	OFFICE OF STATE FIRE MARSHAL *INCIDENT MANAGEMENT TEAMS* **STANDARD OPERATING GUIDELINES**	**Number: SOG- I -2001** **Adoption Date:** July 2012 **Author: Don Schallberger** **Review/Revision Date:**
ERU Program Manager Mariana Ruiz-Temple Date 7/9/12 Mariana Ruiz-Temple, Emergency Response Mgr		

SUBJECT: Planning Section Computer Network System

OBJECTIVE: To identify the use, deployment and maintenance of the Planning Section Computer System

I. SCOPE

The Planning Section Committee has identified a need to improve communication and documentation during IMT deployments. The creation of a "computer network system" (CNS) to assist the planning section in creating Incident Action Plans (IAP), communicate with the Agency Operation Center (AOC) via fax or internet and provide the management team computer access (including fax and internet). Each Team shall be assigned a CNS for their use during State drills, exercises and deployments.

II. GENERAL

a. Components

The configuration of each CNS comprises of:

Qty	CDWG #	Description
1	2686020	Cradle Point MBR1200B Small Business Mobile Broadband Router
3	2698517	Logitech Mouse B100-TAA-Mouse
4	2087065	Tripp Lite 10' yellow Cat5e Snagless RJ45 UTP Patch Cable
2	324500	Tripp Lite 25' Blue Cat5e Snagless RJ45 UTP Patch Cable
1	1068880	Belkin 12 outlet, 8' cord surge
1	2204011	WD My Book Live Personal Cloud Storage-NAS
1	2535189	HP Envy 114 e-All-in-one printers
2	1463748	HP #60XL Black Ink Cartridge
2	1463749	HP #60XL Tri-color Ink Cartridge
3	2177693	Verbatim USB Flash Drive – 2GB
1	----------	Carrying case for all components

b. Set-up

The Set-up instructions (Quick Guide) are contained in Appendix A at the end of this document.

c. CNS Storage/ Deployment

To insure rapid and reliable arrival to the incident command post the Planning Section Chief (PSC) shall be assigned and responsible for storing the CNS[1]. Upon deployment the PSC shall insure the CNS accompanies them with their other deployment supplies and equipment.

Occasionally the PSC will trade their on-call time with another PSC. When this happens the fill-in PSC shall deploy their CNS should a deployment occur. If this trade occurs with a PSC from the pool then the Team PSC shall make arrangements with their IC to pass the CNS with another Command and General Staff member prior to the trade to insure the CNS is available for the on-call team.

d. CNS Set-up/Restoration

The PSC is responsible to insure that the CNS is set-up as soon as a location for the Planning Section is established. On arrival the Documentation Unit Leader may be assigned to set-up the CNS in the Planning Section. All planning Section personnel should be familiar with the set-up if the Documentation Unit Leader is not available.

At the completion of the incident/exercise the Documentation Unit Leader shall copy all electronic files onto a CD or USB drive to be kept with other documentation. The Documentation Unit Leader shall erase all files that were created during the incident/exercise and insure that the structures of the CNS folders are ready for the next use. The Documentation Unit Leader shall break down the CNS and package in travel case for PSC to travel home.

e. Routine Maintenance/Updates

All maintenance and updates shall be performed during the quarterly scheduled Planning Section Committee meetings. Unless an otherwise urgent need occurs all maintenance and updates shall occur at the Spring committee meeting (prior to the fire season). All CNS's will be brought to the meeting, set-up and maintenance and update completed to assure each system is identical in operation. Any additions or changes need to be vetted through the Planning Committee and approved by the IMT Program Manager prior to the spring meeting.

f. Oregon State Fire Marshals Office

Will provide the component's and carrying case for the networks as well as USB modems for internet access.

[1] Planning Section Chiefs will be required to sign a

III. STATE OWNED COMPUTER EQUIPMENT

a. The following applies to all personnel utilizing state owned computer equipment as agreed between the User and the State of Oregon, Office of State Fire Marshal. All State owned computer equipment is subject to the same policies and procedures.

b. AUTHORIZED SOFTWARE INSTALLATION ON STATE OWNED COMPUTERS

All personnel utilizing state owned computer equipment must submit a computer security form (Attachment 1) to the OSFM Program coordinator acknowledging that they have read and agree to the guidelines.

All software purchased or obtained by OSFM will be delivered to the OSFM System Administrator or the OSFM Program Coordinator before being installed on state owned computer equipment. All documentation, including registration material, user manuals, etc. will also be delivered at this time. Upon receipt, software will be checked for viruses.

On a periodic basis, the OSFM System Administrator or the OSFM Program Coordinator will perform physical inventory checks of state owned computers to insure that only authorized software is installed.

Each user is responsible for the software installed on the computer(s) they have. If during periodic inspections, unauthorized computer software is found on state owned computers, this software will be immediately removed and a determination of the person responsible for introducing the software will be made. The person responsible for introducing non-authorized software shall be disciplined in accordance with local policy governing this issue. If the local agency does not have a policy, the contractor will be responsible for any legal action brought against the State as a result of the use of illegal software.
REFERENCE: ORS 291.038, DAS Policy 03-08, and OSP Policy 705.1

c. COMPUTER PROTECTION FROM COMPUTER VIRUSES

Any personnel receiving **software** from any outside source will send that disk to the OSFM System Administrator or OSFM Program Coordinator prior to placing that disk in any state owned computer.

The OSFM System Administrator or OSFM Program Coordinator will use all available virus checking procedures to insure the disk is free of computer viruses before releasing the disk to the user.

If user personnel receive any indication that a virus is present on their computer, they will immediately stop all operations on that computer and report the incident

to the OSFM System Administrator or the OSFM Program Coordinator. The computer will not be used until the machine has been released by one of the above individuals. The computer operator should not, under any conditions, remove a suspect disk from their computer and install it in another computer.

The user will be held financially responsible for any damage to the state owned computer equipment resulting from the introduction of a computer virus.

d. USE OF PERSONAL SOFTWARE ON STATE OWNED COMPUTERS

Use of personally owned, or other non-state owned software, on an agency computer is not permitted.

If during periodic inspections, unauthorized computer software is found on agency computers, this software will be immediately removed and a determination of the person responsible for introducing the software will be made. The person responsible for introducing non-authorized software shall be disciplined in accordance with local policy governing this issue. The user shall also be responsible for all costs associated with the removal of unauthorized software, as well as for the costs of any repairs caused by damage related the installation of that software.

e. USE OF STATE OWNED COMPUTERS FOR PERSONAL PURPOSES.

Use of state owned computers for personal purposes is prohibited.

As stated in the general section of this SOG, all state owned computer equipment are subject to the same policies and procedures as equipment located within a state agency. Included in these policies and procedures is the Department of State Police policy 705.1 subject, microcomputers. Rule #3 of this policy states: "Personal Use: The use of Department microcomputer equipment including hardware, software, documentation, and data is limited only to the support of agency functions. Any unauthorized personal use is strictly prohibited.

Personal use of state owned computers by any Contractor personnel is strictly prohibited.

ATTACHMENT 1

Office of State Fire Marshal
4760 Portland Rd. NE
Salem, OR 97305

ACKNOWLEDGMENT OF COMPUTER POLICIES OF THE OFFICE OF STATE FIRE MARSHAL

I, the undersigned, acknowledge that I have read and will comply with the State Computer policy as stated in SOG- I -2001.

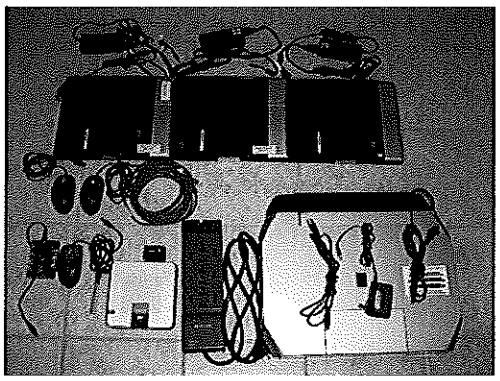
I understand personal use of computer equipment owned by the State of Oregon is prohibited.

I also understand that non-compliance with these SOG's may result in discipline in accordance with local policy governing this issue. If the Users local agency does not have a policy, the contractor will be responsible for any legal action brought against the State as a result of the use of illegal software.

Signature	Date
Printed Name	Team / Position

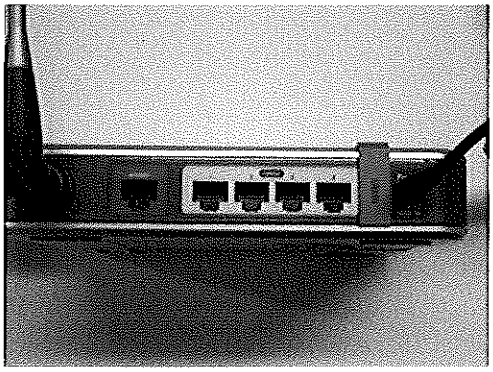
COMPUTER NETWORK SYSTEM SET-UP

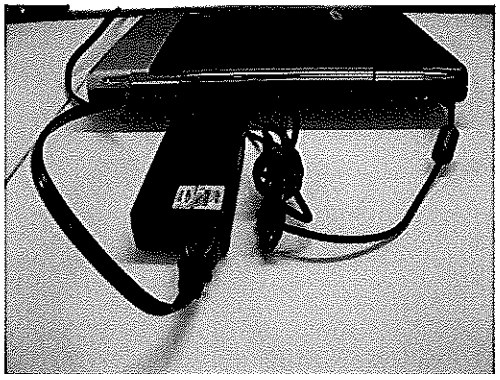
Appendix A



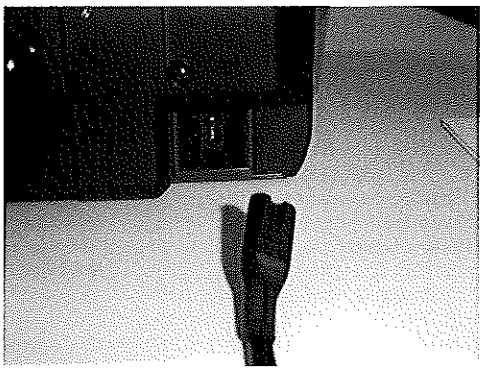
1. Unpack Network box with components. Components should include; Three laptops with power cords and mice. One printer with power cord and interface cable (runs between printer and laptop ERU 19). One router with power cord. Three blue cables that run between computers and router and a USB multi-port adapter.

2. Plug in router to power strip.
   Router power inlet is located on left side of router towards front corner.



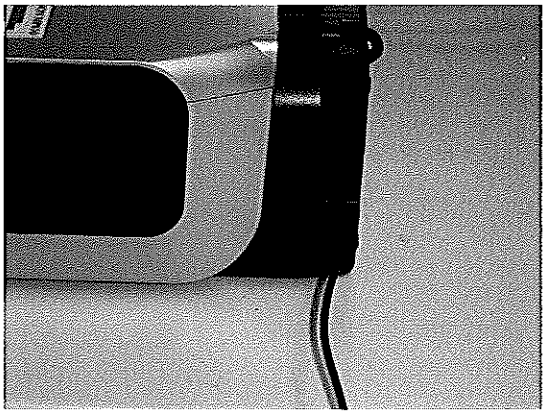


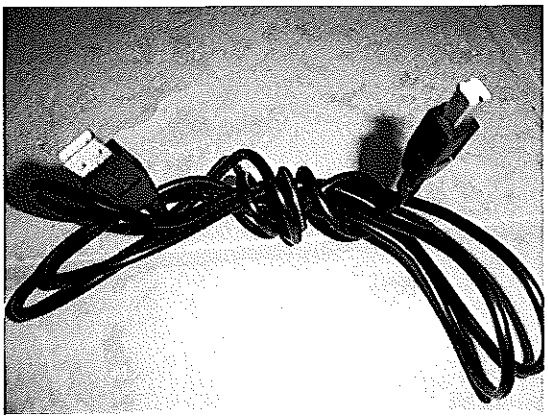
3. Plug in laptops to power strip and power each up.
Laptop power inlet is on back of computer near left corner.



4. Plug printer into power strip and power up.
Printer power inlet is at rear of printer near left corner.

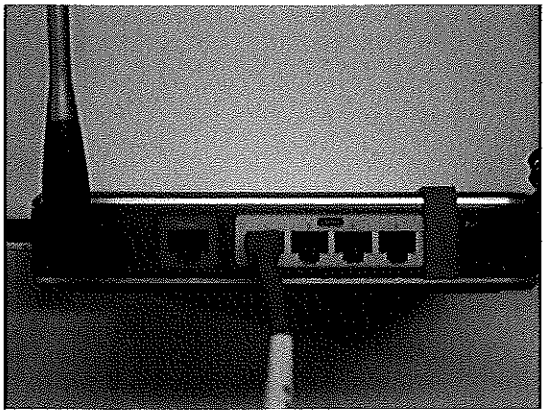
5. Connect data cable between printer and ERU 19 laptop.
Open panel on back of laptop to access USB port (printer is only shared on ERU19).

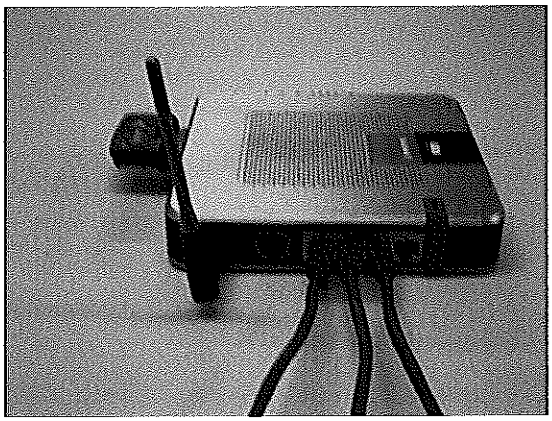




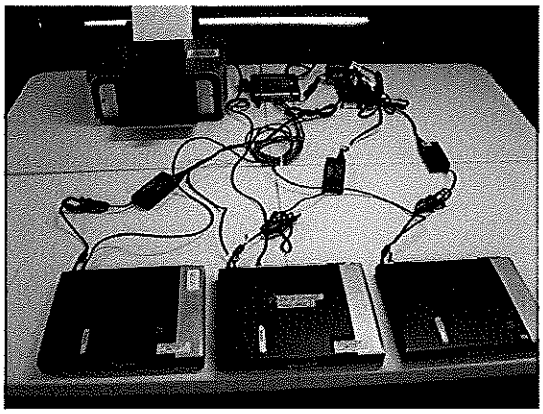
6. Connect one end of a network cable into each laptop network port (large phone jack).
Network inlet port on laptop is next to power inlet.

7. Connect other end of each network cable into the back of the router (the yellow jacks).
   Do not plug anything into the blue port on the back of the router. (This is only used when you have Comcast or DSL or other broadband modem on site).





Sample setup showing all components.



8. Log into each of the laptops. The username and password is osfmdefault.

ERU19 has two shared items on it;

1. IMTShare is a folder on the hard drive of ERU 19 that all laptops can save files to.
2. IMTPrinter_Plans is the printer.

ERU 7 and ERU 12 Both have a shortcut on the desktop to the IMTShare folder

ERU 7 and ERU 12 both have connections to the printer share and it is set as the default printer.

When you hook into the internet the OSFM Emergency Response Page is the home page. There are currently five (5) Favorites established and are listed below;

- NIMS Resource Center
- ICS Resource Center
- National Response Center
- National Incident Fire Center (NIFC)
- Northwest Coordinating Group (NWCG)

If you add favorites they must be added to each computer to be available as they are not cloned independently.