
# LOCAL RADIO STATION

# MODEL VULNERABILITY ASSESSMENT

# CHECKLIST

**Developed by the Toolkit Working Group for the**
**Media Security and Reliability Council**

**November 16, 2004**

# INDEX

# INTRODUCTION

In the aftermath of the tragedy of September 11, 2001, the Federal Communications Commission recognized the fundamental and essential role that local media play in providing and coordinating communications in emergency situations. The Media Security and Reliability Council ("MSRC I") is a Federal Advisory Committee, formed by the FCC, to study, develop and report on communications and coordination designed to assure the optimal reliability, robustness and security of the broadcast and multi-channel video programming distribution industries in emergency situations.

In the course of its work, the MSRC analyzed the current status of media industries and prepared a set of comprehensive best practice recommendations. These recommendations were provided to the FCC and the Media Industry in March 2004 so that, when implemented, will assure optimal reliability, robustness and security of broadcast and MVPD facilities throughout the United States. These comprehensive best practice recommendations can be found at http://www.fcc.gov/MSRC/.

On May 26, 2004 the FCC announced that it would officially re-charter the MSRC to create a local implementation plan designed to promote voluntary implementation of the MSRC I Best Practices by the broadcast and MVPD industries; develop "model" documents and other resources for local entities' use; and formulate any additional best practices that may be needed.

## Scope

The comprehensive best practices from MSRC I recommended that each national media facility (television network facilities, radio network facilities and cable facilities) should have a vulnerability assessment and disaster recovery plan that is periodically reviewed, updated, and practiced. The scope of this document is to provide general guidelines and a generic checklist to assist local radio stations in assessing vulnerabilities which may potentially affect their facilities in the event of an emergency.

**Vulnerability Assessment Guidelines**

When assessing potential vulnerabilities, local radio stations are encouraged to review the following best practices recommendations made by MSRC I:

- Radio broadcasters should have appropriate physical security, augmented by security personnel and/or video surveillance at their key facilities, including studios/newsrooms, satellite transmit and receive sites and antenna/transmitter sites.

- Radio Broadcasters should employ diverse power grid sources wherever feasible.

- Radio broadcasters should take appropriate measures to provide backup power capabilities for their key facilities, including studios/newsrooms, satellite communications and transmitters.

- Radio broadcasters with local news origination should ensure that they have robust and redundant ways to communicate with external news services and remote news teams, such as the use of mobile radio and Internet to augment cell phones.

- Radio broadcasters should have backup signal feeds to their primary satellite transmit and receive sites.

- Radio broadcasters should have redundant signal paths to their primary and backup transmission facilities.

- Radio broadcasters with local news origination should plan to have emergency origination capability at a separate location from their primary studio (*e.g.*, backup studio, transmitter site, remote van, another station, etc).

- Radio broadcasters with local news origination should have a remote vehicle, or some means of delivering live news and information from a remote site.

- Radio broadcasters should have the capability of receiving a remote feed at an additional site from their primary studio (*e.g.*, directly at their tower site, at a backup studio, etc).

- Radio broadcasters should have a backup satellite transmitter and receiver, or an alternate means (*e.g.*, a Satellite Radio receiver, a dedicated phone line or a streaming audio Internet connection) to send and receive signals from and to national news services in emergency situations.

- Radio broadcasters should have a backup transmitter, and should attempt to make practical arrangements for geographic diversity where possible (*e.g.*, provisions for emergency use of other backup transmitter/antenna facilities in the community or other means).

- With the cooperation of federal and local policy makers, all radio broadcasters in a market should collaborate to increase their collective site diversity and redundancy, including their collective news studios, operations, satellite transmit and receive facilities and transmitter and antenna sites.

## VULNERABILITY ASSESSMENT CHECKLIST

The following vulnerability assessment checklist is provided as a tool for use by local radio stations to help facilitate the assessment of vulnerabilities which potentially may exist in their facilities. This checklist is not intended to be comprehensive, and local radio stations are encouraged to adapt its use to accommodate any unique requirements which may exist in their facilities.

| **Disaster Recovery Plan** | | |
|---|---|---|
| Does a Disaster Recovery Plan exist which details how to effectively assess impact to the facilities and recovery operations in the event of an emergency? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan address timely activation of any backup origination facility in time of emergency? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan include backup delivery methods for network or other programming? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan include reception and delivery of emergency news? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan identify essential personnel necessary to carry out restoration efforts? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan include agreements to gain assistance from other broadcast, cable and production operations? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan identify essential equipment and service suppliers, including contract engineers, construction and installation companies, fuel, and external telecommunications providers, to ensure availability of critical resources? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan include alternative methods to communicate with key field personnel in the event that radio, cell systems or other primary methods are inoperable? | ☐ Yes | ☐ No |
| Does the Disaster Recovery Plan include data restoration and offsite backup of program and playback software (restoration of data includes servers, remote control systems, telephones, and routers)? | ☐ Yes | ☐ No |
| Is the Disaster Recovery Plan periodically reviewed and updated? | ☐ Yes | ☐ No |
| Is the Disaster Recovery Plan periodically tested and rehearsed? | ☐ Yes | ☐ No |

| **Studio Planning** | | | |
|---|---|---|---|
| **Backup Origination Facilities** | Does a backup studio exist at an offsite location? | ☐ Yes | ☐ No |
| **Backup Power** | Does the Studio facility have backup power? | ☐ Yes | ☐ No |
| | Does the primary transmission facility have backup power? | ☐ Yes | ☐ No |
| | Does the backup studio facility have backup power? | ☐ Yes | ☐ No |
| | Does the backup transmission facility have backup power? | ☐ Yes | ☐ No |
| | Can backup power operate long enough to implement the recovery plan? | ☐ Yes | ☐ No |
| | Where backup power is available is it automatically activated? | ☐ Yes | ☐ No |
| | Are the backup power systems routinely tested under load? | ☐ Yes | ☐ No |
| | At least once a year is the backup power tested while the facility is disconnected from the power grid? | ☐ Yes | ☐ No |
| **Security** | Are security protocols sufficient to prevent unauthorized access to the studio facilities? | ☐ Yes | ☐ No |
| **Emergency News & Information** | If national network news agreements do not exist, is there an agreement to carry emergency news from alternate sources? | ☐ Yes | ☐ No |
| | In the event of a failure of the newsroom computer system is there an alternate plan to get news on the air? | ☐ Yes | ☐ No |
| | Can Emergency Alert System ("EAS") alerts be received and rebroadcast from backup facilities, if such facilities exist? | ☐ Yes | ☐ No |

| **Terrestrial Transmission** | | | |
|---|---|---|---|
| **Backup Transmission Facilities** | Is there a backup transmitter and antenna available? | ☐ Yes | ☐ No |
| | If there is a backup transmitter and antenna site, is it geographically diverse from the primary location? | ☐ Yes | ☐ No |
| | Does the backup transmitter and antenna provide service to the metro area? | ☐ Yes | ☐ No |
| **Backup Power** | Does the primary transmission facility have backup power? | ☐ Yes | ☐ No |
| | Does the backup transmission facility have backup power? | ☐ Yes | ☐ No |
| | Can backup power operate long enough to implement the recovery plan? | ☐ Yes | ☐ No |
| | Where backup power is available is it automatically activated? | ☐ Yes | ☐ No |
| | Are the backup power systems routinely tested under load? | ☐ Yes | ☐ No |
| | At least once a year is the backup power tested while the facility is disconnected from the power grid? | ☐ Yes | ☐ No |
| **Security** | Are the security protocols sufficient to prevent unauthorized access to the transmission facilities? | ☐ Yes | ☐ No |
| **Redundant Signal Routes** | Is there a backup signal path to the primary transmitter facility? | ☐ Yes | ☐ No |
| | Do these redundant paths include diverse technologies, (i.e., wired and wireless)? | ☐ Yes | ☐ No |
| | Is there a backup signal path to the backup transmitter facility? | ☐ Yes | ☐ No |
| | Do these redundant paths include diverse technologies, (i.e., wired and wireless)? | ☐ Yes | ☐ No |
| | Are there auxiliary TV or radio tuners at the transmitter site that can be used as an alternate source of news and information? | ☐ Yes | ☐ No |
| | Is a RPU system available for remote broadcasts? | ☐ Yes | ☐ No |
| | Can the RPU signal be received at the transmitter site? | ☐ Yes | ☐ No |
| | If so, can the RPU signal be switched into the transmitter by remote control? | ☐ Yes | ☐ No |
| **Transmission remote control** | Can the transmitter site(s) be remotely controlled from locations other than the main studio? | ☐ Yes | ☐ No |
| | Can the transmitter site(s) be controlled with diverse technologies, (i.e., wired and wireless)? | ☐ Yes | ☐ No |