LOCAL CABLE SYSTEM

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 cable operators in assessing vulnerabilities which may potentially affect their cable system in the event of an emergency.

Vulnerability Assessment Guidelines

When assessing vulnerabilities which potentially may exist, cable operators are encouraged to review the following principles based on the recommendations from MSRC I:

- Vulnerability assessments and disaster recovery plans should be made by smaller cable operators as well as the larger ones. Additionally, to be effective, disaster recovery plans should be periodically updated, tested and rehearsed.

- Vulnerability assessments should consider the location and geographic distribution of key facilities in the market, such as headends and hubs.

- Cable operators in a local market should collaborate, where possible, to increase their collective site and equipment diversity, redundancy and interconnections.

- Cable operators should take appropriate measures to provide redundant and geographically diverse equipment for their headend, hub and plant facilities, appropriate to the system's operations and facilities.

- Cable systems should have redundant signal routes as far out in their network as economically practical.

- Where economically feasible, cable operators should continue to appropriately "harden" their plant, particularly in areas prone to severe weather or natural disasters.

- Cable operators should examine essential equipment and service suppliers to ensure that critical resources will have sufficient capacity to meet needs during an emergency.

- Cable systems and local broadcasters in a market should work jointly to develop prevention plans and to improve the redundancies in their interconnections.

VULNERABILITY ASSESSMENT CHECKLIST

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

Disaster Recovery Plan		
Does a "Disaster Recovery Plan" exist which details how to effectively assess impact to system and recovery operations in the event of an emergency?	☐ Yes	☐ No
Does the Disaster Recovery Plan identify essential personnel necessary to carry out restoration efforts?	☐ Yes	☐ No
Does the Disaster Recovery Plan identify essential equipment and service suppliers, including contract construction and installation, fuel, and external telecommunications providers, to ensure the availability of critical resources?	☐ Yes	☐ No
Does the Disaster Recovery Plan include requirements to ensure that necessary restoration and reconstruction materials can be obtained if there is an anticipated shortage in-house?	☐ Yes	☐ No
Does the Disaster Recovery Plan include reciprocal agreements with other cable operators or local broadcast stations?	☐ 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
Is the Disaster Recovery Plan periodically reviewed and updated?	☐ Yes	☐ No
Is the Disaster Recovery Plan periodically tested and rehearsed?	☐ Yes	☐ No

Headend and Hub Facilities			
Backup Power	Does the primary headend facility have backup power?	☐ Yes	☐ No
	Is headend backup power automatically activated?	☐ Yes	☐ No
	Can headend backup power operate long enough to implement your recovery plan?	☐ Yes	☐ No
	Are headend backup power capabilities routinely tested under load?	☐ Yes	☐ No
	Is the headend disconnected from commercial power during backup power capability testing?	☐ Yes	☐ No
	Do hub facilities have backup power?	☐ Yes	☐ No
	Is hub backup power automatically activated?	☐ Yes	☐ No
	Can hub backup power operate long enough to implement your recovery plan?	☐ Yes	☐ No
	Are hub backup power capabilities routinely tested under load?	☐ Yes	☐ No
	Is the hub disconnected from commercial power during backup power capability testing?	☐ Yes	☐ No
Security	Are the security protocols sufficient to prevent unauthorized access to the headend facilities?	☐ Yes	☐ No
	Are security protocols sufficient to prevent unauthorized access to the hub facilities?	☐ Yes	☐ No
Emergency News & Information	Can the system obtain news and information from a studio, local franchise authority or local television broadcast signal (*e.g.*, ENG/SNG trucks or satellite links) in the event of an emergency?	☐ Yes	☐ No
	Does the capability exist to provide some news or information from a location other than the primary headend in an emergency?	☐ Yes	☐ No
	Can Emergency Alert System ("EAS") messages be received and transmitted from a location other than the primary headend in an emergency?	☐ Yes	☐ No
	Do backup facilities exist to receive a signal feed from at least one local television or radio broadcaster in the event the primary means of reception fails?	☐ Yes	☐ No
Backup Equipment	Is spare headend equipment (e.g., antennas, equipment racks, cable, distribution amps, combiner/splitters, signal processors, etc.) available in sufficient quantities in the event of an emergency?	☐ Yes	☐ No

Headend and Hub Facilities			
	Are copies of headend and hub cabling diagrams accessible by essential personnel in the event of an emergency?	☐ Yes	☐ No
	Are backup copies of essential software applications and data available in the event of an emergency?	☐ Yes	☐ No

Physical Plant			
Backup Power	Where applicable, are the standby batteries in system power supplies fully operational?	☐ Yes	☐ No
	Can backup power operate long enough to implement your recovery plan?	☐ Yes	☐ No
	Are the standby batteries periodically maintained and tested under load?	☐ Yes	☐ No
	Are portable generators available in the event standby time is exceeded?	☐ Yes	☐ No
	Does the system employ diverse power grid sources where feasible?	☐ Yes	☐ No
Redundant Signal Routes	Do redundant signal routes exist from headends to hubs?	☐ Yes	☐ No
	If yes, do these redundant routes include diverse paths?	☐ Yes	☐ No
	Are the redundant routes routinely tested?	☐ Yes	☐ No
	Where applicable, do redundant signal routes exist from hub to nodes?	☐ Yes	☐ No
	If yes, do these redundant routes include diverse paths?	☐ Yes	☐ No
	Are the redundant routes routinely tested?	☐ Yes	☐ No
	Where applicable, do redundant signal routes exist from headend or hub to local franchise authorities?	☐ Yes	☐ No
	If yes, do these redundant routes include diverse paths?	☐ Yes	☐ No
	Are the redundant routes routinely tested?	☐ Yes	☐ No
Backup Equipment	Is spare plant equipment (e.g., active and passive devices, fittings, strand and cable, etc) available in sufficient quantity in an emergency?	☐ Yes	☐ No
	Are copies of plant design maps accessible by essential personnel in the event of an emergency?	☐ Yes	☐ No

Customer Support Facilities			
Backup Power	Do customer support facilities have backup power?	☐ Yes	☐ No
	Is backup power automatically activated?	☐ Yes	☐ No
	Can backup power operate long enough to implement your recovery plan?	☐ Yes	☐ No
	Is the customer support facility standby power capabilities routinely tested under load?	☐ Yes	☐ No
Security	Are security protocols sufficient to prevent unauthorized access to customer support facilities?	☐ Yes	☐ No
Backup Equipment	Does the capability exist to divert calls to an alternate customer support facility in the event of an emergency?	☐ Yes	☐ No
	Are backup copies of essential operations and customer support systems available in the event of an emergency?	☐ Yes	☐ No