DIRECT BROADCAST SATELLITE 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 Direct Broadcast Satellite ("DBS") operators in assessing vulnerabilities which may potentially affect their broadcast system in the event of a disaster.

Vulnerability Assessment Guidelines

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

- Vulnerability assessments should consider the location and geographic distribution of key facilities in the market, such as local receive facilities, uplinks, and customer support facilities.

- Vulnerability Assessments and Disaster Recovery Plans should be periodically updated, tested, and rehearsed.

- DBS operators should take appropriate measures to provide redundant and geographically diverse equipment for their facilities.

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

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

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

VULNERABILITY ASSESSMENT CHECKLIST

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

Disaster Recovery Plan		
Is there a written Disaster Recovery Plan which details how to effectively assess impact to your 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 engineers, construction and installation companies, fuel, and external telecommunications providers, to ensure 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 your Disaster Recovery Plan include reciprocal agreements to assist/gain assistance from other satellite broadcasters, broadcasters, or cable operators?	☐ Yes	☐ No
Is the Disaster Recovery Plan periodically reviewed and updated?	☐ Yes	☐ No
Is the Disaster Recovery Plan periodically tested and rehearsed?	☐ Yes	☐ No

Local Receive Facilities			
Backup Transmission Facilities	Is there a backup Local Receive Facility ("LRF")?	☐ Yes	☐ No
Backup Power	Does the primary LRF have backup power?	☐ Yes	☐ No
	Is the backup power automatically activated?	☐ Yes	☐ No
	Can the backup power run long enough to implement the recovery plan?	☐ Yes	☐ No
	Are the LRF backup power capabilities 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 your LRF facilities?	☐ Yes	☐ No
Emergency News & Information	Does the capability exist to obtain news and information, from a broadcaster's backup studio or remote location (*e.g.*, ENG/SNG trucks or satellite links)?	☐ Yes	☐ No
	Are there reciprocal agreements with other satellite operators, broadcasters or cable operators, to maintain local emergency information availability to the uplink?	☐ Yes	☐ No

Uplink and Downlink Facilities			
Backup Transmission Facilities	Are there backup transmission feeds to allow the uplink to receive LRF signals in the event the primary feeds are inoperable?	☐ Yes	☐ No
	Are the backup transmission feeds tested periodically?	☐ Yes	☐ No
	Is there a backup plan for satellite telemetry and control?	☐ Yes	☐ No
	Are there reciprocal agreements with other satellite operators, broadcasters or cable operators, to maintain local emergency information availability to the uplink?	☐ Yes	☐ No
Backup Power	Is there backup power at the uplink?	☐ Yes	☐ No
	Is the backup power automatically triggered?	☐ Yes	☐ No
	Can the backup power operate for the length of time necessary for implementing the recovery plan?	☐ Yes	☐ No
	At least once a year is the backup power tested while the facility is disconnected from the power grid?	☐ Yes	☐ No
Security	Is the physical security at the uplink sufficient to prevent unauthorized access?	☐ Yes	☐ No
Emergency News & Information	Can the backup facility also receive LRF news and information signals to support a local emergency situation?	☐ Yes	☐ No
	Does the backup facility automatically come online in the event of an emergency at the primary facility?	☐ Yes	☐ No

Customer Support Facilities			
Backup Power	Is there backup power at your Customer Support Facility ("CSF")?	☐ Yes	☐ No
	Is the backup power automatically triggered?	☐ Yes	☐ No
	Can the backup power operate for the length of time necessary for implementing the Disaster Recovery Plan?	☐ Yes	☐ No
	At least once a year is the backup power tested while the facility is disconnected from the power grid?	☐ Yes	☐ No
Security	Is the physical security at the CSF sufficient to prevent unauthorized access?	☐ Yes	☐ No
Emergency News & Information	Is there a CSF capable of delivering at least basic services at a separate location other than the primary facility in the case of a catastrophic loss?	☐ Yes	☐ No
	Does the customer support system automatically divert calls in the event of an emergency at the primary facility?	☐ Yes	☐ No
	Is there a backup plan to communicate with the customer support centers in the event of an emergency?	☐ Yes	☐ No
	Is there a communications plan to inform all Customer Service Representatives ("CSR") of local, regional or national emergency information and how to properly communicate it to customers?	☐ Yes	☐ No