

	<b>Standard Operating Procedure</b>		
	Title / Subject  <b><u>Gateway</u></b>	Effective Date 09/13/11	Revision Date 09/13/11
	References		

## Contents

1. Introduction: .....	2
2. Purpose:.....	2
3. Technical Background:.....	2
4. Operational Context:.....	2
5. Recommended Protocol/Standard: .....	3
6. Recommended Protocol Procedure:.....	3
6.1 Gateway Request.....	3
6.2 Gateway Activation.....	4
6.3 Gateway Deactivation .....	4
6.4 Mobile Gateway Problem ID and Resolution .....	5
7. Management: .....	5

## **1. Introduction:**

For the purpose of this Standard Operating Procedure (SOP), a Gateway Patch is defined as a system that allows users, such as Incident Management Teams (IMT) and police, fire, and emergency medical services (EMS) command vehicles, to have the ability to establish the patches needed to cross-connect disparate wireless resources. Gateways also provide users with the ability to control their radio/wireless resources from remote locations.

## **2. Purpose:**

Establish SOPs for the use of a gateway to connect disparate wireless systems to support communications interoperability between dissimilar wireless systems in the field at the incident scene. The resource connection, provided by the gateway, will be between the Statewide Interoperable Radio Network (SIRN), local agencies and the external responding on-scene agency (Federal, State, regional, etc.) in need of interoperability using any available wireless resource patched to the wireless resource of the on-scene agency. The objective is to have an SOP in place for West Virginia to have pre-established gateway wireless resources available to external responding on-scene agencies with the need to interoperate during the incident.

## **3. Technical Background:**

A gateway patch between the SIRN and the external responding on-scene agency (Federal, State, regional, etc.) will enable access by the disparate wireless resource to appropriate authorized talkgroups.

## **4. Operational Context:**

Established mutual aid response protocols between agency assigned talkgroups and the external responding on-scene agency (Federal, State, regional, etc.) will provide the basis for operational activation of the gateway. The following is a hierarchy of projected operations based on priority, with the first operation holding the highest priority:

- A large-scale emergency incident that requires a multi-agency, multi-jurisdictional response (e.g., a natural disaster such as a hurricane, a terrorist incident involving weapons of mass destruction).
- Everyday response-level communications to emergency or urgent incidents that require mutual aid response from multiple agencies (e.g., high-speed pursuits crossing jurisdictional boundaries, a large warehouse fire requiring mutual aid response).
- Special event control activities, generally of a pre-planned nature, involving joint participation of two or more agencies (e.g., a large sporting event such as a college football game, a dignitary visit).
- Drill, maintenance, and test exercises.

## 5. Recommended Protocol/Standard:

Established mutual aid response protocols between SIRN and the external responding on-scene agency (Federal, State, regional, etc.) will provide the basis for operational activation of the gateway. The following is a hierarchy of projected operations based on priority, with the first operation holding the highest priority:

- **Establish National Incident Management System** – Depending on the size of the incident, the use of an Incident Command System (ICS) compliant with the National Incident Management System (NIMS) is recommended when using any regional interoperability resource for large-scale multi-agency, multi-jurisdictional incidents.
- **Plain Language** – All interoperable communications during multi-agency, multi-discipline incidents should be in plain language. Avoid using radio codes, acronyms, and abbreviations as they may cause confusion between agencies. Ensure that all verbal requests for assistance or backup specify the reason for the request.
- **Unit Identification** – Announce your home agency prior to announcing your unit identifier during interoperable communications situations when utilizing the gateway.
- **Encryption** – All encrypted radio users must operate in a “clear” mode when a mobile gateway is used, unless otherwise arranged in advance. Never assume that a mobile gateway can manage encryption between systems.
- **Monitoring** – If ICS is established and it is deemed appropriate, the Incident Commander, or his/her designee, will ensure that each channels / talkgroups connected by the gateway is monitored while in use. In a smaller mutual aid response, the Agency Lead may also require that each channels / talkgroups connected by the gateway be monitored.

## 6. Recommended Protocol Procedure:

### 6.1 Gateway Request

The agency requesting the use of a cross-patch with the gateway connection for incident or event communications support should provide the following information to the agency supporting the operation:

- Name of the agency and appropriate authorization verification (e.g., name of authorized user, lead responder for this agency, security credentials).
- The responsible party for requesting agency command or the lead relevant to the mutual aid request.
- The channels / talkgroups /wireless resources required to be connected.
- The duration of the patch activation.
- The process for patch audio monitoring and the responsible agent for recording (e.g., dispatch center, Incident Commander, Radio Operator [RADO]).
- The designation or type of patch: “Command and Control” or “Tactical Operational.”

## 6.2 Gateway Activation

Once agencies agree to cross-patch their wireless resource, the procedures for establishing communications connectivity are:

- Verify that the necessary elements for connectivity are available (e.g., patch cables, connection slots).
- Select the predetermined channels / talkgroups to establish a cross-patch with the disparate wireless resource.
- Verify the system-wide availability of required resources (coordinate among control point dispatchers).
- Provide radio call sign/designator information to connected agencies as necessary.
- Notify the requested unit/agency to the channels / talkgroups availability.
- Notify the responding units to the appropriate talkgroup and have the units switch to the designated shared channels / talkgroups, if required.
- Confirm responding units are operating on the appropriate channels / talkgroups.
- Identify users on the connected channels / talkgroups using their agency name and unit identifier through a roll call when appropriate (users in a secure setting or a mutual aid response may not require dispatcher validation).
- Announce to users at predetermined time intervals, specifically every hour on the hour, that a gateway connection is in place, and interoperable communications procedures are in effect as deemed necessary by the Incident Commander or Agency Lead.
- Monitor the connected channels / talkgroups to address requests as required.
- Monitor the system for problems that may require technician intervention.
- Monitor for system problems that may require a deactivation of the gateway.
- Record the channels / talkgroups, if required or where appropriate.
- Monitor designated calling channel where required.

## 6.3 Gateway Deactivation

When the gateway connections are no longer required, agencies should follow these deactivation procedures:

- The authorizing agent requests the gateway be deactivated.
- Announcement will be made over connected channels / talkgroups that connections will be deactivated prior to the connection being disabled.
- Prior to gateway deactivation, agencies should ensure that all personnel have returned to their appropriate home channels / talkgroups.
- Agencies may want to conduct a roll call of all affected personnel to confirm they returned to their home systems.
- After deactivation of the gateway, channels / talkgroups should be returned to their normal mode of operations.

## **6.4 Mobile Gateway Problem ID and Resolution**

- Report any problems with the gateway connections to the appropriate point of contact (POC) for that agency.
- A routine gateway test should be completed regularly to confirm availability and operational use.
- After action reports should be utilized to help identify potential problems and prospective solutions.

## **7. Management:**

The cooperating agencies are responsible for the operational management of their system.