



# Best Practices for Telecommunications Network Reliability

The Network Reliability and Interoperability Council (NRIC) makes communications-related Homeland Security recommendations to the FCC and industry.

This white paper outlines the best practices in facilities management recommended by NRIC and offers effective solutions for compliance.

## I. Introduction

The United States Federal Communications Commission (FCC) has quietly been taking additional steps to help industry protect the nation's communications infrastructure from terrorist threats and natural disasters. Through the Network Reliability and Interoperability Council (NRIC), the FCC has been overseeing a thorough analysis of Telecom and Datacom vulnerabilities, potential threats, and gaps in best practices that affect prevention and restoration of service outages. In 2003, the work of various NRIC committees has produced more than 200 best practice recommendations for service providers, network operators, and equipment suppliers to implement in order to fortify U.S. critical communications infrastructure.

This paper is an addendum to the white paper *Integrated Network and Facility Monitoring Systems for Telecommunications*. It extends the concepts of facility management and building automation to Homeland Security, and addresses how the specific physical security recommendations of the NRIC can be met with technology. TAC has many customer testimonials to the importance of Facility Automation Systems (FAS) with regard to communications infrastructure. Protecting Telecom and Datacom facilities always makes good business sense for cost management and efficiency of ongoing operations. In the post-9/11 world, it is also a critical part of protecting communications services from attack, and assisting in restoration after an incident.

## II. The Mandate of the NRIC and Focus Group 1A

The NRIC was formed in 1992 by the FCC to investigate a rash of Telecom service outages, such as fiber cuts, SS7 signaling problems, power failures, 911 outages, and the like. Since that time, NRIC has matured into a single-voice advisor to the FCC on matters of national Telecom and Datacom reliability. Made up of committee members from more than 35 leading private industry companies, the NRIC now has several Focus Groups that oversee national communications reliability, security, and interoperability. These Focus Groups are:

- Focus Group 1 – Homeland Security
  - 1A – Physical Security
  - 1B – Cyber Security
  - 1C – Public Safety
  - 1D – Disaster Recovery & Mutual Aid
- Focus Group 2 – Network Reliability
- Focus Group 3 – Network Interoperability
- Focus Group 4 – Broadband

The purpose of these Focus Groups is to meet periodically, analyze current problems facing manufacturers and service providers, and create recommendations to industry on what best practices can be implemented for improving the mission of that Focus Group. The result is methodical, and independently conceived, expert solutions that each Focus Group documents at [www.nric.org](http://www.nric.org), and publicizes through various public awareness and education campaigns.

Focus Group 1A, *Homeland Security – Physical Security*, is made up of fifty-six senior representatives from Telecom, cable, Internet and satellite industries. In March 2003, this committee published best practice recommendations on improving the physical security of national Telecom and Datacom infrastructure. With the public support of FCC Chairman Michael Powell, more than 200 best practice recommendations have been voted on for adoption and implementation by industry.

*“Today’s meeting marks the end of the first phase of NRIC’s mission to develop best practices that will help fortify our industry’s critical infrastructure and secure communications for all Americans. Our work is just beginning and much will be asked of us in the months ahead. The industry must now act to adopt and implement these recommendations to ensure the viability and operations of our communications services.”*

FCC Chairman Michael Powell, March 14, 2003

Examples of these recommendations<sup>1</sup> are published here, with practical real-world solutions that can be implemented today using technology from TAC.

## II. Continuum for NRIC VI Best Practices

This section lists some of the published NRIC Best Practice recommendations for which TAC has unique solutions. In all, Andover’s Continuum<sup>®</sup> product family can be applied to 47 of the more than 200 specific actions the NRIC recommends.

Each Best Practice has a unique number format that matches the NRIC report:

X – Y – Z # # #

Where X = the most recent NRIC Council (e.g. “6” for NRIC VI in 2003)  
 Y = the Council in which the Best Practice was last edited (i.e. 6 for current work)  
 Z = 0-4 for Network Reliability, 5 for Physical Security, 8 for Cyber Security  
 # # # = any digits, where every Best Practice has a unique Z # # #

BP Number	Best Practice
6-6-5011	In areas of critical infrastructure, Service Providers, Network Operators and Equipment Suppliers <b>should alarm and continuously monitor all means of facility access</b> (e.g., perimeter doors, windows) to detect intrusion or unsecured access (e.g., doors being propped open).

*Continuum* manages all aspects of site access control, permitting remote monitoring and logging of all access events and personnel at doors, gates, equipment vaults, and cross-connect cabinets. *Continuum* sends alarms for invalid entry attempts, intrusion detection, motion detection, or activity seen by DVR video surveillance. In addition to monitoring, *Continuum* can also open and close controlled doors, gates, and cabinets.

BP Number	Best Practice
6-6-5020	Service Providers, Network Operators and Equipment Suppliers should establish corporate standards and practices to <b>drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks</b> associated with administering and servicing multiple platforms.

*Continuum* enables a single-card, single system architecture through its integrated control paradigm. One or many *Continuum* access controllers log alarms and events to a single database, which administers central control of the entire system. If several third-party controllers or devices exist, *Continuum* can serve as the integration point through its support of industry-standard protocols such as BACnet, LONtalk, and Modbus.

<sup>1</sup> The full report of Focus Group 1A, including all 200+ recommendations, can be found at the NRIC website: <http://www.nric.org/pubs/nric6/date.html>, March 14, 2003 documents, Homeland Security – Physical Security Prevention and Restoration Report – Recommendations, Appendix E – NRIC VI Physical Security Prevention Best Practices.

BP Number	Best Practice
6-6-5049	Service Providers, Network Operators and Equipment Suppliers should consider a <b>strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.</b>

Additional manpower is not the answer to better security. Effective use of manpower and the tools of technology are. The tools that augment a guard force are CCTV, motion sensors, proximity reader access controls, and other security devices. As stand-alone technology, these tools are only marginally effective. Combined with an integrated control system such as *Continuum*, they are most effective. Integrated control enables unique security capabilities, such as panning a camera based on where motion is sensed, or using DVR to log surveillance images before and after access control events. By allowing *Continuum* to take over certain security tasks, fewer guards are needed to effectively monitor many locations.

BP Number	Best Practice
6-6-5055	Service Providers, Network Operators and Equipment Suppliers <b>should establish and maintain (or contract for) a 24/7 emergency call center</b> for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up to date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.

The topic of an Alarm Response Center (ARC) was covered thoroughly in the main body white paper this addendum goes with, *Integrated Network and Facility Monitoring Systems for Telecommunications*. An ARC is an integral part of monitoring, control, and response to physical security threats. The ARC is much more than a 24/7 emergency call center. Using *Continuum* monitoring and control, alarms, access records, and other data are sent over the network (via dial-up modem or the Internet) to a central SQL server at the ARC for storage. Operators at graphical workstations are alerted to any critical alarms that require immediate attention. *Continuum* can automatically page or call a technician's cell phone, based on how the system is configured. This enables quick response to security threats with a minimum of staff, and also sends the right person to attend to the incident.

BP Number	Best Practice
6-6-5064	The electronic equipment <b>area environments</b> for Service Providers and Network Operators <b>should be continuously monitored, controlled and alarmed to detect operating parameters that are outside operating specifications (e.g., equipment temperature, humidity).</b>

A key part of any integrated control strategy is managing all relevant physical security alarms under one umbrella. In addition to access control, *Continuum* also monitors temperature, humidity, commercial power, backup generators, batteries, UPS systems, video surveillance, fire, smoke, and water leak detection. Integrated control enables correlation between alarm conditions and related setpoint thresholds. For example, high power consumption or long runtime for an HVAC unit can easily be correlated with an open door event that is permitting hot outdoor air into the facility. The availability of this correlated data in *Continuum* permits a quick response to fix the problem before network equipment malfunctions or is vandalized.

BP Number	Best Practice
6-6-5174	Service Providers, Network Operators and Equipment Suppliers <b>should adopt a comprehensive physical security plan and design that focuses on providing an integrated approach that seamlessly incorporates diverse layers of security (e.g., access control and appropriate life safety systems, CCTV and recording, sensor technology, administrative procedures, personnel policy and procedures and audit trails).</b>

*Continuum* is this integrated monitoring and control system, seamlessly integrating CCTV monitoring and recording, access control, life safety systems, environmental sensors, personnel records, and regulatory compliance audit trails.

BP Number	Best Practice
6-6-5199	Service Providers and Network Operators should ensure <b>outside plant equipment (e.g., Controlled Environmental Vault, remote terminals) has adequate protection against tampering</b> , and should consider monitoring certain locations against intrusion or tampering.

The monitoring and control of remote facilities, such as CEVs, POP sites, RSUs, and other unmanned locations is a critical part of increased physical security of Telecom and Datacom facilities. *Continuum* manages the diverse layers of physical security noted above, and sends data records and alarms as required to a *Continuum* client workstation where an operator can take action. The *Continuum* family of controllers can manage large remote sites with many diverse points of monitoring and control, and can also monitor and control cross-connect cabinets with no power or environmental systems. Large or small, *Continuum* protects outside plant equipment.

### III. Other Best Practices where Continuum applies:

In the previous section, examples were given on how to apply *Continuum* for specific Best Practice recommendations. There are many more Best Practices that match *Continuum* functionality feature-by-feature. In every case below, *Continuum* can completely implement the Best Practice recommendation.

BP Number	Best Practice
6-6-5001	Service Providers, Network Operators and Equipment Suppliers should establish additional access control measures that provide positive identification (e.g., cameras, PIN, biometrics) in conjunction with basic physical access control procedures at areas of critical infrastructure, as appropriate, to adequately protect the assets.
6-6-5003	Service Providers, Network Operators and Equipment Suppliers should periodically audit all physical security procedures and records (e.g., access control, key control, property control, video surveillance, ID administration, sign-in procedures, guard compliance). Audits should include review of logs and records as well as testing of procedures through activities such as penetration exercises.
BP Number	Best Practice
6-6-5004	Service Providers, Network Operators and Equipment Suppliers should periodically audit all data collection, software management and database management systems related to physical security including response plans.

<b>6-6-5005</b>	Service Providers, Network Operators and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points to include monitoring and recording for incident analysis. Where appropriate, consider providing near-real-time remote monitoring and archiving.
<b>6-6-5008</b>	Service Providers, Network Operators and Equipment Suppliers should establish access control procedures that: 1) Confirm identity of individuals, 2) Confirm authorization to access facility, and 3) Create record of access (e.g., written log, access control system log).
<b>6-6-5009</b>	Service Providers, Network Operators and Equipment Suppliers should provide audit trails on their electronic access control systems.
<b>6-6-5015</b>	Service Providers, Network Operators and Equipment Suppliers should establish separation policies and procedures that require the return of all corporate property and invalidating access to all corporate resources (physical and logical) at the time of separation for employees, contractors and vendors.
<b>6-6-5021</b>	Service Providers, Network Operators and Equipment Suppliers should establish and enforce access control and identification procedures for all individuals (including visitors, contractors, and vendors) that provide for the issuing and proper displaying of ID badges, and the sign-in and escorting procedures where appropriate.
<b>6-6-5026</b>	Service Providers, Network Operators and Equipment Suppliers should include security as an integral part of the facility construction process to ensure that security risks are proactively identified and appropriate solutions are included in the design of the facility (e.g., facility location selection, security system design, configuration of lobby, location of mailroom, compartmentalization of loading docks, design of parking setbacks). Consider sign off authority for security and safety on all construction projects.
<b>6-6-5028</b>	Service Providers, Network Operators and Equipment Suppliers should establish policy and procedures related to access control to provide pre-notification of visits and exception access (e.g., emergency repair or response) to critical facilities.
<b>6-6-5032</b>	Service Providers, Network Operators and Equipment Suppliers should establish a procedure governing the assignments of facility access levels to ensure adequate levels of protection and the accountability of local responsible management for individual access based on risk and need for access.
<b>6-6-5040</b>	Service Providers, Network Operators and Equipment Suppliers should install environmental emergency response equipment (e.g., fire extinguisher, high rate automatically activated pumps) where appropriate, and periodically test environmental emergency response equipment (e.g., fire extinguisher, high rate automatically activated pumps).
<b>6-6-5041</b>	Service Providers, Network Operators and Equipment Suppliers should establish and implement policies and procedures to secure and restrict access to power and environmental control systems (e.g., air conditioning, air filtration, standby emergency power, generators, UPS) against theft, tampering, sabotage, unauthorized access, etc.
<b>6-6-5042</b>	Service Providers and Network Operators should establish and implement policies and procedures to secure and restrict access to fuel supplies against theft, tampering, sabotage, ignition, detonation, contamination, unauthorized access, etc.
<b>6-6-5046</b>	Service Providers and Network Operators should ensure critical infrastructure utility vaults (e.g., fiber vault) are secured from unauthorized access.
<b>6-6-5047</b>	Service Providers, Network Operators and Equipment Suppliers should consider ensuring that critical infrastructure utility vaults (e.g., fiber vault) are equipped to detect unauthorized access (such as the use of proximity and intrusion detection alarms). This might require coordination with local utilities.
<b>BP Number</b>	<b>Best Practice</b>
<b>6-6-5054</b>	When guard services are utilized by Service Providers, Network Operators and Equipment Suppliers, a process should be developed to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.
<b>6-6-5068</b>	Service Providers and Network Operators should establish standards, policies and procedures to ensure that 1) the equipment and personnel from collocated Inter-connectors (e.g., CLECs, ILC, IXC, ISP, ASP, INET) are restricted to defined collocation space and designated pathways, 2) Collocated Inter-connectors' access and equipment moves, adds, and changes (MACs) are actively coordinated by the host.

6-6-5069	For Service Providers and Network Operators collocation sites, the host should require all tenants to adhere to the security standards set for that site.
6-6-5078	Service Providers and Network Operators should consider establishing and ensuring dual transmission of all sensitive alarms and reliability of all communications links between the areas of critical infrastructure and monitoring stations in order to prepare for possible communication failures during emergency or disaster situations.
6-6-5090	Service Providers, Network Operators and Equipment Suppliers should base building designs for new construction, major modification and alteration for security should include consideration for the protection of and accessibility to air handling systems, air intakes and air returns.
6-6-5092	Service Providers, Network Operators and Equipment Suppliers should establish incident reporting and investigations program to ensure that all events are recorded, tracked and investigated. Reported information should be analyzed to identify potential trends.
6-6-5095	Service Providers, Network Operators and Equipment Suppliers should implement a tiered physical security response plan for telecommunications facilities that recognizes the threat levels identified in the Homeland Security's Physical Security Alert Status Program.
6-6-5106	Equipment Suppliers should consider participating in and complying with an industry organization that develops standards in their security, logistics and transportation practices.
6-6-5150	A Service Provider and Network Operator tenant within a telecom hotel should meet with the facility provider regarding security matters and include the facility provider in the overall security and safety notification procedures, as appropriate.
6-6-5159	Network Operators should maintain the ability to detect the location of break-ins along optical and electrical transmission facilities.
6-6-5162	Service Providers, Network Operators and Equipment Suppliers should ensure adequate physical protection for facilities/areas that are used to house certificates and/or encryption key management systems, information or operations.
6-6-5163	Service Providers, Network Operators and Equipment Suppliers should develop and implement procedures for video recordings and equipment that cover tape rotation, storage and replacement, assurance of accurate time/date stamping, and regular operational performance checks of recording and playback equipment.
6-6-5182	Service Providers, Network Operators and Equipment Suppliers should consider compartmentalizing loading dock activities from other operations. As appropriate, the following should be considered: enhanced lighting, remote CCTV monitoring and recording, remote dock door closing capabilities and remote communications capabilities.
6-6-5190	Access to critical areas within Telecom Hotels where Service Providers and Network Operators share common space should be restricted to personnel with a jointly agreed upon need for access.
6-6-5192	The facility provider of a telecom hotel utilizing an electronic perimeter access control system should operate such systems with an up-to-date list of all personnel with authorized access to the facility and require periodic updates to this list from the tenants. Each Service Providers and Network Operators tenant of the telecom hotel should provide a current list of all persons authorized for access to the facility and provide periodic updates to this list.
<b>BP Number</b>	<b>Best Practice</b>
6-6-5204	Service Providers and Network Operators should ensure availability of emergency/backup power generators to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.
6-6-5205	Service Providers and Network Operators should periodically test fuel reserves for emergency/backup power generators for contamination.
6-6-5206	Service Providers and Network Operators should maintain sufficient fuel supplies for emergency/backup power generators running at full load for a minimum of 8 hours .

<b>6-6-5209</b>	Service Providers and Network Operators should tightly control access to the AC transfer switch housing area, and ensure that scheduled maintenance of the transfer switch is performed and spare parts are available.
<b>6-6-5213</b>	Where feasible, Service Providers and Network Operators should place fuel tanks underground. Access to fill pipes, vents, manways, etc. should be restricted (e.g., containment by fencing, walls, buildings) to reduce the possibility of unauthorized access. Where feasible, fuel lines should be completely buried to reduce accessibility.

## IV. Conclusion

FCC Chairman Michael Powell chartered NRIC VI January 7, 2002 to focus on Homeland Security by ensuring the security and sustainability of public Telecom networks in the event of a terrorist attack or national disaster. Membership in NRIC was expanded in NRIC VI to include 56 corporate representatives from cable, wireless, satellite, and ISP industries.

The NRIC, as a multi-vendor independent authority, has made clear and specific recommendations to industry for increased physical security at Telecom and Datacom sites, such as COs, Data Centers, Mobile Switching Centers, and Outside Plant. The purpose of systematically identifying these Best Practices is to protect the nation's communications infrastructure against attack and to prepare for service continuation and disaster recovery should an attack occur.

For these Best Practices to be implemented, Service Providers, Network Operators, and Equipment Suppliers must ensure that their current operations and security practices follow these Best Practices. And take action where there are deficiencies.

Andover's Continuum family is designed for this integrated control, monitoring, and security task, and is uniquely positioned to help industry deploy practical and cost-effective infrastructure protection solutions.

## V. Glossary

**ARC:** Alarm Response Center. The group or organization in a company that is responsible for managing alarm incidents that occur at remote unstaffed facilities. Experts in HVAC, security, access control, and other disciplines occupy this center.

**CEV:** Controlled Environmental Vault. An underground room, housing electronic and/or optical equipment under controlled thermal and humidity conditions.

**CCTV:** Closed-Circuit Television. A method for monitoring locations by video camera and displaying images on a central TV monitor. See related DVR.

**CO:** Central Office. The building where end users' lines are joined to switching equipment that connects other end users to each other, both locally and via long distance carriers. The central office contains the associated inside plant network elements to perform this function.

**Cross-connect Cabinet:** A cabinet containing terminals in which jumper wires are used to connect feeder pairs to distribution pairs. Also known as a *servicing area interface* or *cross box*.

**DVR:** Digital Video Recorder. A computer-based systems for recording video images. The digital image format enables storage, indexing, retrieval, and networking of still and motion video segments. See related CCTV.

**Event Correlation:** The mechanism of mapping multiple events to a single alarm condition for the purpose of pinpointing the root cause of a problem.

**FAS:** Facility Automation System. An integrated control and monitoring system used to automate the management of remote offices for the purpose of improving operations and reducing costs.

**HVAC:** Heating, Ventilation, and Air Conditioning.

**Outside Plant:** A general term for remote, unmanned facilities where a Service Providers or Network Operators houses communications and control equipment that supports customer services.

**POP:** Point of Presence. A remote facility where a long distance telephone and data carrier network interfaces with the network of the local exchange carrier.

**RSU:** Remote Switching Unit. A small remotely controlled electronic end office switch that obtains its call and data processing capability from a host office or central office switch.

**SQL:** Structured Query Language. An industry-standard language used for manipulation of data in a relational database.

**UPS:** Uninterruptible Power Supply. A "standby" power source that provides continuous power to a device by automatically switching from standard AC power to a backup battery in the event of a primary power interruption.

**WAN:** Wide Area Network. A network that uses high-speed, long-distance communications cables or satellites to connect computers over distances generally greater than two miles. The Internet itself is considered a WAN.

---

Copyright © 2005, TAC  
All brand names, trademarks and registered trademarks  
are the property of their respective owners. Information  
contained within this document is subject to change  
without notice. All rights reserved.

WP-NRIC  
10/05

[www.tac.com](http://www.tac.com)

