



Alaska Land Mobile Radio Communications System

System Backup and Recovery Procedure 400-5

Version 4

February 16, 2011

Developed in conjunction with:



Bering Straits Information Technology, LLC
A Subsidiary of the Bering Straits Native Corporation



Table of Contents

Table of Contents	1
Document Revision History	2
Acronyms and Definitions	3
1.0 Purpose	5
2.0 Roles and Responsibilities	5
2.1 Executive Council	5
2.2 User Council	5
2.3 Operations Management Office	5
2.4 System Management Office	5
2.5 Information Assurance Officer/Security Manager	6
3.0 System Baselines	6
4.0 Backup Requirements	7
4.1 Daily Backups	7
4.2 Weekly Backups	7
4.3 As-Needed Backups	7
5.0 Media Labeling	8
6.0 Backup Storage	8
6.1 Designated Storage Locations	8
7.0 Recovery Procedures	9
7.1 Recovery Documentation and Procedures	9
7.2 Secure Recovery	9
7.3 Prioritization of Recovery	9
7.4 Required Recovery Personnel	12
8.0 Backup and Recovery Procedure Testing	12
9.0 Training and Awareness	12
10.0 Compliance	12



Document Revision History

Name	Date	Reason for Changes	Version
Coates, Michael	12/22/2008	Approved by the User Council – Final.	2
Shafer, Sherry	3/1/2010	Annual review/update. Approved by the User Council – Final.	3
Shafer, Sherry	2/16/2011	Annual review/update. Approved by the User Council - final.	4

Acronyms and Definitions

Alaska Federal Executive Association (AFEA): federal government entities, agencies and organizations, other than the Department of Defense, that will operate on the shared ALMR system infrastructure.

Alaska Land Mobile Radio (ALMR) Communications System: the ALMR Communications System, which uses but is separate from the State of Alaska Telecommunications System (SATS), as established in the Cooperative Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents member local governments.

Cooperative Agreement: the instrument that establishes ALMR and sets out the terms and conditions by which the system will be governed, managed, operated and modified by the Parties signing the Agreement.

Department of Administration (DOA): a State of Alaska (SOA) department that maintains the SOA Telecommunication System (SATS) and provides information technology (IT) and communications technical support to state agencies.

Department of Defense – Alaska: Alaskan Command, US Air Force and US Army component services operating under United States Pacific Command.

DODI: Department of Defense Instruction

Executive Council: the ALMR Executive Council which is made up of three voting members and two associate members representing the original four constituency groups: the State of Alaska, the Department of Defense, Non-DOD Federal agencies (represented by the Alaska Federal Executive Association), and local municipal/government (represented by the Alaska Municipal League and the Municipality of Anchorage).

FV: FullVision® INM Database Server

Information Assurance (IA): information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IAO: Information Assurance Officer

Key Management Facility (KMF): allows for secure re-keying of radios over the air.



Alaska Land Mobile Radio Communications System System Backup and Recovery Procedure 400-5

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of approximately 278,000. The MOA stretches from Portage, at the southern border, to the Knik River at the northern border, and encompasses the communities of Girdwood, Indian, Anchorage, Eagle River, Chugiak/Birchwood, and the native village of Eklutna.

Operations Management Office (OMO): develops recommendations for policies, procedures, and guidelines; identifies technologies and standards; and coordinates intergovernmental resources to facilitate communications interoperability with emphasis on improving public safety and emergency response communications.

State of Alaska (SOA): the primary maintainer of the SATS (the State's microwave system), and shared owner of the System.

State of Alaska Telecommunications Systems (SATS): the State of Alaska statewide telecommunications system microwave network.

System Management Office (SMO): the team of specialists responsible for management of maintenance and operations of the System.

SSS: System Statistics Server

User/Member: an agency, person, group, organization or other entity which has an existing written Membership Agreement to operate on ALMR with one of the Parties to the Cooperative Agreement. The terms user and member are synonymous and interchangeable.

User Council: the User Council is responsible for recommending all operational and maintenance decisions affecting the System. Under the direction and supervision of the Executive Council, the User Council has the responsibility for management oversight and operations of the System. The User Council oversees the development of System operations plans, procedures and policies under the direction and guidance of the Executive Council.

UCS: User Configuration Server

ZDS: Zone Database Server

ZSS: Zone Statistics Server

1.0 Purpose

This procedure defines required actions to be taken by System Management Office (SMO) and Operations Management Office (OMO) personnel while performing System backup and recovery operations.

This procedure meets or surpasses the minimum accepted level of backup and recovery for ALMR systems in the form of technical, operational, and managerial control as required under DODI 8500.2, Information Assurance (IA) Implementation and NIST SP800-53, Recommended Security Controls for Federal Information Systems.

2.0 Roles and Responsibilities

2.1 Executive Council

The Executive Council (EC) shall be responsible for the management and imposition/enforcement of sanctions when violations of the System Backup and Recovery Procedure warrant action.

2.2 User Council

The User Council (UC) shall be responsible for the formal approval of the System Backup and Recovery Procedure, and any revisions hereafter.

2.3 Operations Management Office

The Operations Management Office (OMO) is responsible for:

- Briefing the UC and the EC of violations pertaining to System Backup and Recovery when notified by the Information Assurance Officer/Security Manager
- Verifying backups (daily, weekly, and as needed) are being completed, as required
- Verifying the operating system media and other critical software is stored, as required
- Verifying a master list of ALMR hardware and software components exists and is stored, as required
- Ensuring backup and recovery procedures are tested annually, as required, and briefing the UC and EC of the results

2.4 System Management Office

The System Management Office (SMO) shall coordinate and oversee all backup and recovery operations. This includes, but is not limited to, overseeing:

- Maintenance and backup of an ALMR hardware asset baseline

- Access control and storage of all ALMR backup media
- Scheduling and performance of critical System backups
- Coordination of recovery efforts during a System disaster or incident
- Training of all personnel responsible for backup and recovery procedures

2.5 Information Assurance Officer/Security Manager

The Information Assurance Officer (IAO)/Security Manager shall be responsible for:

- Developing, disseminating, and periodically reviewing/updating formal documented procedures that address purpose, scope, roles and responsibilities, and compliance with System backup and recovery
- Facilitating the implementation of the backup and recovery procedures, if/when required
- Managing reported issues identified under the scope of the System Backup and Recovery Procedure
- Reporting violations to the OMO
- Documenting any actions to be taken in the form of a sanction and forwarding, through the OMO, to the EC for approval

3.0 System Baselines

The SMO will maintain a compiled list of all ALMR hardware and software components. A backup copy of this inventory shall be stored in a fire-rated container and not located on site with the original.

The baseline will include the following items regarding each piece of hardware:

- Manufacturer
- Type
- Model
- Physical location
- Network topology / architecture

The baseline will include the following items regarding each piece of software:

- Manufacturer
- Type
- Version
- Software license number(s)
- User manuals
- Procedures

The SMO will be responsible for ensuring that new/upgraded hardware or software added to the ALMR System is documented within the baseline.

4.0 Backup Requirements

Backup operations will be implemented in a way as to minimize impact on the network and system resources.

4.1 Daily Backups

Each day a full data backup shall be performed for each of the ALMR essential database systems.

4.1.1 The following daily automatic server database backups shall be utilized for each Zone:

- System Statistics Server (SSS)
- Zone Database Server (ZDS)
- Zone Statistics Server (ZSS)
- FullVision® INM Database Server (FV)

4.1.2 The backup schedule for each of these servers can be managed from the remote management terminal of the User Configuration Server (UCS) and ZSS.

4.1.3 Access to the UCS and ZSS should be obtained by initiating a telnet session to the Terminal Server at the same site that you are scheduling backups for.

4.1.4 Additionally, the database which contains the ALMR hardware baseline shall be backed up daily to ensure database changes can be restored or reversed, as needed.

4.2 Weekly Backups

4.2.1 A backup of all dispatch console configuration files shall be performed weekly.

4.2.2 A backup of all ALMR controlled Key Management Facility (KMF) server databases shall be performed at least weekly.

4.3 As-Needed Backups

All network device configurations shall be backed up before and after system changes. This includes, but is not limited to, domain controllers, router, firewall, and switch configurations.

4.3.1 System Change/Upgrade Backup

A System backup, to include System status data, will be created before any major System changes are enacted or before any System upgrades are performed. The backup will be retained in the designated offsite location for at least five working days



after the changes. After changes have been completed, and a successful reboot has been accomplished, the regular backup schedule shall be resumed.

4.3.2 Weekend and Holiday Procedures

Writable backup media shall be left in all automatic backup devices during holidays and weekends to ensure automatic backups continue to complete successfully. The writable media used during holidays and weekends shall be moved to the designated off-site location on the next business day.

5.0 Media Labeling

All backup media should be clearly labeled to ensure the content can be quickly recognized.

6.0 Backup Storage

Back-up copies, or the original media of the operating system and other critical software, shall be stored in a fire-rated container and not located on site with the operational software.

This material will be stored within a secure area that is restricted to authorized individuals only.

Additionally, all backup media created from daily/weekly backup procedures will be stored in an off-site location.

6.1 Designated Storage Locations

The following designated storage location(s) are approved for all System backup media.

ALMR System Location	Backup Media Storage Location
Zone 1 Master Site 5900 E Tudor Rd Anchorage, AK 99507	5700 E Tudor Road Anchorage, AK 99507
Zone 2 Master Site Building 1192 Birch Hill, Fort Wainwright	911 Cushman Street. Fairbanks, AK 99701
TrackIt® Server 4600 DeBarr Ave Anchorage, Alaska 99508	5700 E Tudor Road Anchorage, AK 99507

Table 6-1. Designated Storage Locations



7.0 Recovery Procedures

7.1 Recovery Documentation and Procedures

All backup and recovery operations shall follow the documented procedure which is specific to the backup software use, and tailored to the data which is being backed up.

7.2 Secure Recovery

7.2.1 Hardware and software which is used by ALMR personnel for backup and recovery of the ALMR System shall be protected from unauthorized access or modification with the same diligence that is applied to the ALMR System itself.

7.2.2 If appropriately cleared personnel, as defined by the Security Manager, are unavailable to perform maintenance or repair, personnel with a lesser clearance may be used but only under escort and monitored/escorted by approved ALMR personnel, as defined by the Security Manager.

7.2.3 If at any point during the resumption of systems a situation is encountered which could inhibit a trusted recovery, ALMR personnel will cease resumption activities, document the situation, and consult with the Security Manager. It is the responsibility of the Security Manager to determine the appropriate mitigating procedures necessary to enable a trusted recovery of the System. The Security Manager shall maintain the documented information of the incident.

7.3 Prioritization of Recovery

In the event that recovery is required on multiple systems, priority groups have been established to guide the recovery of the systems. Systems in Priority Group 1 should be recovered first, then Priority Group 2 next, and continuing until all systems are restored.

Priority for Restoration - Zone Level		
Priority Group	Device	Purpose
Group 1	UCS	Voice Critical Hosts
	Gateway Router	
	Core LAN Switch (HP 5308)	
	Core LAN Switch (Cisco)	
	Core Router	
	Nortel Switch	
	Zone Controller	
	Zone Database Server	
	Exit Router	
	MGEG	
ADM/CDM		

	AEB	
	CEB	
Group 2	PN Router	CEN Connectivity
	Intrusion Detection Appliance	
	Firewall	
	Border Router(s)	
	Backup Gateway Router	
Group 3	GGSN	Data Sub-System
	PDR (PDG)	
	RNG (PDG)	
	Data Collection Device	
Group 4	T-Server	Telephony
	PBX	
	CLAN	
	VAL	
	Echo Cancellor	
	Interconnect Server	
	Data Collection Device	
Group 5	Analog Remote Access	Zone NM
	Digital Remote Access	
	Zone Statistics Server (ZSS)	
	Air Traffic Router (ATR)	
	ZMDS	
	MOSCAD Server	
	MOSCAD IP Gateways	
	MOSCAD Clients	
	MOSCAD RTUs	
	Data Collection Device	
	NM Client	
	FullVision [®] /RM	
	Infovista (Multizone Only)	
	SSS (Multizone Only)	
	Serviceability Server	
	Serviceability Server	
	Core Security Management Server (CSMS)	
	ArcSight Client-Server	
	Nortel Network Management Station	
	Cisco Network Management Station	
Traffic Analyzer Tool		
Genesis ATIA		
NTMS		

Table 7-1. Zone Restoration Priority Groups



*Alaska Land Mobile Radio Communications System
System Backup and Recovery Procedure 400-5*

Priority for Restoration – Site Level		
Priority Group	Device	System Sub-location
Group 1	Site Router	ISR site
	Site Lan Switch	ISR site
	Site Controller	ISR site
	Base Radio	ISR site
	Subscriber	ISR site
	Site Router	Dispatch site
	Site Lan Switch	Dispatch site
	Gold Elite Console Op	Dispatch site
	NM Clients	Dispatch site
	Channel Bank	Dispatch site
	Prime Site Router	Simulcast Prime site
	Site Lan Switch	Simulcast Prime site
	Site Controller	Simulcast Prime site
	ATAC(comparator)	Simulcast Prime site
	TRAK(gps)	Simulcast Prime site
	Base Radio	Simulcast Prime site
	Channel Bank	Simulcast Prime site
	NTP Server	Simulcast Prime site
	Comparator	Simulcast Prime site
	Remote Site Router	Simulcast Remote site
	Site Lan Switch	Simulcast Remote site
	Channel Bank	Simulcast Remote site
	Base Radio	Simulcast Remote site
	NTP Server	Simulcast Remote site
Group 2	NM Client (CEN Location)	Remote NM site
	CEN NM Client Router	Remote NM site
	CEN NM Client Switch	Remote NM site
	MOSCAD RTUs	ISR site
	MOSCAD Clients	ISR site
	Data Collection Device	ISR site
	DHCP Hosts for CSS	ISR site
	Subscriber	Dispatch site
	Backup Site Router	Dispatch site
	Border Router	Dispatch site
	Data Collection Device (Customer Host)	Dispatch site
	DHCP Hosts for CSS	Simulcast Prime site
	Subscriber	Simulcast Prime site
	Simulcast Prime Terminal Server	Simulcast Prime site
	Dial-up Client for Simulcast Prime Terminal Server	Simulcast Prime site

	MSC9600	Simulcast Prime site
	MOSCAD RTUs	Simulcast Prime site
	MOSCAD Clients	Simulcast Prime site
	DHCP Hosts for CSS	Simulcast Prime site
	Data Collection Device	Simulcast Remote site
	Subscriber	Simulcast Remote site
	MOSCAD RTUs	Simulcast Remote site
	Data Collection Device	Simulcast Remote site
	DHCP Hosts for CSS	Simulcast Remote site

Table 7-2. Site Level Restoration Priority Groups

7.4 Required Recovery Personnel

The SMO will be available to respond 24/7 immediately upon failure notification and shall coordinate emergency maintenance support for key information technology assets.

8.0 Backup and Recovery Procedure Testing

The Backup and Recovery Procedure for the ALMR System shall be tested annually by the SMO, and all results of the test shall be recorded and provided to the Operations Manager.

9.0 Training and Awareness

All personnel responsible for recovery of the ALMR System shall receive appropriate training specific to their roles in the backup and recovery process.

10.0 Compliance

Compliance with the System Backup and Recovery Procedure is outlined in ALMR System Backup and Recovery Policy Memorandum 400-5.