Occupant Evacuation & COOP Plan

US Forest Service
Rocky Mountain Interagency Cache
Bldg 810/Door N27
Denver Federal Building
Lakewood, CO

This Plan establishes evacuation and emergency procedures for Bldg 810 of the Denver Federal Building, in accordance with Occupational Safety and Health Standard 1910.38(a). This Plan will be kept in the RMK Cache office area and also posted in the warehouse section.

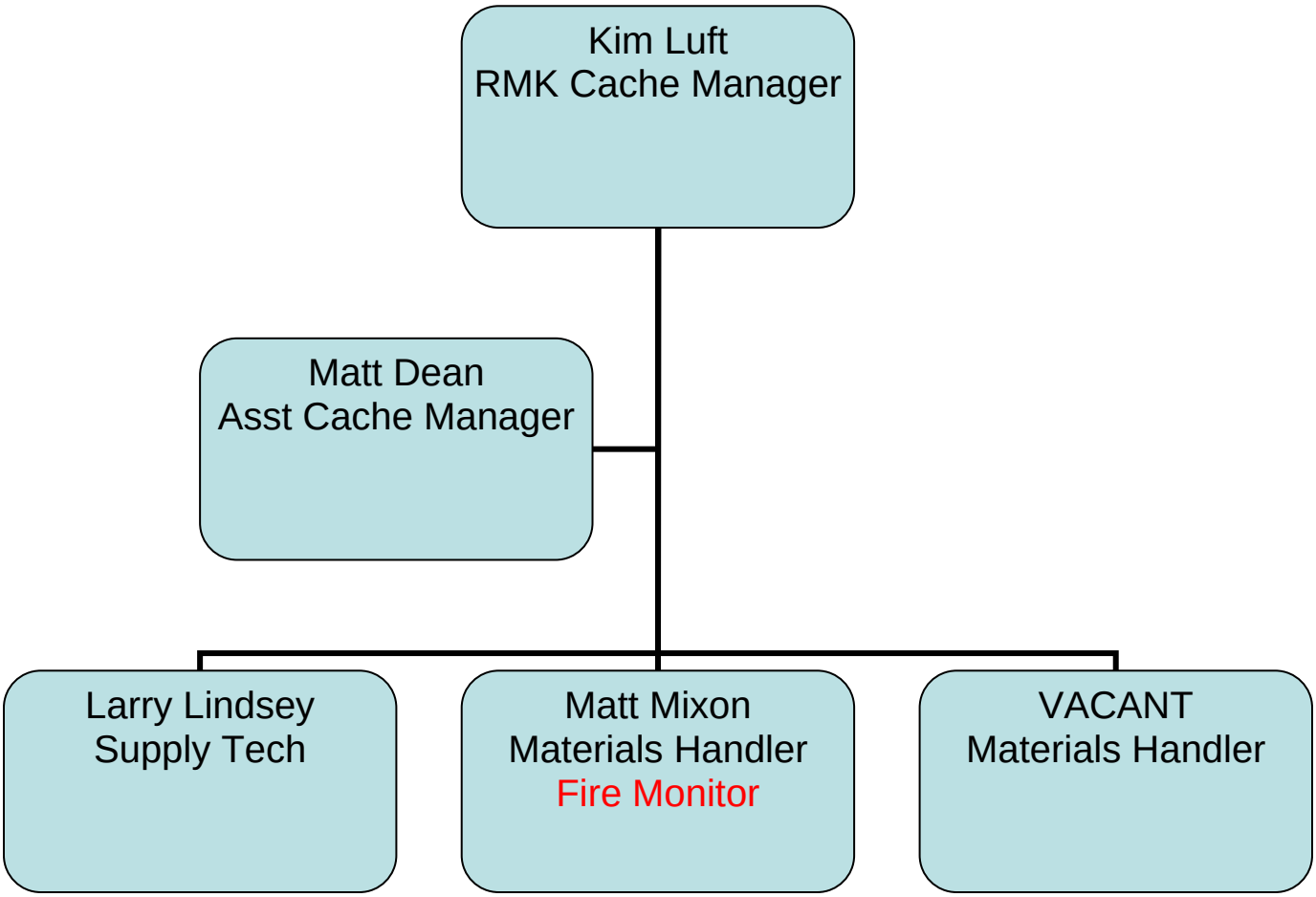
A. AUTHORITY

1. 29 CFR 1910.38, and 29 CFR 1910.38 (E)
2. Disaster Control and Civil Defense in Federal Buildings @(PBS publication 24601a)
3. Federal Property Management Regulations
4. USDA Department Manual

B. PROVISIONS OF THE PLAN

1. Direct access to emergency services through the use of 9-911 will be available to USDA employees at all times.
2. If an emergency occurs inside or outside the building, total building evacuation will be determined by the Cache Manager or acting. When the alarm sounds, occupants **MUST** evacuate to their assigned safe zones outside.
3. Alarm boxes and fire extinguishers are located on each floor and are identified on each floor map.
4. In an emergency evacuation, all occupants MUST evacuate immediately to their outside safe zone. Maps showing alarm locations and staging areas are located throughout the building in the areas.

Table of Contents


Kim Luft
RMK Cache Manager
Matt Dean
Asst Cache Manager
Larry Lindsey
Supply Tech
Matt Mixon
Materials Handler
Fire Monitor
VACANT
Materials Handler

Phone Roster of Cache Organization

POSITION	NAME	TELEPHONE NO.
Cache Manager	Kim Luft	202-4965
Asst Cache Manager	Matt Dean	202-4941
Supply Tech	Larry Lindsey	202-4945
Materials Handler	Matt Mixon	202-4945
Materials Handler	VACANT	VACANT

EMPLOYEE RESPONSIBILITY

In the event of an emergency, employees should:

1. Notify supervisor/manager.
2. Evacuate immediately if you are directed to do so follow instructions of Organizational Officials.
   a. Do not turn around and go back.
   b. Travel in single file. Stay to the right when moving down the stairs.
   c. Assist your co-workers and visitors if they need help.
3. Gather at your staff's pre-determined Safe Zone (maps posted throughout the building). Check in with your supervisor or acting. REMAIN in your work group at the SAFE ZONE until told by Organization Officials to re-enter the building or to leave the premises.
4. **DO NOT attempt to fight fire or confront demonstrators.**

EMERGENCY TELEPHONE NUMBERS

US Forest Service Law Enforcement & Investigation	303-275-5268
Jefferson County Emergency Calls	9-911
Lakewood Fire Department	303-969-0245
Lakewood Police Department	303-987-7111
Federal Protective Service	303-236-2911
FBI Field Office	303-629-7171
Poison Control Center	303-629-1123
Building Owner/Manager Ron Lofton	720-560-5881
Emergency Operations Center	303-236-2911
Fire/Police NON EMERGENCY After Hours/Holidays	303-236-6709
Occupant Emergency Coordinator Ben Kelley	303-356-8834

DUTIES AND RESPONSIBILITIES

1. **Cache Manager's Duties**: The Manager is responsible for implementing and developing the Occupant Emergency Plan. The goal is to protect life and property and to minimize damage.

   Duties include:

   a. Insures that the basic provisions of the Plan are disseminated to all building employees.
   b. Directs the activities of the Organization in an emergency.
   c. Maintains liaison and directs the principal officers or their designees on problems arising in the selection and training of employees for the Organization.
   d. Maintains liaison with the local fire department, police department and Building Manager.
   e. Arranges for posting on appropriate bulletin boards a roster of Organization personnel who have responsibilities for emergency operations.

f. Takes necessary actions to ensure that the facility's Organization operates safely and efficiently in emergencies. Coordinates with the Building Manager to select, organize and train an emergency response team.

2. **Asst Cache Manager**: Serves as the principal assistant to the Manager and acts during Manager's absence. Insures the Plan is current and Organization personnel know their responsibilities for emergency operations.

3. **Fire Monitor (Lead Material Handler)**: The Fire Monitor duties are:

a. Know the location of fire extinguishers in their area of responsibility.

b. Know how to operate extinguishers.

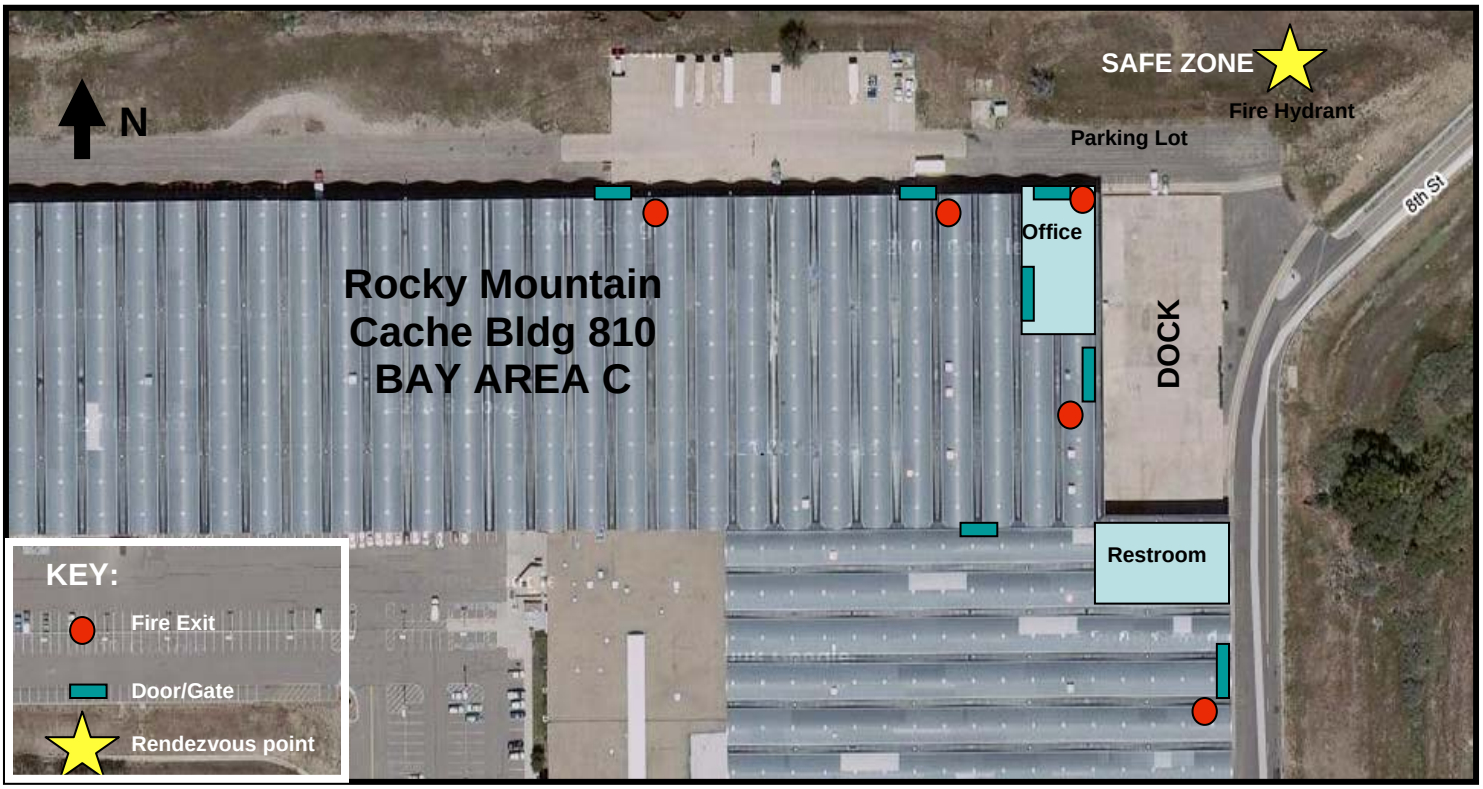
c. Assisting the Manager in any duties the Manager may assign.

EMERGENCY AND EVACUATION PROCEDURES

Emergency Procedures

Upon notification;

1. Officials will inform the building occupants of the emergency.
2. Organization will immediately assume their designated duties.
3. Employees must follow directions and cooperate.
4. Walk to SAFE ZONE and await further instructions.



Evacuation Procedures

Evacuation will occur when the FIRE ALARM SOUNDS.

In other situations, the Manager will decide on what evacuation orders will be given.

Occupants take the following action:

1. Walk to nearest fire exit.
2. Obey the instructions of managers/officials.
3. Walk to the SAFE ZONE and wait for instructions from organization official.
4. **UNLESS SUCH ACTION WOULD ENDANGER LIFE**, put classified or sensitive documents in safe or secure location; place exposed records in cabinets or desk drawers or spread covers to protect them, disconnect electrical equipment and take your purse and coat. The last person to leave the room closes but DOES NOT LOCK the door.

Supervisors in each staff will assign an assistant to hearing impaired people. Assistants will notify the person of the alarm and ensure that they evacuate the building.

The cache manager or assistant manager will do a head count to insure all occupants have evacuated. This is reported to organization officials.

1. Persons with disabilities and their assistants will REMAIN at the SAFE ZONE.
2. RESCUE will be initiated by the Fire department. Occupants are not to return to the building to help someone get out.

FIRE IN BUILDING

Upon discovering a fire, activate fire alarm and, if possible, notify a manager giving the location of the fire.

The manager telephones/notifies Forest Service assigned Safety Coordinator giving location of fire and proceeds with evacuation plan.

Occupants must follow the **evacuation** procedures previously enumerated.

Fire Monitor will access the situation and determine the need to extinguish a fire and/or evacuate the effected area.

Fire Monitors can leave the building after known occupants have evacuated.

ENEMY ATTACK

The Lakewood Fire Department and the Denver Federal Center operate Civil Defense sirens that are sounded to warn of an enemy attack.

ALERT SIGNAL: This is a steady tone for three to five minutes signaling that essential emergency information will be broadcast. Any employee with a radio in their possession should turn it on and report emergency broadcasts directly to their manager, who will relay to the Coordinator.

If evacuation is necessary, occupants evacuate according to directions of the manager.

Occupants should take their coats and purses when leaving the work area.

ATTACK WARNING SIGNAL: This is a wavering tone or a series of short blasts for three to five minutes. It signifies that an actual attack has been detected. Occupants perform the following actions:

1. Take cover under desks, tables, or large objects that will give protection against flying glass and debris.
2. Stay against the wall and away from the windows.
3. Leave cover when notified by the Organization Officials or manager.

EXPLOSION

In the event of an explosion that affects the building, take the following actions:

1. If possible, notify the Fire Department by activating the nearest building alarm box, or calling Fire Department.
2. Take cover under tables, desks or other objects that will give protection against flying glass or debris.
3. Call or have nearby person contact a manager to give location of explosion. Manager telephones the Building Manager and explains the situation.
4. After effects of explosion have subsided, Coordinator will decide whether to evacuate the building.
5. If an evacuation is necessary, occupants evacuate to their SAFE ZONE and wait for instructions from Organization officials.

EARTHQUAKE

Upon experiencing an earthquake, occupants should take the following actions:

INDOOR PROCEDURE:

1. DUCK, COVER, and HOLD. Take COVER under a sturdy desk or table that will offer protection against flying glass or debris. DUCK into a corner, against an interior wall, under a doorway or into a narrow hall or corridor. Protect your head and neck with your arms. If possible, HOLD onto something sturdy. Keep away from windows to avoid flying glass.
2. WAIT until the ground stops shaking and it is safe to move. Be prepared for after shocks.
3. Do not use the telephone unless the situation is critical.
4. Stay in your immediate area. You will be notified when to evacuate the building.

Building Manager will notify the Fire Department of any fires.

Immediately after an earthquake, Organization Officials take the following actions:

1. Search area and report to manager regarding damage to the building and status of employees.
2. Prepare the area for evacuation. Gather employees in one safe zone (i.e., an open area, one with less damage, an enclosed office, etc.).
3. If possible, extinguish small fires.
4. Reserve telephones for emergency calls.

5. Direct occupants away from hazards such as broken glass, spilled fluids, damaged equipment, loose plaster, crumbling ceilings, etc.
6. If required, request assistance from outside sources (Disaster Corps).
7. Turn on radio for information about the extent of community damage.

OUTDOOR PROCEDURE:

Get away from buildings, trees, walls, and power lines.

When the ground stops shaking: (Expect after shocks.)

1. Check for injuries in your immediate area. Initiate first aid if necessary. Move injured people to a safe zone if possible (i.e., an area with less damage or an open area).
2. Stay clear of fallen debris, broken glass and electrical wires.

CHEMICAL ACCIDENT

A chemical accident could endanger the occupants of the building. Building occupants should perform the following actions:

1. Occupant notifies Manager of danger.
2. Manager telephones Building Manager and explains the situation.
3. Manager decides jointly with the Building Manager whether to evacuate the building.
4. If an evacuation is necessary, occupants evacuate under direction of the Manager.
5. Manager or Building Manager telephones the Fire Department and explains the situation.

Occupants avoid fumes by moving crosswind; they should never move upwind or downwind.

TORNADOES

Upon sighting a funnel cloud, occupants shall immediately notify manager or Building Manager and then take the following actions:

1. Move into interior warehouse Bay Area C.
2. Do not leave cover until advised to do so.
3. Do not go outdoors except on advice of Organization officials.
4. Once outside the building, proceed to a safe area away from falling debris or electrical wires.
5. Be alert to additional funnel clouds.
6. Normal activities should not be resumed until an “all Clear” has been issued by the National Weather Service

Manager will notify the Fire Department of any fires.

Immediately after a tornado, **Organization personnel** perform the following actions:

1. Turn off all lights and appliances.
2. Report any obvious damage to utility lines to the Building Manager.
3. If possible, extinguish small fires.
4. Reserve telephones for emergency calls.
5. Look for other hazards such as broken glass, spilled fluids, damaged equipment, loose plaster, crumbling ceilings, etc. and take appropriate action.
6. If required, request assistance from outside sources (Disaster Corps.).
7. Turn on radio for information about the extent of community damage.
8. Make every effort to carry out routine procedures and return building to normal operations.

DEMONSTRATIONS

If there a demonstrators in or around the Denver Federal Center:

1. Notify the Building Manager
2. Report to your supervisor
3. DO NOT interact with demonstrators.
4. Stay inside the building unless otherwise directed.

If a LOCK DOWN becomes necessary. FOLLOW DIRECTIONS. Communication will be via phone or by intercom.

BOMB THREAT

When a bomb threat is received, either orally or in writing,

1. Attempt to fill out the attached "BOMB THREAT CHECKLIST",
2. Immediately call (303) 236-2911 Federal Protective Service Control Center
3. Notify the Coordinator or Floor Monitor.

The manager will coordinate emergency procedures.

HAZARDOUS WEATHER

The Coordinator will follow the Denver Federal Executive Board's uniform method for dismissing employees during adverse weather conditions.

YELLOW OR RED ALERT

GSA will notify Organization officials in the event of a *Yellow* or *Red Alert*.

Yellow Alert condition is a situation that has developed to the point where additional preparedness measures are required.

Red Alert condition requires immediate measures to protect against an ongoing situation.

The Emergency Operations Center is at the Denver Federal Center, telephone number 303-236-2911.

The Emergency Operations Center will provide agency officials with current information for evaluation and coordination of emergency action decisions.

BOMB THREAT CHECKLIST

Exact time of call: _____

Exact words of caller: _____
_____
_____

Questions to ask:

1. When is bomb going to explode? _____
2. Where is the bomb? _____
3. What does it look like? _____
4. What kind of bomb is it? _____
5. What will cause it to explode? _____
6. Did you place the bomb? _____
7. Why? _____
8. What is your address? _____
9. What is your name? _____

CALLER'S VOICE (circle):

Calm	Disguised	Nasal	Angry	Broken
Stutter	Slow	Sincere	Lisp	Rapid
Giggling	Deep	Crying	Squeaky	Excited
Stressed	Accent	Loud	Slurred	Normal

If voice is familiar, whom did it sound like? _____

BACKGROUND SOUNDS (circle):

Animals	clear	voices	music	House noises
motor	Office machinery	PA system	static	voices

Other _____

Threat Language (circle):

Well-spoken	foul	irrational	incoherent	taped	Message read

Person receiving call: _____

Date: _____

Report call immediately to: 9-911, then Building Manager.

CONTINUITY OF OPERATIONS AND DISASTER RECOVERY (COOP):

LEVELS OF COOP IMPLEMENTATION

The four COOP levels are determined by the extent of the geographic area affected.

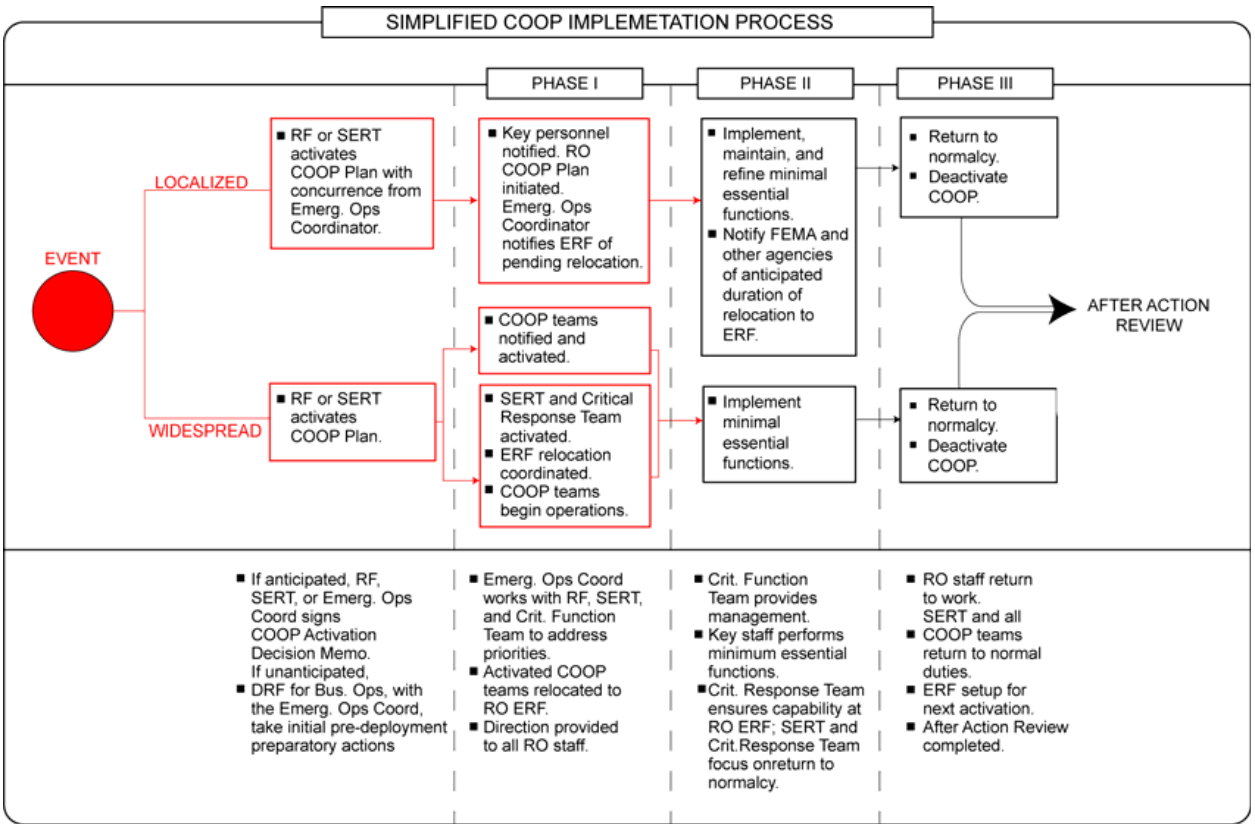
COOP Level 1: Affects part of a building that houses Forest Service Fire Cache essential functions:
A building, which houses essential functions, is operational, but normal business operations are suspended in a room, floor, level, or section due to fire, explosion, water damage, or other localized incidents. During this type of scenario, personnel who inhabit affected parts of the building relocate into the office area or other available space in the cache. The Regional Forester may grant administrative leave for the duration of the emergency. The Cache Manager will notify personnel if this is the case.

COOP Level 2: Affects the building that houses Forest Service essential functions:
A building is closed for normal business activities, but the cause of the disruption has not affected surrounding buildings, utilities, or transportation systems. The likely cause of business disruption is structural fire; system/mechanical failure; loss of utilities to include water or steam; or an explosion that causes no significant damage to surrounding buildings or utility systems. For this scenario, a local COOP incident requires inhabitants who perform essential functions from the affected building to relocate to the Regional Office (RO), Floor 3 training room or available space. The Regional Forester may grant non-essential employees administrative leave or request them to work from home. The Cache Manager will notify personnel if this is the case.

COOP Level 3: Affects the building that houses Forest Service essential functions and the surrounding area:
A building and the surrounding buildings and area are closed to normal business activities as a result of widespread utility failure; massive explosion (whether or not originating in the building that houses essential functions); severe earthquake; civil disturbance; or credible threats or actions that would preclude access or use of the building and surrounding area. Under this level of emergency there is uncertainty regarding whether additional events such as secondary explosions, aftershocks, or cascading utility failures could occur. Since COOP Level 3 emergencies can quickly escalate, they are handled identically to a COOP Level 4 emergency. If the Forest Service Regional Office (RO) is unaffected, cache personnel will relocate there on the 3rd floor, in either the training room or available space. Once accountability is reported, the Regional Forester grants non-essential personnel administrative leave until further notice. The Cache Manager will report personnel status and notify personnel of leave.

COOP Level 4: Affects the Denver/Lakewood area:
The area closes to normal business activities as a result of actual or threatened terrorist attack using weapons of mass destruction such as chemical, biological, radiological, or nuclear agents. Under this level of emergency, the President may declare a national security emergency, and implement many or all Federal department, Agency, and COOP Plans. Implementation for COOP Level 4 emergencies encompasses all buildings and facilities housing essential functions within the Denver Area. This scenario involves full activation of the COOP Plan with essential personnel relocating to the alternate ERF (see RMG COOP Plan).

IMPLEMENTATION PROCESS



Known threats and emergencies include natural, technological, and human induced events. Known threats and emergencies afford advance warning that can permit the orderly alert, notification, evacuation, and if necessary, relocation of employees. Examples of known threats include:

• Hurricane
• Transportation accident resulting in a threat of a release of hazardous materials (HAZMAT)
• Threat of a terrorist incident.

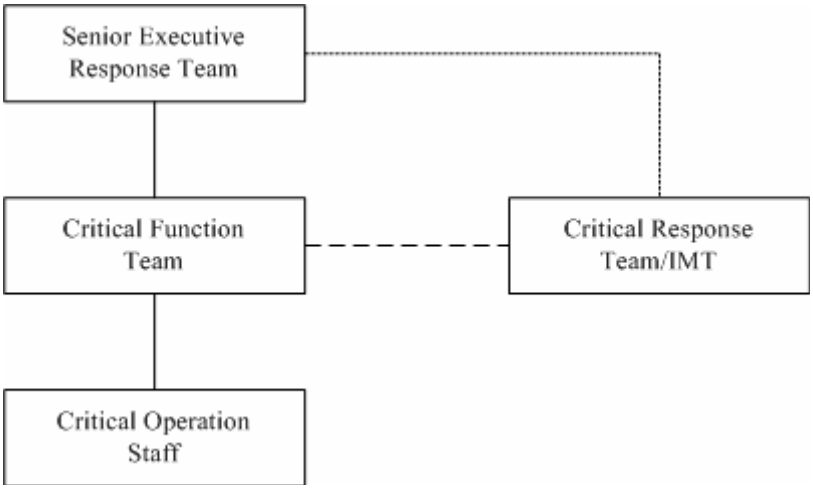
During known threat and emergency conditions, the Regional Forester or his Designee will make the decision to implement the COOP Plan and order the deployment of the Senior Executive Response Team and the Critical Response Team. This decision considers information from FS Law Enforcement and Investigation, the Emergency Operations Manager, and other sources that become aware of the actual or potential crisis. At this time, the Regional Forester also determines the direction for Regional Office and Cache employees not involved in COOP activities. This may include activating the COOP Plan while maintaining normal Agency operations.

Unanticipated Implementation

Many natural, technological, or human-induced events can occur without warning and require COOP activation. Unanticipated threats and emergencies can include earthquakes, tornadoes, or terrorist incidents. Under certain conditions during an unanticipated threat or emergency

affecting Regional Office, the cache, DRF for Business Operations, in coordination with the Emergency Operations Manager, may commence actions for survival and take initial pre-deployment preparatory actions. However, only the Regional Forester or Designee can implement the COOP Plan.
If the threat or emergency occurs during business hours, it will most likely begin with the execution of the site's Occupant Emergency Plan (OEP), which outlines how to quickly evacuate employees from the building. During these first hours, implementing the COOP Plan is second priority, until the Regional Forester or SERT assesses the incident and brings it under control.
To ensure proper record-keeping for an unanticipated implementation, the Emergency Operations Manager or Critical Response Team Incident Commander completes a Decision Memorandum for appropriate signature as soon as possible. The Decision Memorandum documents the proper COOP procedures to follow by the Emergency Operations Manager.

Figure shows the overall COOP organizational structure.



Implementation Process

Implementation of the COOP Plan is determined by whether the event is widespread or localized and on the impact of the event on a department, business unit, or facility operation. The COOP Plan implementation procedures operate around a time-phase approach that ensures efficient use of resources.
There are three phases to implementation activities that apply to both localized and to widespread emergencies:
• Phase I—Activation and Relocation (0–12 Hours)
• Phase II—Emergency Relocation Facility (12 Hours–Termination)
• Phase III—Reconstitution/Regeneration (Termination and Return to Normal Operations).

Implementation Activities for Localized Events

A localized event impacts smaller or isolated areas of a facility, such as a department, business unit, office, or sub-element. The Regional Forester or Designee is responsible for carrying out the implementation of the COOP Plan during a localized event. Implementation of the COOP Plan will more than likely be limited to the office directly affected, and the Cache Manager will notify cache personnel on reporting and relocating activities.

Implementation Activities for Widespread Events

A widespread event impacts a significant number of employees or could force the relocation of a significant number of employees. It is an Agency-wide, city/region-wide, or national security disruption. During a widespread event, the Cache Manager evaluates the emergency situation and reports to higher a SITREP.

Listing of functions of the Regional Office during COOP activation:

Law Enforcement and Investigations (LEI)
• Protect the public, employees, natural resources and other property under the jurisdiction of the Forest Service
• Investigate and enforce applicable laws and regulations
• Prevent criminal violations through informing and educating visitors and users
• Coordinate with local, State and Federal law enforcement agencies.

State and Private Forestry (SPF)
• Coordinate interagency fire emergency preparedness and response
• Coordinate National Response Plan disaster/emergency operations
• Coordinate disaster/emergency response operations with State and local cooperators.

Human Resources (HR) • Assist with Critical Incident Management
• Process Death Benefits
• Process Employee Payroll.

Chief Financial Office (CFO)
• Audit Appeals and Financial Ability Determination
• Provide safe keeping of cash/check and other financial instruments
• Process essential payments.

Acquisition Management (AQM)
• Monitor and maintain contracting operations
• Monitor and maintain leasing operations
• Monitor and maintain agreements.

Engineering (ENG)
• Perform EPA Coordination of hazardous materials
• Provide technical expertise and response to Forest Bridge work
• Provide technical expertise and response to explosives
• Provide technical expertise and response to earthquake damage
• Provide technical expertise and response to flood damage.
Communications &

Legislative Affairs (CLA)
• Provide employee emergency notifications through media and internal communication systems
• Provide press releases on critical agency programs and current situation.

Information Solutions Organization (ISO)
•Maintain integrity of telecommunications and computer systems. •Implement contingency and disaster recovery plans.

EMERGENCY RELOCATION FACILITY

The Regional Office, 740 Simms Street, Golden, Colorado provides the relocation facility in the event of an emergency or threat that disables the continuation of operations at the RMK Cache, Bldg 810, Lakewood, Colorado. Take a good look at telecommuting from home for a majority of employees. Test this staff by staff. COOP team members are responsible for their own transportation to the RO, regardless of whether the threat was anticipated or unanticipated. All COOP team members must report to the designated facility within 12 hours of activation of the COOP Plan.

Regional Office and RMK Cache Employees

The majority of regional office and cache employees should be instructed to stay at home unless told otherwise; telecommute. All other Regional Office and cache employees and contractors are to follow instructions provided by COOP team personnel. If not designated to relocate to the RO, follows instructions from the Emergency Operations Manager or through the local media. This may include relocating to other office space and/or being placed on Administrative Leave. Employees are to monitor one or more of the following media to obtain information in this regard

- •KCNC Channel 4
- •KUSA channel 9
- •KOA850 AM radio station
- •USFS recording- 303-275-5500.

Interagency Cache Business System Re-engineering Project

(ICBS-R) Continuity of Operations/Business Resumption Plan

Table of Contents

ICBS-R COOP/Business Resumption Plan

Introduction

This document is the Continuity of Operations Plan/Business Resumption Plan for the new Interagency Cache Business System (ICBS). From here on, it will be referred to as the Business Resumption Plan or "BRP."

The purpose of this plan is to aid the users in the event that they are unable to connect to the ICBS application via their usual method (e.g. internet browser on an agency personal computer; logging a wireless bar code scanning device onto a wireless local area network; etc.).

The Business Resumption Plan explains potential procedures and resources for diagnosing system problems and continuing cache operations when the primary means of accessing ICBS become unavailable. The plan also includes a template that should be filled in for each cache with specific contact names and numbers to be used in case of an emergency.

System background

The new ICBS system is being developed for use by National and selected Local Area Support Caches by the ICBS Re-engineering Project ("ICBS-R") Team. ICBS-R is an NWCG-sponsored project. The foundation of the new ICBS a commercial warehouse management/distributed order management system called "Yantra ®," which is a product of the Sterling Commerce Corporation ®. Customizations to Yantra have been made in such a way as to facilitate future releases of the core product. In other words, when a new version of Yantra is released, code changes to ICBS should be very minimal.

ICBS itself consists of the software and associated databases, which are housed on servers at the USDA National Information Technology Center (NITC) in Kansas City, MO. Because it's based on a centralized system rather than on individual copies of software and databases at each cache site, it will enable the interagency cache system to operate as a single enterprise. This will enable the nationwide system of caches to more efficiently manage the overall NFES inventory. However, this also presents the challenge of providing secure and reliable access for each user at each cache facility. The key requirement for meeting this is that each cache has dependable access to an agency-provided network.

A typical ICBS user in a cache will access the system by logging onto their agency PC or laptop, opening a browser (e.g. Internet Explorer ®), entering the URL/website for the application, and then logging into the system with a user name and password. Warehouse workers will log onto a Symbol® wireless bar code scanner device, then log onto the ICBS "mobile terminal" version of the application.

With current cache WMS (Warehouse Management System) software, most warehouse processes are written by warehouse workers on hard copy forms and print-outs for entry at a later time by keyboard operators in a supply office. With the new ICBS, most cache processes will be recorded in real time on the system via wireless scanning devices. Because of this, properly

configured scanning devices and a wireless local area network (WLAN) are necessary to conduct warehouse operations with scanners.

One final aspect of the new system's architecture is that print tasks such as forms, reports and various bar code labels are sent from the ICBS system at NITC to networked printers in cache offices or on the warehouse floor. Two key software programs - Loftware® and Cognos® - are used within Yantra to generate these print tasks. Printing via a non-networked local plug-in printer is not an option. Thus, printers must be configured and networked print tasks tested before a cache is brought online. This often involves changes to various agency/department network settings, firewalls, etc. Once set up and tested, maintaining the connection is mostly dependent on access to the agency network.

As with the current systems, users will need to have a "Plan B" in place for times when network access, or individual components of the new system, is not operational.

User Responsibility

The user's responsibility in carrying out this plan include:

1. Familiarize yourself with the plan
2. Enhance the plan to reflect any unique local conditions
3. Identify appropriate methods of recovery
4. Identify backup equipment/locations for activating contingency plans
5. Identify personnel to carry out the plan
6. Brief all personnel on the location and contents of the plan
7. Implement the plan
8. Test the plan
9. Keep the plan updated

Proactive Mitigation

Because it is a tool that enables caches to provide incident support, ICBS is considered a "mission critical" software program. Many potential problems can be mitigated by knowing who to call when a certain problem arises (such as the ICBS helpdesk, local IT support personnel, etc.).

In most cases, the ICBS Helpdesk is the user's "one stop shop" for obtaining user support. Helpdesk personnel will be trained to work with agency/department personnel (e.g. NITC technicians, network and wireless specialists) and third party providers (e.g. Symbol device support) to trouble-shoot and resolve problems that users are experiencing. At this time support for WLAN issues is most likely going to be provided by the host agency's regular IT helpdesk (e.g. EUSC for FS caches), but ICBS helpdesk personnel will be trained to work with users to determine whether or not it's a WLAN problem or something else.

Local IT support, if it exists, can also be helpful. Such local support can be invaluable if the solution to an "ICBS problem" is to obtain alternate access to a network, a temporary

replacement PC, a replacement printer, to set up a temporary supply office in another building, to install network cables and ports, etc. These local personnel might also be aware of local or agency network changes that could adversely affect a user's ability to access ICBS. Cache managers are encouraged to communicate their ICBS access requirements to any local IT personnel.

Troubleshooting

The first step to business resumption is troubleshooting the problem of being denied access to the ICBS system. The primary goal is to determine the source of the problem and what steps are needed to resolve the issue.

Examples of events that prevent the ICBS user from accessing the ICBS servers or scanners could include: power or phone line outages, disruption of the local area network (LAN) or WLAN, server problems at NITC, etc.

Basic troubleshooting techniques for the ICBS system include:

For PC users:

1. Is the problem limited to one computer?
    a. Try a different computer in your office.
2. Are computers of just one agency unable to connect to the internet?
    a. Try a different computer in your office that connects through a different agency network (BLM, USFS, State).
3. Is the local network available?
    a. Can you access another internet site outside the government network?
    b. Can you access the agency network via a connection in another nearby office?
4. Is another Cache able to access ICBS?
    a. Is the ICBS server operating at NITC?
    b. If the server is up, the Helpdesk will work with NITC to determine whether the problem is occurring at NITC or elsewhere.

For scanner users:

5. Is the problem limited to one wireless device?
    a. Try a different scanner
6. Is the problem with some component of the WLAN?
    a. Do several scanners fail to connect to the application?

Contingency Planning

The key to business continuity and resumption is developing and testing contingency plans for various scenarios. Cache Managers should review their cache-specific BRP with their cache

staff and with their local IT support staff if there is one, and develop steps for continuing or resuming business in the event of some sort of outage.

There are several scenarios that should be considered:

- Can access ICBS via PC, but not via WLAN, so scanners cannot be used
- Cannot access ICBS via either PC or scanning devices
- Cannot access ICBS via normal agency PC and network, but scanners and WLAN are still functional
- Cannot access ICBS via agency network, but dial-up or ISP/VPN connection to internet is available
- Building has lost electrical power, back-up power is not available, or building is otherwise unusable due to natural or human-caused event

There are several possible contingencies for continuing and resuming business operations:

A. Use other agency computers/Regional Office Access

This plan assumes the problem is with specific agency's network. Users would log on to another agency's computer to access ICBS with their normal user name and password.

This plan requires (a) more than one agency computer at or near the cache location; (b) any necessary settings and configurations have been tested; (e.g. NITC/USDA/agency networks have been opened to specific printers) and (c) a user with authority to log onto another agency computer is available.

B. Dial-up via a agency modem bank/ISP VPN/Coordinate with IT

This plan allows users to connect to the ICBS server(s) at NITC via an agency network, but accessing that network is though an agency-provided dial-up connection. This requires a computer with a modem. In some agencies, modems are provided in laptops but not in PCs, and in other agencies, no modems are provided at all and dial-up isn't an option.

It is most expedient if the computer is configured ahead of time with dial-up networking as users will likely need IT support to configure the computer. This may be difficult after normal business hours, and dial-up needs to be tested prior to the actual need arises.

As an alternative to dial-up access, agency networks can be accessed via a subscription-based Internet Service Provider (ISP) such as AOL, and an agency provided Virtual Private Network (VPN) account. The advantage of this approach is that a high speed internet connection should provide much better performance than a dial-up connection. As with the dial-up option, ISP and VPN accounts should be established and tested before the need arises.

C. Use off-site facilities/Regional Office

This option enables a user to move to a pre-established location and resume using ICBS there. Because of the significant prep work required to design, install, test and deploy a WLAN, this option will probably be most viable if ICBS is used in a non-scanning mode (i.e. document warehouse activities on hard copy forms/print-outs and enter the data via keyboard afterwards). This is similar to the way the legacy ICBS is used today. Users might find it helpful to print out key forms ahead of time so that they're ready for this mode of operation.

To facilitate this option, a pre-existing agreement should exist with a public office or vendor. If an extended off-site operation is anticipated and wireless scanning is desired, a suitable site should include network availability (agency or VPN through an internet service provider); PCs; networked laser and label printers; WLAN and scanning device architecture; etc. All of this will require significant set-up and testing time.

In rare cases, the WLAN at the affected cache might be available, while the PCs and printers used in the supply office are not. In these cases, warehouse work could continue at the cache with wireless scanners, and only the office staff would relocate to an off-site office with network, PC and printer capability.

D. Activate agreement with neighboring cache/NRK

There are at least two ways to implement this approach:

1. The first option requires a pre-identified agreement with a neighboring cache to enter your information into the ICBS system should you be unable to access the server. This would generate tasks that a) could be printed and faxed to the affected cache for completion in a non-scanning mode, or b) could be sent directly to the warehouse scanning devices in the affected cache (if the WLAN is intact and communicating with ICBS). .
2. A second way is for the affected cache to completely hand off support of its incidents to the second cache. Because the new system is centralized, this becomes a very viable option because all incident information is centralized and available to any authorized

In either scenario, when the issue is resolved, your office would resume control of your cache workload cache. NRK POC numbers: Patrick Nooney (406-329-4932), Bonny Resner (406-329-4949), and James Chapman (406-896-2872).

E. Use paper-based system

This plan assumes that all options have been exhausted in the continuity of cache ICBS operations. This option requires users to enter data on card stock resource order forms, issues, returns, or other specifically-identified cache forms for the issuance and return of supplies.

Once the system problems have been resolved, the data is entered into the ICBS system. This could very well be the option of choice at this point in time for the caches – especially if the system outage is anticipated to be remedied quickly.

ICBS Emergency Contact Sheet

The following is a template for documenting actions taken to resolve problems concerning a cache's ability to use ICBS. Cache-specific contacts and phone numbers should be filled in ahead of time by personnel at each cache.

Date/Time Notified	Action	Contact and Telephone Number(s)
1.	**Check local network status** Contact Primary IT staff: Flint Cheney Contact Backup IT staff: Doug Wagner	**303-236-0646 o** **303-886-2179 c** **303-275-5104 o** **303-506-1317 c**
2.	**Check with neighbor to see if their network is working.** Primary Contact: Cindy Finley Secondary Contact: Dawn Kerns	**303-275-5131** **303-275-5739**
3.	**If previous two actions are working:** Contact the ICBS Helpdesk	
4.	**Check with local Internet Service Provider, if you are having access problems:** Contact Primary IT staff: Flint Cheney Contact Backup IT staff: Doug Wagner	**303-236-0646 o** **303-886-2179 c** **303-275-5104 o** **303-506-1317 c**
5.	**Activate your backup Business Resumption Plan** A. Use other agency computers B. Dial-up / ISP VPN C. Use of off-site facilities D. Activate agreement with neighboring cache	

Date/Time Notified	Action	Contact and Telephone Number(s)
	E. Use paper-based system	
6.	**Agency dial-up access to network** **ICBS Help Desk** **Henry Myint**	**617-480-9662**
7.	**Loss of power to building:** **1. Secure Building** **2. Relocate to RO Floor 3** **3. Await further instructions**	
8.	**Telephone isn't working:** **1. Utilize cell phone to call support** **2. Open ticket for assistance** **3. Await further instruction**	
9.	**WLAN Issues/Problems Support** Contact Primary IT staff: Flint Cheney Contact Backup IT staff: Doug Wagner	**303-236-0646 o** **303-886-2179 c** **303-275-5104 o** **303-506-1317 c**
10.	**Symbol Scanning Device Support:** Business Hours: ICBS Help Desk **Henry Myint**	**617-480-9662**

Date/Time Notified	Action	Contact and Telephone Number(s)
11.	**Zebra Z4M Plus Label Printer Support:** Business Hours: ICBS Help Desk **Henry Myint**	**617-480-9662**
12.		
13.		

Insert your own emergency contacts here or others we may have overlooked.		
Date/Time Notified	**Action**	**Contact and Telephone Number(s)**
1.	Regional Office: Bill Ott Brian Bischof	303-275-5749 303-275-5758
2.		

3.		
4.		
5.		

Appendix B

Additional Suggested Items to Ensure Access to ICBS

It's desirable for each interagency support cache to have the capability of accessing the ICBS system by a minimum of two access methods.

1. Primary: The local agency network (LAN, WAN, etc).
2. Secondary Methods:
    a. Another agency network
    b. An Internet Service Provider
    c. Dialing in to the local area network to access ICBS

Backup computers:

- Access to laptops with modems for setting up alternative dial-up methods.

Analog Phone Line available for modem dialing usage:

- A number of telephone systems are now digital and cannot be used with a modem for dialing into another system.
- Consider the option of having one or two analog phone lines dedicated for this use.

Modem Capability:

- A minimum modem capability would be a 56.2 Kbaud data modem.
- A spare external modem may be considered as a backup.

Accessing ICBS via Dial-Up

There is no modem bank for direct dial-up to ICBS at the USDA National Information Technology Center (NITC), but users might be able to access ICBS by dialing directly into an agency-provided local area network. This option requires a computer with an internal or external modem that has been configured to dial out.

You will need to contact an agency IT staff to have back-up computers configured and to obtain instructions on dialing out. If this is an option at your site, it is imperative that the computers be configured by the IT staff prior to the urgent need for dial-up access.

Dial-up Connection Numbers

Primary Dial-up Number	**Coordinate with Flint**
Secondary Dial-up Number	
Additional Numbers	

Dial-Up Profile Usage Guidelines

The following are some general caveats for agency dial-up access:

1. User names and passwords must not be shared. If this information is shared, you are responsible for all activity with the profile.

2. Most agencies have policies or regulations on proper usage of computers, including the Internet. Keep in mind that in addition to the agency that employs you, the regulations of the agency that provides dial-up access will also apply since you are utilizing its networks to access the internet, and subsequently, ICBS. The most restrictive policy could be enforced and may result in disciplinary action consistent with the nature and scope of such activity.

3. In addition to policy, regulation and public law, there is what is known as "efficient use of the network." Inefficient use of the network slows down the network for other users. ICBS is a mission-critical application. Network resources are limited, so please consider this when utilizing your profile.

   Some examples of inefficient usage are:
   - Listening to the am/fm radio on our computer.
   - Services such as ESPN Sports Update or other automated data update or collection services.
   - Getting your hourly stock quotes over the computer network.
   - Watching videos over the Internet.

   These activities can be a heavy drain on network resources and may adversely affect <u>everyone</u> sharing the network.

   Some policy References: *Please consult your agency computer personnel for complete listing.*

   - Agency Computer Profile Responsibility Forms (i.e. BLM Form 1264-3, User Profile for FS)
   - Agency handbooks, manuals, & other regulations (i.e. Dept. of Interior Manual 375 DM 19.11M)
   - 5 CFR §2635 Subpart G – Misuse of Government Time, Equipment, and Information
   - Public Law 99-474 Prohibits unauthorized use of the US Government computer and/or software.