Physical Security Committee			
Best Practice Number	**Best Practice Description**	**Final Priority**	**Notes**
7-7-5107	Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.	Critical	It is critical that network operators, service providers and equipment suppliers perform risk assessments of their communications networks for all configurations and develop risk mitigation procedures/processes to reduce the duration or severity of future critical communications outages. This is of particular importance where there is a concentration of equipment, circuits, facilities, etc. and the impact of a major failure could cascade to a larger geographic region.
7-7-5196	MOPs: Network Operators and Service Providers should ensure that contractors and Equipment Supplier personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.	Critical	Any time a technical change is made to equipment that supports critical and essential emergency services, a detailed step-by step procedure needs to be written and followed explicitly in order to preclude unplanned service failures that may be caused by technical ignorance, carelessness, accident and/or incomplete work activity.
'7-7-5084	<b>Hardware & Software Quality Assurance:</b> Network Operators, Service Providers and Equipment Suppliers should consider ensuring that outsourcing of hardware and software includes a quality assessment, functional testing and security testing by an independent entity.	Critical	Employing an additional independent entity to provide independent verification and validation adds an additional layer of protection from a separate set of technical experts in order to ensure that critical essential emergency services remain operational.
7-7-5113	Network Operators, Service Providers and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF).	Critical	While it is not uncommon for communications service providers to diversely route emergency or critical communications from the service provider's location over diverse transport facilities (i.e. cables), the transport facilities commonly enter the building structure where such communications are utilized at one entry point to the building/structure. Thus the cable entry point to the building itself becomes a potential "single point for failure" should an excavation crew or others accidentally severe the cables) entering the building.
'7-7-5197	Network Operators, Service Providers, and Property Managers should periodically inspect, or test as appropriate, the grounding systems in critical network facilities.	Critical	Power surges and/or transients can lead to a loss of critical communications , as well as costly damage to low voltage electronic equipment if grounding systems are not properly installed or have been compromised. Further, improperly grounded equipment experiencing a power surge can result in component degradations that may result in latent failures that can be extremely difficult to isolate and resolve. Periodic inspections and/or routine testing of grounding systems can minimize the potential for interruptions to critical communications.
7-6-5170	Network Operators, Service Providers and Equipment Suppliers should control or disable all administrative access ports (e.g., manufacturer) into R&D or production systems (e.g., remap access ports, require callback verification, add second level access gateway).	Critical	To ensure that only authorized personal can manage the communications systems, there should be no back-doors or remote access with weak security. Having such access may lead to confusion with multiple parties updating the systems or in a worst case, may be used as a basis for a malicious attack against the communications system.
7-7-5074	Network Operators, Service Providers, and Equipment Suppliers should document in a Disaster Recovery Plan the process for restoring physical security control points for critical infrastructure facilities.	Critical	During times of a natural or man-made disaster, it will be critical to ensure the physical security control points are fully operational. This is particularly important when the situation has resulted from a man-made or terrorist attack and the possibilities of additional actions are unknown.

Physical Security Committee			
Best Practice Number	**Best Practice Description**	**Final Priority**	**Notes**
7-7-5071	In order to prepare for contingencies, Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.	Critical	In order to be ready to address various contingencies that may arise at any time, it is necessary to maintain close liaison with and to maintain priority communications with appropriate emergency operations centers, disaster relief and key government personnel. Once an emergency occurs, it will be difficult to try to develop the appropriate contacts in the various organizations that must be coordinated with.
'7-7-5112	Network Operators, Service Providers and Equipment Suppliers should, at the time of the event, coordinate with the appropriate local, state, or federal agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area).	Critical	During the week of Sep 11 following terrorists attacks and also following Hurricane Katrina events in New Orleans, restoration efforts were hampered by personnel identification practices and the lack of clear plans relative to who may or may not gain access to the blighted areas. Furthermore, the personal safety of restoration personnel and emergency responders can affect the timeliness of service restoration and delivery of aid.
7-6-5162	Network Operators, Service Providers 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.	Critical	Certificates and key management systems are used to generate the credentials for access to various critical components of the communications system. If the certificates and systems used to generate keys are damaged or unavailable, then the systems they govern will eventually fail due to authentication failures. Furthermore, stolen information can be used a basis for malicious attacks against the system by reconfiguring key systems.
'7-7-5126	Network Operators, Service Providers and Equipment Suppliers should plan for contingency staffing to perform critical functions in response to crisis situations (e.g., natural disasters, labor strike, terrorist attack).	Critical	
'7-7-5046	Network Operators and Property Managers should ensure critical infrastructure utility vaults are secured from unauthorized access.	Highly Important	
'7-7-5199	Network Operators and Service Providers should provide appropriate protection for outside plant equipment (e.g., Controlled Environmental Vault, remote terminals) against tampering and should consider monitoring certain locations against intrusion.	Highly Important	
'7-7-5028	Network Operators, Service Providers and Equipment Suppliers should establish policies and procedures related to access control to provide exception access (e.g., emergency repair or response, forgotten credential, etc.).	Highly Important	
'7-7-5229	Network Operators, Service Providers and Property Managers should have controlled access to comprehensive facility cabling documentation (e.g., equipment installation plans, network connections, power, grounding and bonding) and keep a backup copy of this documentation at a secured off-site location.	Highly Important	
'7-7-5041	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and implement policies and procedures to secure and restrict access to power, environmental, security, and fire protection systems.	Highly Important	
'7-6-5142	Network Operators, Service Providers and Equipment Suppliers should work together to deploy safeguards to protect the software (i.e. generic or upgrade releases) being loaded to network elements through assured communications protocols in order to prevent sabotage.	Highly Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-6-5173	Network Operators and Equipment Suppliers should design wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) to minimize the potential for interception.	Highly Important	Providers of services to people who are deaf (e.g. phone/video relay/ASL interpretation) need to retain secure access to appropriate wireless networks
'7-7-5187	Property Managers of collocation and telecom hotel facilities should be responsible and accountable for common space, critical shared areas (e.g., cable vault, power sources) and perimeter security for the building with consideration of industry standards and best practices.	Highly Important	
'7-6-5274	Network Operators, Service Providers, Equipment Suppliers and Property Managers should, in facilities using automated access control systems, install one mechanical lock to permit key override access to the space(s) secured by the access control system in the event the system fails in the locked mode. An appropriate procedure should be followed to track and control the keys.	Highly Important	
'7-7-5005	Network Operators, Service Providers and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points.	Highly Important	
'7-7-5026	Network Operators, Service Providers, Equipment Suppliers and Property Managers 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. Where appropriate, this review may include elements such as facility location selection, security system design, configuration of the lobby, limitation of outside access points (both doors and windows), location of mailroom, compartmentalization of loading docks, design of parking setbacks, placement and protection of air handling systems and air intakes, structural enhancements, and ramming protection. Consider sign off authority for security and safety on all construction projects.	Highly Important	
'7-7-5034	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing contractual obligations requiring contractors, subcontractors and vendors to conduct background investigations of all personnel who require unescorted access to areas of critical infrastructure or who require access to sensitive information related to critical infrastructure.	Highly Important	
'7-7-5123	Network Operators should maintain and control access to accurate location information of critical network facilities in order to identify physical locations hosting critical infrastructure assets.	Highly Important	
'7-7-5164	Network Operators, Service Providers and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company vehicles and trailers to the appropriate authorities.	Highly Important	
'7-7-5217	Network Operators, Service Providers, Equipment Suppliers and Property Managers should raise awareness of appropriate personnel regarding possible secondary events immediately after an incident and promptly report any suspicious conditions.	Highly Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5022	Network Operators, Service Providers and Equipment Suppliers should internally identify and document areas of critical infrastructure as part of security and emergency response planning. This documentation should be kept current and protected as highly sensitive proprietary information.	Highly Important	
'7-7-5001	Network Operators, Service Providers and Equipment Suppliers should establish additional access control measures that provide two factor 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.	Highly Important	
'7-7-5010	Network Operators, Service Providers and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.	Highly Important	
'7-7-5011	Network Operators, Service Providers, Equipment Suppliers and Property Managers should alarm and monitor critical facility access points to detect intrusion or unsecured access (e.g., doors being propped open).	Highly Important	
'7-6-5012	Network Operators, Service Providers and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel.	Highly Important	
'7-7-5015	Network Operators, Service Providers and Equipment Suppliers should establish separation policies and procedures that require the return of all corporate property and invalidate access to all corporate resources (physical and logical) to coincide with the separation of employees, contractors and vendors.	Highly Important	
'7-7-5021	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and enforce access control and identification procedures for all individuals (including visitors, contractors, and vendors) that provide for the issuing of ID badges, and the sign-in and escorting procedures where appropriate.	Highly Important	
'7-6-5024	Network Operators, Service Providers and Equipment Suppliers should include security as an integral part of the strategic business planning and decision making process to ensure that security risks are properly identified and appropriately mitigated.	Highly Important	
'7-7-5027	Security and Human Resources (for Network Operators, Service Providers or Equipment Suppliers) should partner on major issues to ensure that security risks are identified and plans are developed to protect the company's personnel and assets (e.g., hiring, downsizing, outsourcing, labor disputes, civil disorder).	Highly Important	
'7-7-5029	Network Operators, Service Providers, Equipment Suppliers and Property Managers should facilitate the availability of security related hardware and media (e.g., spare hardware) and/or a contingency plan for its availability in the event of a disaster.	Highly Important	
'7-7-5030	Network Operators, Service Providers and Equipment Suppliers should provide a level of security protection over critical inventory (i.e., spares) that is proportionate to the criticality of the equipment.	Highly Important	
'7-7-5031	Network Operators, Service Providers and Equipment Suppliers should establish a role for the security function (i.e., physical and cyber) in business continuity planning, including emergency response plans and periodic tests of such plans.	Highly Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5040	Network Operators, Service Providers, Equipment Suppliers and Property Managers should install environmental emergency response equipment (e.g., fire extinguishers, high rate automatically activated pumps) where appropriate, and periodically inspect the equipment.	Highly Important	
'7-7-5066	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should ensure that sensitive information pertaining to critical infrastructure is considered proprietary and access is restricted appropriately, both internally and externally. Appropriate markings are required to qualify for exemption from disclosure under FOIA.	Highly Important	
'7-7-5095	Network Operators, Service Providers, Equipment Suppliers and Property Managers should implement a tiered security response plan for communications facilities that recognizes the threat levels identified in the Homeland Security Advisory System.	Highly Important	
'7-7-5096	Network Operators, Service Providers and Equipment Suppliers should require compliance with corporate security standards and programs for contractors, vendors and others, as appropriate. This requirement should be included as part of the terms and conditions of the contract that the contractor or vendor has with the company, and should also be made to apply to their subcontractors.	Highly Important	
'7-6-5097	Network Operators, Service Providers and Equipment Suppliers should establish and implement corporate security standards and requirements in consideration of the best practices of the communications industry (e.g., NRIC Best Practices).	Highly Important	
'7-7-5110	Network Operators should not share information pertaining to the criticality of individual communication facilities or the traffic they carry, except with trusted entities for justified specific purposes with appropriate protections against further disclosure.	Highly Important	
'7-7-5111	Network Operators should not share information regarding the location, configuration or composition of the telecommunication infrastructure where this information would be aggregated at an industry level without proper protection measures acceptable to the information provider.	Highly Important	
'7-6-5131	Network Operators should provide appropriate security for emergency mobile trailers (both pre- and post-deployment) in order to protect against a coordinated terrorist attack on emergency communications capabilities.	Highly Important	
'7-6-5133	Network Operators should protect the identity of locations where emergency mobile trailers and equipment are stored.	Highly Important	
'7-7-5160	Network Operators, Service Providers, Equipment Suppliers and Property Managers should account for the possible absence of critical personnel in their business continuity plan.	Highly Important	
'7-6-5172	Network Operators, Service Providers and Equipment Suppliers should not permit unsecured wireless access points for the distribution of data or operating system upgrades.	Highly Important	
'7-7-5174	Network Operators, Service Providers, Equipment Suppliers and Property Managers should utilize a coordinated physical security methodology that incorporates diverse layers of security in direct proportion to the criticality of the site.	Highly Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5220		Highly Important	
'7-7-5277	Network Operators, Service Providers and Equipment Suppliers who develop hardware, software or firmware should ensure that appropriate security programs are in place for protecting the product from theft or industrial espionage, taking into consideration that some developmental environments around the world present a higher risk level than others.	Highly Important	
'7-7-5279	Network Operators, Service Providers and Equipment Suppliers should consider site specific (e.g., location, region, country) threat information during security program development.	Highly Important	
'7-7-5116	Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide periodic briefings and/or make available industry/Government guidance for identifying suspicious letters or parcels, to personnel (employees or contractors) involved in shipping, receiving or mailroom activities at major locations or critical sites. Protocols for handling any suspicious items should be established in advance and implemented upon the receipt of any suspicious letter or parcel.	Highly Important	
'7-6-5165	Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers (e.g., remote software developers) have the equipment and support necessary to secure their computing platforms and systems to the equivalent level of those on-site. Security software, firewalls and locked file cabinets are all considerations.	Highly Important	
'7-7-5070	Network Operators, Service Providers and Equipment Suppliers should consider establishment of a senior management function for a chief security officer (CSO) or functional equivalent to direct and manage both physical and cyber security.	Highly Important	
'7-6-5200	Network Operators, Service Providers and Equipment Suppliers should establish and implement procedures for the proper disposal and/or destruction of hardware (e.g., hard drives) that contain sensitive or proprietary information.	Highly Important	
'7-7-5048	Network Operators, Service Providers and Equipment Suppliers should establish and implement a policy that requires approval by senior member(s) of the security department for security related goods and services contracts.	Important	
'7-7-5121	Network Operators, Service Providers and Equipment Suppliers should develop and consistently implement software delivery procedures that protect the integrity of the delivered software in order to prevent software loads from being compromised during the delivery process.	Important	
'7-7-5262	Network Operators, Service Providers and Equipment Suppliers should evaluate the vulnerability of storage locations in an effort to protect critical spares.	Important	
'7-7-5020	Network Operators, Service Providers and Equipment Suppliers should consider establishing corporate standards and practices to drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks associated with administering and servicing multiple platforms.	Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5088	Equipment Suppliers should ensure appropriate physical security controls are designed and tested into new products and product upgrades (e.g., tamper resistant enclosures).	Important	
'7-7-5032	Network Operators, Service Providers and Equipment Suppliers should establish a procedure governing the assignment of facility access levels.	Important	
'7-7-5002	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop and implement periodic physical inspections and maintenance as required for all critical security systems.	Important	
'7-7-5003	Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit compliance with physical security policies and procedures.	Important	
'7-7-5014	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and maintain inventory control measures to protect all media associated with Master Key Control (MKC) systems and access control systems.	Important	
'7-7-5019	Network Operators, Service Providers and Equipment Suppliers should consider establishing an employee awareness training program to inform employees who create, receive or transfer proprietary information of their responsibilities for compliance with proprietary information protection policies and procedures.	Important	
'7-6-5069	For Network Operators, Service Providers collocation sites, the Property Manager should require all tenants to adhere to the security standards set for that site.	Important	
'7-6-5149	Network Operators, Service Providers and Equipment Suppliers should, where feasible, ensure that intentional emissions (e.g., RF and optical) from network equipment and transmission facilities are secured sufficiently to ensure that monitoring from outside the intended transmission path or beyond facility physical security boundaries cannot lead to the obtaining of critical network operations information.	Important	
'7-7-5033	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing and implementing background investigation policies that include criminal background checks of employees. The policy should detail elements of the background investigation as well as disqualification criteria.	Important	
'7-7-5006	Network Operators, Service Providers, Equipment Suppliers and Property Managers should have policies and procedures that address tailgating (i.e. following an authorized user through a doorway or vehicle gateway). At critical sites, consider designing access points to minimize tailgating.	Important	
'7-7-5009	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that access control records are retained in conjunction with company standards.	Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5013	In facilities where master key systems are used, Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing hierarchical key control system(s) (e.g., Master Key Control systems) with record keeping data bases and implemented so that keys are distributed only to those with need for access into the locked space (e.g., perimeter doors, offices, restricted areas).	Important	
'7-7-5018	Network Operators, Service Providers and Equipment Suppliers should periodically conduct reviews to ensure that proprietary information is protected in accordance with established policies and procedures.	Important	
'7-6-5023	Network Operators, Service Providers and Equipment Suppliers should establish and enforce a policy that requires all individuals to properly display company identification (e.g., photo ID, visitor badge) while on company property. Individuals not properly displaying a badge should be challenged and/or reported to security.	Important	
'7-6-5025	Network Operators, Service Providers and Equipment Suppliers should include security as an integral part of the merger, acquisition and divestiture process to ensure that security risks are proactively identified and appropriate plans are developed to facilitate the integration and migration of organizational functions (e.g., Due Diligence investigations, integration of policy and procedures).	Important	
'7-7-5042	Network Operators, Service Providers and Property Managers should establish and implement policies and procedures to secure and restrict access to fuel supplies.	Important	
'7-7-5043	Network Operators, Service Providers, Equipment Suppliers and Property Managers should comply with security standards for perimeter lighting.	Important	
'7-7-5044	Network Operators, Service Providers, Equipment Suppliers or Property Managers should plan and maintain landscaping at facilities to enhance the overall level of building security wherever possible. Landscaping at critical facilities should not obstruct necessary security lighting or camera views of ingress and egress areas, and landscaping should also avoid creating fire hazards or hiding places.	Important	
'7-6-5049	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.	Important	
'7-6-5050	When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers and Property Managers, a supervision plan should be established that requires supervisory checks for all posts.	Important	
'7-6-5051	When guard services are utilized by Network Operators, Service Providers and Equipment Suppliers, consider establishing incentives and recognition programs to increase morale and reduce turnover.	Important	
'7-7-5052	Network Operators, Service Providers, Equipment Suppliers and Property Managers using guard services should ensure that each post has written detailed post orders including site specific instructions, up to date emergency contact information and ensure that on the job training occurs.	Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5053	Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit guard services to ensure satisfactory performance, and compliance with organizational contractual requirements.	Important	
'7-6-5054	When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers or Property Managers, 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.	Important	
'7-7-5067	Network Operators, Service Providers and Equipment Suppliers should make security an ongoing priority and provide periodic, at least annually, security awareness information to all personnel. Where appropriate, include contractors and other regular visitors.	Important	
'7-7-5068	Network Operators, Service Providers and Property Managers should establish standards, policies and procedures that, where feasible, separate Inter-connector equipment and personnel access from ILEC floor space.	Important	
'7-7-5089	Service Providers, Network Operators and Equipment Suppliers should establish, implement and enforce appropriate procedures for the storage and movement of equipment and material, including trash removal, to deter theft.	Important	
'7-7-5091	Network Operators, Service Providers and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.	Important	
'7-7-5092	Network Operators, Service Providers and Equipment Suppliers should establish an incident reporting mechanism and investigations program so that security or safety related events are recorded, analyzed, and investigated as appropriate.	Important	
'7-7-5099	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider keeping centralized trash collection outside the building to reduce the potential for fire and access to the building. Dumpsters should be located away from the buildings where feasible.	Important	
'7-7-5100	Network Operators, Service Providers and Equipment Suppliers should interact as needed with federal, state, and local agencies to identify and address potential adverse security impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes).	Important	
'7-7-5105	Network Operators and Equipment Suppliers should consider the security implications of equipment movement both domestically and internationally, including movement across borders and through ports of entry.	Important	
'7-6-5106	Equipment Suppliers should consider participating in and complying with an industry organization that develops standards in their security, logistics and transportation practices.	Important	
'7-7-5114	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish, implement and enforce mailroom and delivery procedures that recognize changes in threat conditions.	Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5115	Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide and reinforce as appropriate mail screening procedures to relevant employees and contractors to increase attention to security.	Important	
'7-7-5120	Network Operators, Service Providers, Equipment Suppliers and Property Managers should evaluate the potential benefits and security implications when making decisions about building and facility signage, both internally and externally.	Important	
'7-7-5129	Network Operators and Service Providers who are required by the government to file outage reports for major network outages should ensure that such reports do not unnecessarily contain information that discloses specific network vulnerabilities, in order to prevent such information from being unnecessarily available in public access.	Important	
'7-7-5130	Network Operators, Service Providers and Equipment Suppliers and the Government should conduct public and media relations in such a way as to avoid disclosing specific network or equipment vulnerabilities that could be exercised by a terrorist.	Important	
'7-6-5132	Network Operators should identify primary and alternate transportation (e.g., air, rail, highway, boat) for emergency mobile trailers and other equipment and personnel.	Important	
'7-7-5134	Network Operators, Service Providers and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together.	Important	
'7-7-5141	Network Operators, Service Providers and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations.	Important	
'7-7-5151	Network Operators, Service Providers and Property Managers located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.	Important	
'7-7-5152	Network Operators, Service Providers and Equipment Suppliers should consider performing targeted sweeps of critical infrastructures and network operations centers for listening devices when suspicion warrants.	Important	
'7-7-5153	Network Operators, Service Providers and Equipment Suppliers should ensure that critical information being provided to other companies as part of bid processes is covered under non-disclosure agreements and limited to a need to know basis.	Important	
'7-7-5158	Network Operators, Service Providers and Equipment Suppliers should consider unannounced internal security audits at random intervals to enforce compliance with company security policies.	Important	
'7-7-5163	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing procedures for video equipment and recording, where utilized (e.g., storage, accurate time/date stamping and regular operational performance checks).	Important	
'7-7-5166	Equipment Suppliers should, wherever feasible, isolate R&D and software manufacturing of Network Elements from general office systems to prevent unauthorized access.	Important	

Physical Security Committee			
Best Practice Number	**Best Practice Description**	**Final Priority**	**Notes**
'7-7-5167	Network Operators, Service Providers and Equipment Suppliers should provide secured methods, both physical and electronic, for the internal distribution of software development and production materials.	Important	
'7-6-5168	Equipment Suppliers should periodically review personnel background information and assess changes in personnel, departmental, or corporate environment as they affect the security posture of R&D and manufacturing areas and processes.	Important	
'7-6-5169	Equipment Suppliers should establish and implement an information protection process to control and manage the distribution of critical R&D documentation and the revisions thereto (e.g., serialize physical and electronic documentation to maintain audit trails).	Important	
'7-7-5175	Network Operators, Service Providers and Equipment Suppliers should establish a proprietary information protection policy to protect proprietary information in their possession belonging to the company, business partners and customers from inadvertent, improper or unlawful disclosure. The policy should establish procedures for the classification and marking of information; storage, handling, transfer and transmission of information as well as the destruction of information.	Important	
'7-6-5185	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure the inclusion of fire stair returns in their physical security designs. Further, they should ensure that there are no fire tower or stair re-entries into areas of critical infrastructure, where permitted by code.	Important	
'7-7-5188	Network Operators and Service Providers in multi-tenant communications facilities (e.g., telecom hotels) should provide or arrange security for their own space with consideration of NRIC Best Practices and in coordination with the existing security programs for the building.	Important	
'7-7-5192	Network Operators and Service Providers tenants of a telecom hotel should provide a current list of all persons authorized for access to the Property Manager, provide periodic updates to this list, and provide instructions for exceptions (e.g., emergency restoration personnel).	Important	
'7-7-5216	Network Operators, Service Providers and Property Managers should consider providing secure pre-constructed exterior wall pathways for mobile generator connections or tap box connections.	Important	
'7-7-5234	Network Operators, Service Providers and Property Managers should provide or arrange for security to protect temporary equipment placements and staging areas for critical infrastructure equipment in a disaster area.	Important	
'7-6-5254	During restoration efforts, Network Operators and Service Providers should not permit unsecured wireless access points for the distribution of critical data or operating system upgrades.	Important	
'7-6-5255	Network Operators, Service Providers and Equipment Suppliers should ensure that temporary wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) used during an incident are subsequently disabled or secured.	Important	

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
'7-7-5256	Network Operators, Service Providers and Equipment Suppliers should monitor temporary connections of network test equipment that are established for restoration to prevent access by unauthorized personnel.	Important	
'7-6-5265	Network Operators', Service Providers', Equipment Suppliers' and Property Managers' senior management should actively support compliance with established corporate security policies and procedures.	Important	
'7-7-5269	Network Operators, Service Providers, Equipment Suppliers and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.	Important	
'7-7-5280	Network Operators, Service Providers and Equipment Suppliers should instruct security personnel to confirm the authenticity of directions to supersede existing security processes or procedures.	Important	
'7-6-5179	Network Operators, Service Providers and Equipment Suppliers should establish policies and procedures that mitigate workplace violence.	Important	