting a large network such as the System consists of the following:

11.1.2.1 Define radio network security policies

11.1.2.1.1 Define what needs to be protected

11.1.2.1.2 Set up policies for external network connectivity

11.1.2.1.3 Define policies for User access controls and anti-virus

11.1.2.1.4 Define policies for mobile data User access controls and anti-virus

11.1.2.2 Fully utilize built-in security countermeasures

11.1.2.2.1 Anti-virus, intrusion detection, firewalls, access controls and operating system hardening

11.1.2.3 Perform radio network security management

11.1.2.3.1 Monitor network barriers and anti-virus 24 hours/day, 7 days/week

11.1.2.3.2 Proactively maintain security devices up to date

11.1.2.3.3 Pre-test and deploy security updates (periodic and urgent)

11.1.2.3.4 Be ready with incident response plan and team 24 hours/day, 7 days/week

11.1.2.3.5 Proactively update configurations as new threats emerge

11.1.2.3.6 Enforce and maintain User access controls

11.1.2.3.7 Conduct and test system backup and recovery procedures

11.1.2.3.8 Conduct ongoing security assessments and User training

12.0 Site Book Management

Site Book management includes the management of the documentation within the books and the process of updating the books that are on the sites, in the operations offices and distributed to specific Users. The System Management and Operations Management Team will track and manage modifications to data records, as they are communicated. This includes providing information to each Site Book and operations team member, as needed.

13.0 Standard Operating Procedures/Processes

There will be operating procedures for obtaining helpdesk services, technical support, network monitoring services, infrastructure repair, advanced replacement services, system survey and analysis, software subscription releases, software upgrade design services, infrastructure software installation services, subscriber radio repair and reports.

14.0 User Management

Add/Change/Delete Form

POC: _____ Email: _____

Serial Number/ID numbers:
1._____ (A)(C)(D) Alias_____ ID_____
2._____ (A)(C)(D) Alias_____ ID_____
3._____ (A)(C)(D) Alias_____ ID_____
4._____ (A)(C)(D) Alias_____ ID_____

For convenience, we will accept information on an Excel spreadsheet if it is attached to this form, just add the comment “See Attached” on line 1 above.

Is this is required by a certain date/time? _____.

Emailed codeplug to System Manager: YES / NO (circle one)

Information:_____
_____
_____
_____
_____
_____

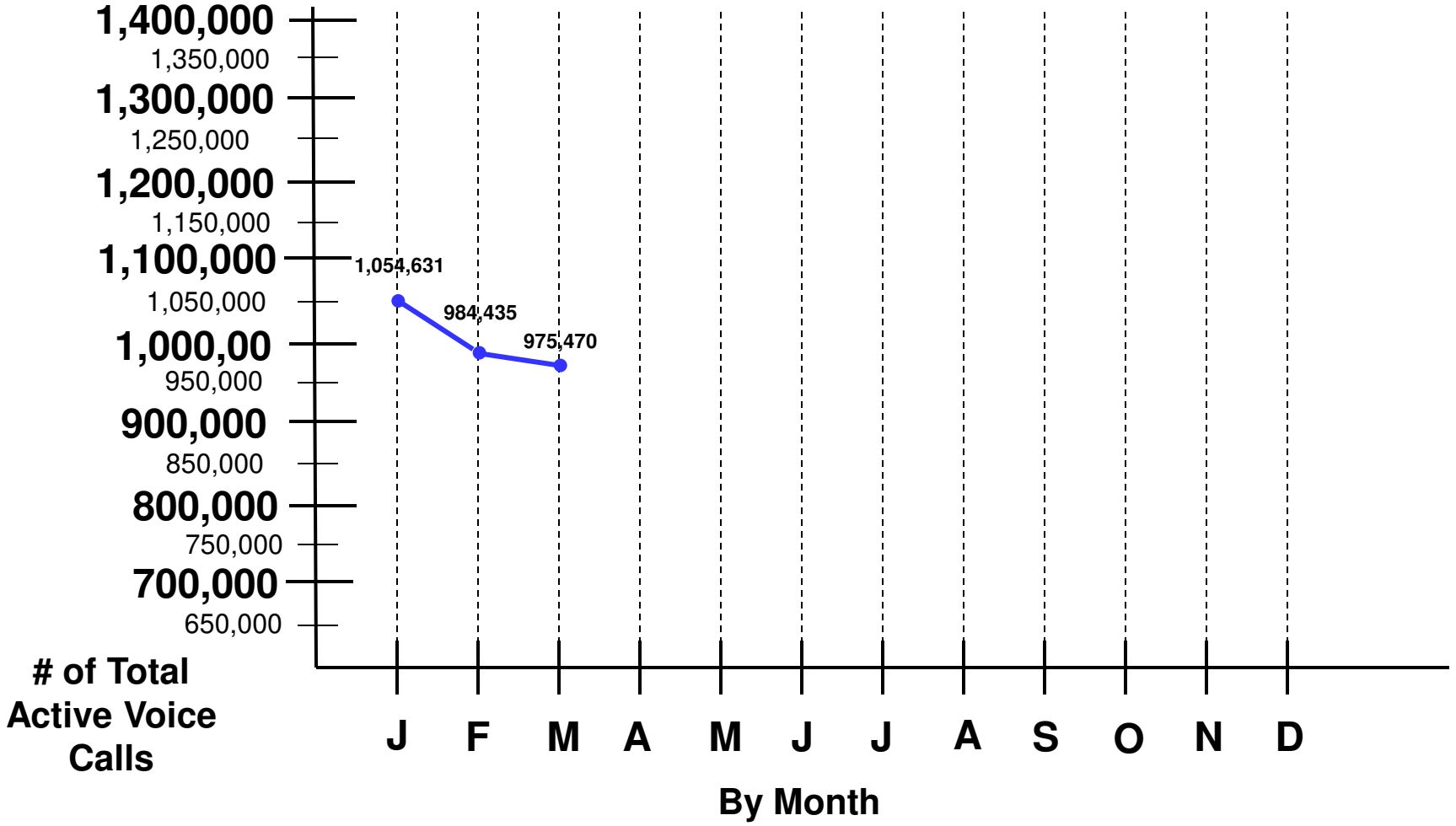
Programming Service Shop: _____.

Advance System Key number(s):_____.

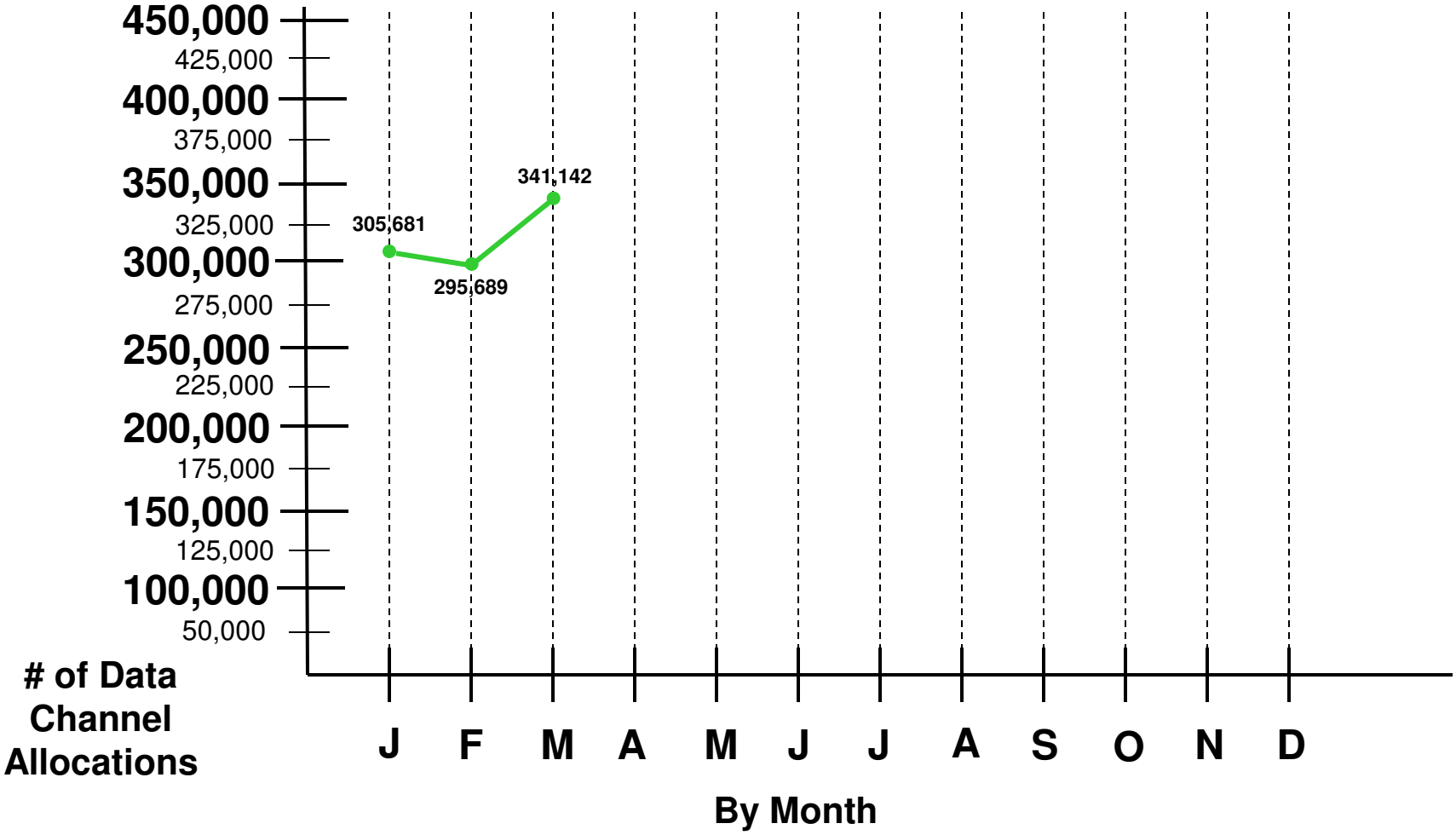
Date Shipped/Delivered: _____.

Software Version	Flash Code	System Technician	Date

2013 System Performance
Active Voice Calls



2013 System Performance
Data Channel Allocations



2013 System Performance
Busy Voice Calls