NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/Unchanged/Deleted
7-7-5001	Service Providers, Network Operators 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.		Changed
7-7-5002	Service Providers, Network Operators, Equipment Suppliers and Property Managers should develop and implement periodic physical inspections and maintenance as required for all critical security systems.		Changed
7-7-5003	Service Providers, Network Operators, Equipment Suppliers and Property Managers should periodically audit compliance with physical security policies and procedures.	Examples of policies and procedures for review may include access control, key control, property control, video surveillance, ID administration, sign-in procedures, guard compliance.	Changed
6-6-5004	Recommend deletion. Superseded by BP 5003.		Deleted
7-7-5005	Service Providers, Network Operators and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points.		Changed
7-7-5006	Service Providers, Network Operators, 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.		Changed
6-6-5008	Recommend deletion. Superseded by BP 5021.	Move to reference section of 5021...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).	Deleted
7-7-5009	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that access control records are retained in conjunction with company standards.		Changed
7-7-5010	Service Providers, Network Operators and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.		Changed
7-7-5011	Service Providers, Network Operators, 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).		Changed
7-6-5012	Service Providers, Network Operators and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel.		Unchanged
7-7-5013	In facilities where master key systems are used, Service Providers, Network Operators, 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).		Changed
7-7-5014	Service Providers, Network Operators, 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 .	Media associated with Master Key Control systems includes: master keys, key blanks, cards, tokens, fobs.	Changed
7-7-5015	Service Providers, Network Operators 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.		Changed
6-6-5016	Recommend deletion. Superseded by BP 5015.		Deleted

7-7-5018	Service Providers, Network Operators and Equipment Suppliers should periodically conduct reviews to ensure that proprietary information is protected in accordance with established policies and procedures.		Changed
7-7-5019	Service Providers, Network Operators 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.		Changed
7-7-5020	Service Providers, Network Operators 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.		Changed
7-7-5021	Service Providers, Network Operators, 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.	Objectives of access control may include 1) identification of the requesting entity individuals, 2) authorization to access facility, and 3) Creation of record of access (e.g., written log, access control system log).	Changed
7-7-5022	Service Providers, Network Operators 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.		Changed
7-6-5023	Service Providers, Network Operators 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.		Unchanged
7-6-5024	Service Providers, Network Operators 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.		Unchanged
7-6-5025	Service Providers, Network Operators 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).		Unchanged
7-7-5026	Service Providers, Network Operators, 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.		Changed

7-7-5027	Security and Human Resources (for Service Providers, Network Operators 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).		Changed
7-7-5028	Service Providers, Network Operators 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.).		Changed
7-7-5029	Service Providers, Network Operators, 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.		Changed
7-7-5030	Service Providers, Network Operators 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.		Changed
7-7-5031	Service Providers, Network Operators 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.		Changed
7-7-5032	Service Providers, Network Operators and Equipment Suppliers should establish a procedure governing the assignment of facility access levels.		Changed
7-7-5033	Service Providers, Network Operators, 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.		Changed
7-7-5034	Service Providers, Network Operators, 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.		Changed
6-6-5036	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-6-5037	Recommend deletion. Superseded by BP 5034.		Deleted
6-6-5038	Recommend deletion. Superseded by BP 5026.		Deleted
7-7-5040	Service Providers, Network Operators, 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.		Changed
7-7-5041	Service Providers, Network Operators, 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.	Examples of power and environmental systems: HVAC, standby emergency power, generators, UPS.	Changed
7-7-5042	Service Providers, Network Operators and Property Managers should establish and implement policies and procedures to secure and restrict access to fuel supplies.		Changed
7-7-5043	Service Providers, Network Operators, Equipment Suppliers and Property Managers should comply with security standards for perimeter lighting.	For example; SLB, Illuminating Engineering Society of North America (IESNA), http://www.iesna.org.	Changed

7-7-5044	Service Providers, Network Operators, 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.		Changed
6-6-5045	Recommend deletion. Superseded by BP 5044.		Deleted
7-7-5046	Network Operators and Property Managers should ensure critical infrastructure utility vaults are secured from unauthorized access.	For example, access to fiber vaults though manholes.	Changed
6-6-5047	Recommend deletion. Superseded by BP 5199.		Deleted
7-7-5048	Service Providers, Network Operators 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.		Changed
7-6-5049	Service Providers, Network Operators, 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.		Unchanged
7-6-5050	When guard services are utilized by Service Providers, Network Operators, Equipment Suppliers and Property Managers, a supervision plan should be established that requires supervisory checks for all posts.		Unchanged
7-6-5051	When guard services are utilized by Service Providers, Network Operators and Equipment Suppliers, consider establishing incentives and recognition programs to increase morale and reduce turnover.		Unchanged
7-7-5052	Service Providers, Network Operators, 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.		Changed
7-7-5053	Service Providers, Network Operators, Equipment Suppliers and Property Managers should periodically audit guard services to ensure satisfactory performance, and compliance with organizational contractual requirements.		Changed
7-6-5054	When guard services are utilized by Service Providers, Network Operators, 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.		Unchanged
7-6-5055	Service Providers, Network Operators and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center 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.		Unchanged
6-6-5056	Recommend deletion. Superseded by 5026.		Deleted
7-7-5057	Service Providers, Network Operators and Equipment Suppliers should consider an enhanced level of emergency response for locations supporting critical functions.		Changed
7-7-5058	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).	Some local regulations and building codes may influence the options available.	Changed

6-6-5059	Recommend deletion. Superseded by BP 5120.		Deleted
7-7-5061	Equipment Suppliers should consider ergonomics and human-centric factors when designing user interfaces (e.g., hardware labeling, software, documentation).		Changed
7-7-5062	Service Providers, Network Operators and Equipment Suppliers, should staff critical functions at appropriate levels, considering human factors such as workload and fatigue.		Changed
6-6-5063	Recommend deletion. Superseded by BP 5026.		Deleted
7-7-5064	Service Providers, Network Operators and Property Managers should alarm and monitor critical electronic equipment areas to detect parameters that are outside operating specifications (e.g., temperature, humidity).		Changed
6-6-5065	Recommend deletion. Superseded by 5096.		Deleted
7-7-5066	Service Providers, Network Operators, 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.		Changed
7-7-5067	Service Providers, Network Operators 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.		Changed
7-7-5068	Service Providers, Network Operators and Property Managers should establish standards, policies and procedures that, where feasible, separate Inter-connector equipment and personnel access from ILEC floor space.	For example; CLECs, ILC, IXC, ISP, ASP, INET.	Changed
7-6-5069	For Service Providers and Network Operators collocation sites, the Property Manager should require all tenants to adhere to the security standards set for that site.		Unchanged
7-7-5070	Service Providers, Network Operators 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.		Changed
7-7-5071	In order to prepare for contingencies, Service Providers, Network Operators 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.		Changed
7-6-5073	Service Providers, Network Operators and Equipment Suppliers should perform risk assessment on significant network changes (e.g., technology upgrades).		Unchanged
7-7-5074	Service Providers, Network Operators, and Equipment Suppliers should document in a Disaster Recovery Plan the process for restoring physical security control points for critical infrastructure facilities.		Changed
7-7-5076	Network Operators and Service Providers should ensure and periodically review intra-office diversity of critical resources including power, timing source and signaling leads (e.g., SS7).	Example: where CCS links traverse D4 channels banks, the D4 channel bank are often shelves in bays. The first level of diversity is that the CCS links are on different interfaces to different D4 channel banks, the channel banks aggregate link (DS-1) connects to diverse M13 multiplexes or DCS frames, continuing through the multiplexing levels across diverse transport paths. This could be called NE diversity.	Changed

7-7-5078	Service Providers and Network Operators should be automatically notified upon the loss of alarm data and react accordingly.		Changed
7-7-5079	Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points.		Changed
7-7-5080	Network Operators should identify and track critical network equipment, location of spares, and sources of spares to ensure the long term continuity and availability of communication service.		Changed
7-6-5081	Equipment Suppliers should provide serial numbers on critical network components (e.g., circuit packs, field replaceable units).		Unchanged
6-6-5082	Recommend deletion. Superseded by BP 5080.		Deleted
7-7-5083	Service Providers, Network Operators and Equipment Suppliers should maintain the availability of spares for critical network systems.	Emergency replacements that can be shipped from equipment vendor within a short period of time usually within 24 hours.	Changed
6-6-5085	Recommend deletion. Superseded by BP 5089		Deleted
7-6-5086	Equipment Suppliers should consider electronically encoding a unique identifier into non-volatile memory of critical elements (e.g., Field Replaceable Units, FRUs) for integrity and tracking.	Possible guidelines include GR282, GR815 and TL9000.	Unchanged
6-6-5087	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
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).		Changed
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.		Changed
6-6-5090	Recommend deletion. Superseded by BP 5026.		Deleted
7-7-5091	Service Providers, Network Operators and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.	The US Department of State offers information on international travel at http://www.state.gov/travel/.	Changed
7-7-5092	Service Providers, Network Operators 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.	Similar best practice for cyber security is 8548.	Changed
6-6-5093	Recommend deletion. Superseded by BP 0599, 5226 & 1058.		Deleted
6-6-5094	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-5095	Service Providers, Network Operators, 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.		Changed

7-7-5096	Service Providers, Network Operators 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.		Changed
7-6-5097	Service Providers, Network Operators 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).		Unchanged
7-6-5098	Service Providers, Network Operators and Equipment Suppliers should ensure that all network infrastructure equipment meets the minimum requirements of ANSI T1.319 (fire resistance).		Unchanged
7-7-5099	Service Providers, Network Operators, 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.		Changed
7-7-5100	Service Providers, Network Operators 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).		Changed
6-6-5102	Recommend deletion. Superseded by BP 8066.		Deleted
6-6-5103	Recommend deletion. Superseded by BP 5070.		Deleted
6-6-5104	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
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.	US Custom's and Trade Partnership Against Terrorism (C-TPAT) initiative to strengthen overall supply chain and border security). See http://www.customs.ustreas.gov/impoexpo/impoexpo.htm TAPA - Technology and Asset Protection Association.	Changed
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.		Unchanged
7-7-5107	Service Providers, Network Operators and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.		Changed
6-6-5109	Recommend deletion. Superseded by BP 5066.		Deleted
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.		Changed
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.		Changed

7-7-5112	Service Providers, Network Operators 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).		Changed
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.		Changed
7-7-5114	Service Providers, Network Operators, Equipment Suppliers and Property Managers should establish, implement and enforce mailroom and delivery procedures that recognize changes in threat conditions.		Changed
7-7-5115	Service Providers, Network Operators, Equipment Suppliers and Property Managers should provide and reinforce as appropriate mail screening procedures to relevant employees and contractors to increase attention to security.		Changed
7-7-5116	Service Providers, Network Operators, 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.		Changed
7-7-5117	Equipment Suppliers of critical network elements should consider designing electronic hardware to industry requirements (e.g. NEBS) to minimize susceptibility to electromagnetic energy, shock, vibration, voltage spikes, and temperature.		Changed
7-7-5118	Equipment Suppliers of critical network elements should test electronic hardware to ensure its compliance with design criteria for tolerance to electromagnetic energy, shock, vibration, voltage spikes, and temperature.		Changed
7-6-5119	Equipment Suppliers of critical network elements should document the technical specifications of their electronic hardware, including characteristics such as tolerance limitations to electromagnetic energy, vibration, voltage spikes and temperature. Access to such documentation should be restricted to those having a need to know.		Unchanged
7-7-5120	Service Providers, Network Operators, 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.	Companies should weigh the marketing benefits of external signage versus identifying potential targets. For example, some believe posting restricted access signs in internal areas deters inadvertent access. Others believe restricted access signs identify potential targets.	Changed
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.		Changed
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.		Changed
6-6-5124	Recommend deletion. Superseded by BP 5123.		Deleted
6-6-5125	Recommend deletion. Superseded by BP 1009, 1023, 1010.		Deleted

7-7-5126	Service Providers, Network Operators 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).		Changed
7-7-5127	Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should provide a GETS (Government Emergency Telecommunications Service) card to essential staff critical to disaster recovery efforts and should consider utilizing Wireless Priority Service (WPS) for essential staff. Appropriate training and testing in the use of GETS & WPS should occur on a regular basis (i.e., in conjunction with testing of the corporate disaster recovery plan).		Changed
7-7-5128	Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should maintain accurate records for GETS (Government Emergency Telecommunications Service) cards and WPS (Wireless Priority Service) phone assignments as staff changes occur.		Changed
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.		Changed
7-7-5130	The government, Service Providers, Network Operators and Equipment Suppliers 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.		Changed
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.		Unchanged
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.		Unchanged
7-6-5133	Network Operators should protect the identity of locations where emergency mobile trailers and equipment are stored.		Unchanged
7-7-5134	Service Providers, Network Operators and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together.		Changed
7-7-5135	Service Providers, Network Operators and Equipment Suppliers should participate in the Network Reliability and Interoperability Council and its focus groups in order to develop industry Best Practices for addressing and mitigating public communications infrastructure vulnerabilities.		Changed
6-6-5137	Recommend deletion. Superseded by BP 5100.		Deleted
7-7-5138	Network Operators should plan for the possibility that impacted network nodes cannot be accessed by company personnel for an extended period of time and define the corporate response for restoration of service.	For example; wide scale destruction, radiological, chemical or biological contamination.	Changed
7-7-5139	Service Providers, Network Operators and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites.		Changed
6-6-5140	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted

7-7-5141	Service Providers, Network Operators and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations.		Changed
7-6-5143	Service Providers and Network Operators (e.g., Satellite Operators) should maintain access to a back-up or secondary 'uplink site' to provide tracking, telemetry and control (T.T.&C.) support for all operational communications spacecraft. The back-up or secondary site must be geographically diverse from the primary uplink facility, active and tested on some regular schedule to insure readiness and timely response.		Unchanged
7-6-5144	Network Operators should manage and maintain a current database of all satellite transmit and receive sites (i.e. uplink and downlink facilities) that are operational and/or support their services and networks. The database information should list location (i.e. street address, latitude and longitude), service provider and phone number, site manager contact and phone number, control point if remotely controlled, and equipment type used at the site.		Unchanged
7-6-5146	Service Providers and Network Operators should develop and manage recovery plans to ensure the timely restoration of services in the event of transponder loss, satellite payload failure, and satellite failure.		Unchanged
6-6-5147	Recommend deletion. Superseded by BP 8066.		Deleted
6-6-5148	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-6-5150	Recommend deletion. Superseded by BP 5151.		Deleted
7-7-5151	Property Managers, Service Providers and Network Operators located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.		Changed
7-6-5152	Service Providers, Network Operators Equipment Suppliers should consider performing targeted sweeps of critical infrastructures and network operations centers for listening devices when suspicion warrants.		Unchanged
7-7-5153	Service Providers, Network Operators 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.		Changed
6-6-5155	Recommend deletion. Superseded by BP 5175, 5070, and 8066.		Deleted
6-6-5157	Recommend deletion. Superseded by BP 5100.		Deleted
7-7-5158	Service Providers, Network Operators and Equipment Suppliers should consider unannounced internal security audits at random intervals to enforce compliance with company security policies.		Changed
6-6-5159	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-5160	Service Providers, Network Operators, Equipment Suppliers and Property Managers should account for the possible absence of critical personnel in their business continuity plan.		Changed

7-7-5163	Service Providers, Network Operators, 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).		Changed
7-7-5164	Service Providers, Network Operators and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company vehicles and trailers to the appropriate authorities.		Changed
7-6-5166	Equipment Suppliers should, wherever feasible, isolate R&D and software manufacturing of Network Elements from general office systems to prevent unauthorized access.		Unchanged
7-6-5167	Service Providers, Network Operators and Equipment Suppliers should provide secured methods, both physical and electronic, for the internal distribution of software development and production materials.		Unchanged
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.		Unchanged
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).		Unchanged
7-6-5171	Equipment Suppliers should design network equipment to reduce the likelihood of malfunction due to failure of the connected devices (i.e. in order to reduce the potential for cascade failures).		Unchanged
7-7-5174	Service Providers, Network Operators, 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.		Changed
7-7-5175	Service Providers, Network Operators 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.		Changed
6-6-5178	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-6-5179	Service Providers, Network Operators and Equipment Suppliers should establish policies and procedures that mitigate workplace violence.		Unchanged
6-6-5180	Recommend deletion. Superseded by BP 5026.		Deleted
6-6-5182	Recommend deletion. Superseded by BP 5026.		Deleted
6-6-5183	Recommend deletion. Superseded by BP 5026.		Deleted
6-6-5184	Recommend deletion. Superseded by BP 5052.		Deleted
7-6-5185	Service Providers, Network Operators, 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/stair re-entries into areas of critical infrastructure, where permitted by code.		Unchanged
6-6-5186	Recommend deletion. Superseded by BP 5238.		Deleted

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.		Changed
7-7-5188	Service Providers and Network Operators 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.		Changed
6-6-5189	Recommend deletion. Superseded by BP 5187, 5188.		Deleted
6-6-5190	Recommend deletion. Superseded by BP 5187.		Deleted
7-7-5191	Service Providers and Network Operators that are tenants within telecom hotels should plan accordingly to protect their own facilities from potential risks within the building complex (e.g., fire suppression system, plumbing, hazardous materials).		Changed
7-7-5192	Service Provider and Network Operator 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).		Changed
6-6-5193	Recommend deletion. Superseded by BP 5192.		Deleted
7-6-5194	Equipment Suppliers should design electronic hardware to minimize susceptibility to electrostatic discharge.		Unchanged
7-6-5195	Equipment Suppliers should keep track of network product identification (e.g., circuit pack serial number), repair, modification and decommissioning records.		Unchanged
7-7-5197	Network Operators, Service Providers, and Property Managers should periodically inspect, or test as appropriate, the grounding systems in critical network facilities.		Changed
7-7-5198	Equipment Suppliers should design their products to take into consideration protection against the effects of corrosion and contamination.		Changed
7-7-5199	Service Providers and Network Operators 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.		Changed
7-6-5200	Service Providers, Network Operators 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.		Unchanged
6-6-5202	Recommend deletion. Superseded by BP 5263.		Deleted
7-7-5203	Network Operators, Service Providers, and Property Managers should develop, maintain and administer a comprehensive program to sustain a reliable power infrastructure.		Changed
7-7-5204	Service Providers, Network Operators and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) 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.		Changed
6-6-5205	Recommend deletion. Superseded by BP 5232.		Deleted

7-7-5206	Service Providers, Network Operators and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load to allow for contracted refueling.		Changed
7-7-5207	Service Providers, Network Operators and Property Managers should take appropriate precautions to ensure that fuel supplies and alternate sources of power are available for critical installations in the event of major disruptions in a geographic area (e.g., hurricane, earthquake, pipeline disruption). Consider contingency contracts in advance with clear terms and conditions (e.g., Delivery time commitments, T&Cs).		Changed
7-7-5208	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that electrical work (e.g., AC and high current DC power distribution) is performed by qualified technicians.		Changed
7-7-5209	Service Providers, Network Operators and Property Managers should restrict access to the AC transfer switch housing area, ensure that scheduled maintenance of the transfer switch is performed, and ensure that spare parts are available.		Changed
7-6-5210	Service Providers, Network Operators and Property Managers should discourage use of Emergency Power Off (EPO) switches between the primary battery supplies and the main power distribution board. EPO switches are not recommended for use in traditional -48V DC battery plants.		Unchanged
7-7-5211	Service Providers, Network Operators and Property Managers should disable power equipment features that allow switching off of power equipment from a remote location (i.e., dial up modem). During severe service conditions, such features may be activated to allow a degree of remote control.		Changed
7-7-5212	Service Providers, Network Operators and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.		Changed
7-7-5213	Service Providers, Network Operators and Property Managers should, where feasible, place fuel tanks in a secured and protected area. Access to fill pipes, fuel lines, vents, manways, etc. should be restricted (e.g., containment by fencing, walls, buildings, buried) to reduce the possibility of unauthorized access.		Changed
7-7-5214	Service Providers, Network Operators and Property Managers should consider placing all power and network equipment in a location to increase reliability in case of disaster (e.g., floods, broken water mains, fuel spillage). In storm surge areas, consider placing all power related equipment above the highest predicted or recorded storm surge levels.		Changed
7-7-5216	Service Providers, Network Operators and Property Managers should consider providing secure pre-constructed exterior wall pathways for mobile generator connections or tap box connections.		Changed
7-7-5217	Service Providers, Network Operators, 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.	For example, shipping and receiving, mailroom, emergency response and security personnel.	Changed

7-7-5218	Equipment Suppliers should implement a comprehensive security program for protecting hardware, firmware and software from malicious code insertion or tampering during development and delivery, taking into consideration that some developmental environments around the world present a higher risk level than others.		Changed
6-6-5219	Recommend deletion. Superseded by BP 5218.		Deleted
7-7-5220	Service Providers, Network Operators and Equipment Suppliers who utilize foreign sites should establish and implement a comprehensive physical security program for protecting corporate assets, including personnel, at those sites.		Changed
7-7-5221	Service Providers, Network Operators and Equipment Suppliers should consider limiting the dissemination of information relating to future locations of key leadership.		Changed
7-7-5222	Service Providers, Network Operators and Equipment Suppliers should consider providing trouble call centers with a physically diverse back-up capability that can quickly be configured to receive the incoming traffic and take appropriate action.		Changed
7-7-5223	Service Providers, Network Operators and Equipment Suppliers should establish a plan for providing technical support that prevents the loss of one facility or location from disabling their ability to provide support.		Changed
6-6-5224	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-5225	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that Business Continuity Plan(s) are restricted to those with a need-to-know.		Changed
7-7-5226	Service Providers, Network Operators and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.		Changed
7-7-5227	Service Providers, Network Operators, Equipment Suppliers and Property Managers should perform after-action reviews of emergency response and restoration of major events to capture lessons learned (e.g., early warning signs) and to enhance emergency response and restoration plans accordingly. A process similar to NRIC VII Appendix Z, “Recovery Incident Response (IR) Post Mortem Checklist” can be used to capture and identify countermeasures to prevent or mitigate the impact of future incidents and to quickly and effectively restore service from such events in the future.	NRIC Appendix Z can be found at: http://www.bell-labs.com/user/krauscher/nric/Cyber%20Security%20Appendices.pdf	Changed
7-6-5228	Service Providers, Network Operators and Equipment Suppliers should consider including cross-subsidiary resource sharing and communications in business continuity plans to support emergency response and restoration.		Unchanged
7-7-5229	Service Providers, Network Operators 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.		Changed
6-6-5230	Recommend deletion. Superseded by BP 5138 and 5198.		Deleted

7-6-5231	Service Providers, Network Operators, Equipment Suppliers and Property Managers should develop documentation for the restoration of power for areas of critical infrastructure including such things as contact information, escalation procedures, restoration steps and alternate means of communication. This documentation should be maintained both on-site and at centralized control centers.		Unchanged
7-7-5232	Service Providers, Network Operators, and Property Managers should test fuel reserves used for standby or backup power for contamination at least once a year or after any event (e.g., earth tremor, flood) that could compromise the integrity of the tank housing, fill pipe or supply pipe.	These tests should include inspection for water, sediment, organic contaminates, and any other items that may inhibit the peak performance of the standby/backup generator.	Changed
7-7-5233	Service Providers, Network Operators and Equipment Suppliers should verify proper functioning of electronic surveillance equipment (e.g., CCTV, access control logs, alarm monitoring) at critical access points after any incident that may impact such equipment.		Changed
7-7-5234	Service Providers, Network Operators 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.		Changed
7-6-5235	Service Providers, Network Operators and Equipment Suppliers should ensure that impacted alarms and monitors associated with critical utility vaults are operational after a disaster event.		Unchanged
7-7-5236	Property Managers should take the lead in restoration efforts of the base building infrastructure from an incident at a multi-tenant facility. Tenants should provide points of contact to the Property Manager to allow for coordination, support and additional resources as necessary.		Changed
7-7-5237	Service Providers, Network Operators and Equipment Suppliers should verify the integrity of system spares and replenish utilized spares, as appropriate, as part of a disaster response at a facility.		Changed
7-7-5238	Service Providers and Network Operators who are tenants in multi-tenant facilities (e.g., telecom hotels) should coordinate security and restoration efforts with the Property Manager.		Changed
7-6-5239	Property Managers for multi-tenant facilities should maintain a crisis management plan for restoration following an incident.		Unchanged
7-7-5240	Service Providers, Network Operators, Equipment Suppliers and Property Managers should have a provision for responding to malfunctioning access control equipment.		Changed
7-7-5241	Service Providers, Network Operators and Equipment Suppliers should consider placing access and facility alarm points to critical or sensitive areas on backup power.		Changed
7-7-5242	Service Providers, Network Operators and Equipment Suppliers should reassess the criticality of associated facilities following a catastrophic incident (i.e., loss of one facility may make others more critical).		Changed
7-6-5243	Service Providers, Network Operators and Equipment Suppliers should restrict visits and tours at the affected areas during the restoration period following a major incident.		Unchanged
7-6-5244	Service Providers, Network Operators and Equipment Suppliers should make all employees, contractors, and others with access to critical infrastructure during restoration aware of changes to security posture resulting from the incident, and increased vigilance should be encouraged.		Unchanged
7-7-5245	Service Providers, Network Operators and Equipment Suppliers should document the use of non-standard equipment during restoration to review and/or replace those devices as appropriate.		Changed

6-6-5246	Recommend deletion. Superseded by BP 5234.		Deleted
7-7-5247	Service Providers, Network Operators, Equipment Suppliers and Property Managers should take into account failed security systems after an event when determining restoration priorities.		Changed
7-6-5248	Service Providers, Network Operators and Equipment Suppliers should perform a risk assessment on significant network changes resulting from restoration efforts.		Unchanged
7-6-5249	Network Operators should consider geographic separation of network redundancy during restoration, and address losses of redundancy and geographic separation following restoration.		Unchanged
7-6-5250	Network Operators should consider intra-office diversity of all critical resources during restoration, and address losses of diversity following restoration.		Unchanged
6-6-5251	Recommend deletion. Superseded by BP 5078.		Deleted
7-7-5252	Network Operators should evaluate the priority on re-establishing diversity of facility entry points (e.g., copper or fiber conduit, network interfaces for entrance facilities) during the restoration process.		Changed
7-6-5253	Service Providers, Network Operators and Equipment Suppliers should use lessons learned from restoration efforts to update recovery plans for transponder loss, satellite payload failure, and satellite failure.		Unchanged
7-7-5256	Service Providers, Network Operators and Equipment Suppliers should monitor temporary connections of network test equipment that are established for restoration to prevent access by unauthorized personnel.		Changed
6-6-5257	Recommend deletion. Superseded by BP 5258.		Deleted
7-7-5258	Service Providers, Network Operators and Equipment Suppliers should define and assign responsibility for retrieval of all corporate assets (e.g., access cards, equipment) and ensure temporary physical and logical access is removed after completion of a restoration effort for all temporary personnel associated with the restoration.		Changed
7-7-5259	Service Providers, Network Operators, Equipment Suppliers and Property Managers should establish and enforce access control and identification procedures for all individuals (including temporary contractors, and mutual aid workers) at restoration sites for which they have responsibility. Provide for issuing and proper displaying of ID badges, and the sign-in and escorting procedures, where appropriate.		Changed
7-7-5260	Service Providers, Network Operators, Equipment Suppliers and Property Managers should brief affected personnel involved in a restoration on any significant changes to access control procedures.		Changed
7-7-5261	Network Operators, Service Providers and Property Managers should identify carrier interconnection points and coordinate restoral plans, as appropriate.		Changed
7-7-5262	Service Providers, Network Operators, Equipment Suppliers should evaluate the vulnerability of storage locations in an effort to protect critical spares.		Changed
7-7-5263	Service Providers, Network Operators and Equipment Suppliers should use cables with adequate reliability and cable signal integrity. Such properties as flammability, strain reliefs and signal loss should be considered. If non-standard cables are used because of an emergency restoration, they should be marked as temporary and should be replaced with standard cables as soon as practical.		Changed

7-6-5265	Service Provider, Network Operator, Equipment Supplier and Property Manager senior management should encourage and establish a corporate culture that promotes corporate security policies and procedures.		Unchanged
6-6-5266	Recommend deletion. Superseded by BP 5270.		Deleted
7-7-5267	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that operating procedures are clearly defined, and followed by personnel during emergency situations in order to avoid degradation of cyber and physical security due to a diversion.		Changed
6-6-5268	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-5269	Service Providers, Network Operators, Equipment Suppliers and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.		Changed
7-7-5270	Service Providers, Network Operators, Equipment Suppliers and Property Managers personnel should be aware that terrorists or malicious groups may use false information to cause heightened public or employee awareness to divert attention and resources to other areas away from their intended physical or cyber target. Where feasible, information (e.g., news sources, e-mail) should be authenticated and cross-verified to ensure accuracy of information.		Changed
7-7-5271	Service Providers and Network Operators should consider physical and cyber security issues in Mutual Aid Agreements (e.g., authorization, access control, badging).	Local exchange carrier Mutual Aid agreement can be found on the National Coordinating Center for Telecommunications web page at http://www.ncs.gov/ncc/.	Changed
7-7-5272	Service Providers, Network Operators and Equipment Suppliers should include security considerations in disaster recovery plans for critical infrastructure sites.		Changed
6-6-5273	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-6-5274	Service Providers, Network Operators, 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.		Unchanged
7-7-5275	Service Providers, Network Operators and Equipment Suppliers should consider backup power capabilities for Command and Control (Crisis Teams) so that communications and access to critical systems can be maintained in the event of a significant disruption to commercial power.	This could include, but is not limited to, moving crisis team personnel to locations where there exists long-term power backup, installing generator backup at certain critical sites, etc.	Changed
7-7-5276	Service Providers, Network Operators and Equipment Suppliers that use networked electronic access control systems should apply appropriate security and reliability principles for critical systems (e.g., cyber security).		Changed
7-7-5277	Service Providers, Network Operators 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.		Changed
6-6-5278	Recommend deletion. Superseded by BP 5277.		Deleted

7-7-5279	Service Providers, Network Operators and Equipment Suppliers should consider site specific (e.g., location, region, country) threat information during security program development.		Changed
7-7-5280	Service Providers, Network Operators and Equipment Suppliers should instruct security personnel to confirm the authenticity of directions to supersede existing security processes or procedures.		Changed
7-7-0501	Network Operators and Service Providers should report problems discovered from their operation of network equipment to the Equipment Supplier whose equipment was found to be the cause of problem.		Changed
6-5-0502	Recommend deletion. Superseded by BP 5135.		Deleted
6-5-0503	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0504	Network Operators and Service Providers, in order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, should consider maintaining "hot spares" (circuit packs electronically plugged in and interfacing with any element management system, as opposed to being stored in a cabinet) for mission critical elements.	To determine appropriateness of this Best Practice, certain factors should be considered, including redundancy, single points of failures for critical subscribers, etc.	Changed
7-7-0505	Network Operators and Service Providers should have procedures in place to process court orders and subpoenas for wire taps or other information.		Changed
6-5-0509	Recommend deletion. Superseded by BP 0530, 0599, 1064, 5135, 1004, 1009.		Deleted
7-5-0511	Service Providers and Network Operators should provide training for their operations personnel on network-level trouble shooting.		Unchanged
7-5-0514	When available, Network Operators and Service Providers should utilize a management system capability (e.g., CORBA, SNMP) providing a single interface with access to alarms and monitoring information from all critical network elements.		Unchanged
7-7-0520	Network Operators and Service Providers should have a route policy that is available, as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting.		Changed
7-7-0521	Equipment Suppliers, Network Operators, and Service Providers should work toward implementing industry standards for interconnection points.	For example, IETF standards and applicable ANSI T-1 Standards.	Changed
6-5-0525	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-5-0527	Recommend deletion. Superseded by BP 5064.		Deleted
6-5-0528	Recommend deletion. Superseded by BP 0548.		Deleted
7-7-0529	Service Providers, Network Operators and Equipment Suppliers should support sharing of appropriate information pertaining to outages as an effort to decrease the potential of further propagation (e.g., ATIS NIIF reference document).	The NIIF documents are available at http://www.atis.org.. Industry guidelines for the sharing of information about network outages is included in the NIIF Reference Document Part VII.	Changed
7-7-0530	Service Providers, Network Operators, and Equipment Suppliers should participate in interoperability testing (including services), as appropriate, to maintain reliability across connected networks.		Changed
7-5-0531	Service Providers and Network Operators should require staff to use grounding straps when working with equipment where appropriate.		Unchanged

7-7-0532	Network Operators should periodically audit for physical and logical diversity called for by network design and take appropriate measures as needed.		Changed
6-5-0534	Recommend deletion. Superseded by BP 5130, 5174, 0599, 5135.		Deleted
6-5-0535	Recommend deletion. Superseded by 5130, 5135, 5129.		Deleted
7-5-0538	Equipment Suppliers' network element (including OSS) software should be backward compatible.		Unchanged
7-7-0539	Equipment Suppliers should share trend information (availability, etc.) with their Network Operators and Service Providers.		Changed
7-5-0540	Equipment Suppliers should share countermeasures resulting from analysis of an outage with Network Operators using the same equipment.		Unchanged
7-7-0541	Equipment Suppliers, Network Operators, and Service Providers should store multiple software versions for critical network elements and be able to fallback to an earlier version.		Changed
7-7-0542	Equipment Supplier processes (e.g., software upgrade) should include prevention and detection of malicious code insertion from Original Equipment Manufacturers (OEMs), contractors, and disgruntled employees.		Changed
7-7-0543	Service Providers should establish agreements with property managers for both regular and emergency power.		Changed
6-5-0544	Recommend deletion. Superseded by 5214.		Deleted
6-5-0545	Recommend deletion. Superseded by 0584.		Deleted
7-7-0546	Network Operators and Service Providers should minimize single points of failure in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).		Changed
7-7-0547	Network Operators and Service Providers should place critical network databases (e.g., directory server, feature server, Service Control Point (SCP)) in a secure environment across distributed locations to provide service assurance (e.g., maintainability, connectivity, security, reliability) consistent with other critical network elements.		Changed
7-7-0549	Network Operators should develop an engineering design for critical network elements and inter-office facilities that addresses diversity, and utilize management systems to provision, track and maintain that inter-office and intra-office diversity.		Changed
7-5-0550	Equipment Suppliers and Network Operators should ensure synchronization and security of databases. Procedures should also be in place to allow for manual configuration in the event of a failure of automatic synchronization system. It is also recommended that provisioning technicians be restricted from all commands except those that are needed for their work. Avoid any "global" commands or unauthenticated, privileged access that may have the potential for significant impact.		Unchanged
7-7-0552	Equipment Suppliers' software fault insertion testing (including simulating network faults such as massive failures) should be performed as a standard part of an Equipment Supplier's development process.		Changed
7-5-0553	Equipment Suppliers hardware fault insertion testing (including simulating network faults such as massive failures) should be performed as a standard part of an Equipment Supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress fault recovery software.		Unchanged
7-5-0554	Equipment Suppliers hardware and software fault recovery design processes should converge early in the development cycle.		Unchanged

7-7-0557	Equipment Suppliers should make efforts to minimize the possibility of having a silent failure on any system component, especially critical components. Equipment Suppliers should also constantly review the level of inspection and surveillance on critical components so silent failures are not able to manifest throughout the life of the product.		Changed
6-5-0559	Recommend deletion. Superseded by 0600.		Deleted
6-5-0560	Recommend deletion. Superseded by 0600.		Deleted
7-7-0561	Equipment Providers should provide timely documentation that is complete and easy-to-use. The availability of electronic media to customers for documentation is essential.	The operations and maintenance manual should give an overview of the system and identify procedures for regularly scheduled operations, including security administration (ref. GR-815, GR-1332) and should cover methods to recover from total and partial network element outages. In addition, the documentation should be clear on how to manage emergency and unforeseen situations, and include a technical support escalation process.	Changed
7-5-0562	Equipment Suppliers should use a change control and release planning process to keep track of the changes to the product and the corresponding documentation.		Unchanged
6-5-0563	Recommend deletion. Superseded by 0590		Deleted
7-7-0564	Equipment Suppliers should develop and update training for their products with a clear understanding of customer needs and human factors.	Advanced training should be developed for personnel responsible for the technical support of various products, including operations supervisors, maintenance engineers, operational support personnel, communications technicians, and security administrators. Training should cover local and remote operations.	Changed
7-7-0565	Equipment Suppliers should establish and use metrics to identify key areas and measure progress in improving quality, reliability and security during product development and field life cycle.	This can be done as follows: request and use customer feedback, jointly perform detailed Root Cause Analysis for reported hardware failures, software faults and procedural errors, working together to establish reliability and performance field objectives. Based on these, suppliers and Network Operators and Service Providers should identify, plan, and implement improvements in the development process as well as processes associated with documentation and training.	Changed
7-7-0583	Network Operators, Service Providers and Equipment Suppliers should adopt an industry uniform method of reporting and tracking significant service outages (e.g., TL-9000 standard outage template).	For example: www.questforum.org/resources/public_pres/2004_BPC/S12-c_McCain.pdf,	Changed
7-7-0584	Service Providers, Network Operators and Equipment Suppliers and Government representatives [of the National Security Emergency Preparedness (NS/EP) community] should work together to support appropriate industry and international organizations to develop and implement NS/EP standards in packet networks.		Changed
7-7-0587	Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should avail themselves of the Telecommunications Service Priority (TSP) program and support / promote as applicable.	The TSP Program is a FCC program used to identify and prioritize telecommunication services that support NSEP missions. The TSP Program also provides a legal means for the telecommunications industry to provide preferential treatment to services enrolled in the program. More information on the TSP Program can be obtained from the National Communications System (NCOS) Office of Priority Telecommunications, Manager National Communications System, Attn: OPT/N3, 701 South Courthouse Road, Arlington, Virginia 22204-2198, on telephone 703-607-4932 or email at TSP@NCS.GOV.	Changed

7-7-0588	Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements.	A successful program should educate its target audience on the technology, its benefits and risks, and the magnitude of traffic carried. The training might include the functionality and the network impact of failure of active and standby (protect) equipment in processors, interfaces, peripheral power supplies, and other related components, and the identification of active and standby (protect) units. Special emphasis should focus on the systematic processes for trouble isolation and repair.	Changed
7-7-0589	Network Operators, Service Providers, and Equipment Suppliers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on production network elements, especially when new technology is introduced in the network.	This training should stress a positive reinforcement of procedures at all times. This training should also emphasize the steps required to successfully detect problems and to isolate the problem systematically and quickly without causing further system degradation. Lack of troubleshooting experience and proper training in trouble detection and isolation usually prolongs the trouble detection and isolation process. Special emphasis should be placed on maintaining and troubleshooting problems related to system power equipment which can add significant delay to restoration activities.	Changed
7-7-0590	Equipment Suppliers, Network Operators, and Service Providers should prepare Methods of procedure (MOPs) for core infrastructure hardware and software growth and change activities as appropriate.	As far as practicable, the MOP should be prepared by the people who are subject matter experts. The MOP should be approved by the managers responsible for engineering, line operations, installation, and other functions, as appropriate; and deviations from the documented process should also be approved by this team. When it is necessary to reference other documents in the MOP, these references should be detailed and include appropriate issue/date information. The MOP should identify each step required to perform the work. As each work function is completed, it should be signed off in the MOP.	Changed
6-5-0591	Recommend deletion. Superseded by 0529		Deleted
7-7-0592	Network Operators and Service Providers should provide duplicated, non-co-located maintenance administration, surveillance and support for network elements. Monitoring and administration locations should be minimized to provide consistency of operations and overall management.		Changed
6-5-0593	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0594	Maintaining SS7 Link Diversity - Network Operators and Service Providers should follow industry guidelines for validating SS7 link diversity. SS7 link diversification validation should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity.	Must have password to access the page. Then pick the document. "ATIS-0300018 NIIF 5013 NIIF Reference Document Part III- Attachment G- SS7 Link Diversity Validation Guidelines - Version 7.1" http://www.atis.org/niif/_com/passwordprotectdocs.asp	Changed
7-7-0596	Network Operators and Service Providers should carefully review all re-home procedures, undertake meticulous pre-planning before execution, and ensure that re-home procedures are carefully followed.	http://www.atis.org/niif/_com/passwordprotectdocs.asp	Changed
7-7-0597	Network Operator and Service Provider network technicians should be trained in (1) detection of conditions requiring intervention, (2) escalation procedures, and (3) manual recovery techniques.		Changed

6-5-0598	Recommend deletion. Superseded by 5239, 1001, 1002, 1004, 1006, 1009, 1010, 1016.		Deleted
7-7-0602	Network Operators and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).	The volume of alarms during provisioning creates a potential for alarm saturation and makes it very difficult to differentiate between a real alarm and those caused by other activities. A common practice is to simply inhibit these alarms or set their thresholds so high they do not report. The danger here is that there must be a fail-safe measure to turn these alarms back on when the facility is carrying traffic.	Changed
7-7-0604	Network Operators and Service Providers should establish synchronization coordinator(s) who has responsibility for the network synchronization. The synchronization coordinator(s) should be accessible to their Network Operations Centers.	The Network Operators and Service Providers may wish to publish their contact information in the forums in which they participate. The forums may include organizations and groups promoting inter-operability, operations, reliability and service restoration such as NRIC, ATIS, NCS, etc.. Network Operators and Service Providers may want to consider implementing a mailbox (e.g., sync@<serviceprovider>.tld).	Changed
7-7-0605	Network Operators and Service Providers should assess the synchronization needs of the network elements and interfaces that comprise their networks to develop and maintain a detailed synchronization plan.	The synchronization plan should include interfaces, customers (both retail and wholesale) and network peers. The plan should encompass all services provided by and used by the Network Operators and Service Providers. The plan should include: synchronization hierarchy, failure avoidance, redundancy and backup for resilience, FMECA and SPOFA. Synchronization performance expectations (24hr slip rate) should be determined in both primary and backup operation scenarios. Timing loop analysis must be performed in the primary arrangement and in all potential failure scenarios.	Changed
6-5-0606	Recommend deletion. Superseded by 0607.		Deleted
7-7-0608	Service Providers and Network Operators should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks. Interconnecting companies should address the control of overflow conditions in their bilateral agreements.		Changed
7-7-0609	Service Providers and Network Operators should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes.	See BP 1031 for additional mutual aid information.	Changed
6-5-0610	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0611	Equipment Suppliers should provide secure electronic distribution of documentation and software, where feasible.	Electronic access to documentation will allow better version control and ease of access for field personnel. Additionally, electronic access allows implementation and delivery of future enhancements such as interactive methods and information. Local back-up copies should be readily available.	Changed
7-7-0612	Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.		Changed
6-5-0613	Recommend deletion. Superseded by 5076, 5080, 5083.		Deleted
7-5-0615	Network Operators and Service Providers should test complex configuration changes before and after the change to ensure the appropriate and expected results		Unchanged
7-5-0618	Network Operators and Service Providers should establish mutually agreed upon reliability thresholds with Equipment Suppliers for new hardware (e.g., routers, switches, call servers, signaling servers) brought into service on the network.		Unchanged

7-5-0620	Equipment Supplier's should endeavor to meet requirements outlined in the GR-63 01 Network Equipment-Building System (NEBS) Requirements for Power and Communication Cables (e.g., power, fire, temperature, humidity, vibration).		Unchanged
7-7-0621	Network Operators and Service Providers should consider abandoning and / or removing existing cable that does not meet NEBS standards, if it is economically feasible and safe to do so.		Changed
7-5-0622	Network Operators, Service Providers, and Property Managers should use ANSI T1.311-1998 "Standard for Telecommunications Environmental Protection, DC Power Systems" for key equipment locations (e.g., routers, central office switches, and other critical network elements) to reduce fires associated with DC power equipment.		Unchanged
7-7-0623	Network Operators and Service Providers using Valve Regulated Lead Acid (VRLA) batteries should perform annual maintenance by performing a discharge test or by using an ohmic test instrument.	The aging properties of these batteries can lead to thermal runaway that may cause a fire. See SR-NWT-001307	Changed
7-5-0624	Network Operators, Service Providers, and Property Managers are encouraged to establish case history files, by equipment category for rectifiers, to facilitate decisions to replace such equipment with more efficient equipment based on failure trends.		Unchanged
7-5-0625	Network Operators, Service Providers, Property Managers, and Equipment Suppliers should consider placing electric utility transformers external to buildings.		Unchanged
7-5-0626	Network Operators, Service Providers, and Property Managers should regularly inspect building mechanical equipment (e.g., air handling fans, air compressors, pumps).		Unchanged
7-7-0627	Network Operators, Service Providers, and Property Managers should exercise, service, and calibrate AC circuit breakers per manufacturers' recommendations.		Changed
7-5-0628	Network Operators and Service Providers should develop and implement defined procedures for removal of unused equipment and cable (e.g., cable mining) if this work can be economically justified without disrupting existing service.		Unchanged
7-7-0629	Network Operators, Service Providers and Property Managers should implement a training program for contractors working in critical equipment locations to ensure they understand the need for protecting the continuity of service and all fire safety requirements applicable to the facility.		Changed
7-5-0630	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop and execute standard Method of Procedure (MOP) for all vendor work in or external to equipment locations with emphasis on service continuity and safety precautions.		Unchanged
7-5-0631	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should develop a comprehensive Site Management and/or Building Certification Program to ensure that every critical equipment location has carefully documented procedures to ensure fire safety. These procedures should include, among other things, guidance for the safe operation of all electrical appliances at this facility, including space heaters which are a frequent source of fires.		Unchanged
7-7-0632	Network Operators and Service Providers that use soldering irons in the provision or maintenance of service should periodically review the work processes and safety precautions applicable to safe operations of these work tools.		Changed
7-7-0633	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should prohibit smoking in buildings.		Changed

7-7-0634	Network Operators, Service Providers and Property Managers together with the Power Company and other tenants in the location, should verify that aerial power lines are not in conflict with hazards that could produce a loss of service during high winds or icy conditions.		Changed
7-7-0635	Network Operators, Service Providers, and Property Managers should ensure that AC surge protection is provided at the power service entrance to minimize the effects caused by lightning or extremely high voltages.	TR-NWT-001011 "Generic Requirements for Surge Protection Devices"	Changed
6-5-0636	Recommend deletion. Superseded by 5197.		Deleted
6-5-0637	Recommend deletion. Superseded by 0602, 0612, 0692, 0761, 5002, 5078, 5235.		Deleted
6-5-0638	Recommend deletion. Superseded by 5044.		Deleted
6-5-0639	Recommend deletion. Superseded by 5099.		Deleted
7-5-0640	Network Operators, Service Providers, and Property Managers should ensure proper air filtration.		Unchanged
6-5-0641	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-5-0642	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-5-0644	Network Operators, Service Providers, and Property Managers should use over-current protection devices and fusing.		Unchanged
6-5-0647	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-5-0648	Network Operators, Service Providers and Property Managers should ensure certified inspection of boilers & fuel storage units.		Unchanged
7-7-0649	Service Providers, Network Operators, and Property Managers should ensure critical network facilities have appropriate fire detection and alarm systems.		Changed
7-7-0650	Network Operators, Service Providers, and Property Managers should place strong emphasis on human activities related to the operation of power systems (e.g., maintenance procedures, alarm system operation, response procedures, and training) for operations personnel.		Changed
7-7-0651	Network Operators, Service Providers, and Property Managers should consider providing diversity within power supply and distribution systems so that single point failures are not catastrophic. For large battery plants in critical offices, consider providing dual AC feeds (odd/even power service cabinets for rectifiers). Transfer switches should be listed to a UL standard for Transfer Switch Equipment. When transfer breaker systems are used, they must be mechanically and electrically interlocked.		Changed

7-7-0652	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should adhere to the following applicable power engineering design standards; Telcordia GR-513-CORE (Power - LSSGR section 13), Telcordia GR-63-CORE (NEBS), Telcordia GR-295-CORE (Isolated Ground Planes), Telcordia GR-1089-CORE (Electromagnetic Compatibility), and ANSI T1.311 (DC power Systems).		Changed
7-5-0653	Network Operators, Service Providers, and Property Managers should retain complete authority about when to transfer from the electric utility and operate standby generators.		Unchanged
7-5-0654	Network Operators, Service Providers and Property Managers should not normally enter into power curtailment or load sharing contracts with electric utilities.		Unchanged
7-5-0656	Network Operators and Service Providers should establish a general requirement for power conditioning, monitoring and protection for sensitive equipment.		Unchanged
7-5-0657	Network Operators, Service Providers, and Property Managers should design standby generator systems for fully automatic operation and for ease of manual operation, when required.		Unchanged
7-7-0658	Network Operators, Service Providers, and Property Managers should maintain adequate fuel on-site and have a well-defined re-supply plan. Generator life support systems (e.g., radiator fan, oil cooler fan, water transfer pumps, fuel pumps, engine start battery chargers) should be on the essential AC bus of the generator they serve.		Changed
6-5-0659	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-5-0660	Network Operators, Service Providers, and Property Managers should have a plan that is periodically verified for providing portable generators to offices with and without stationary engines.		Unchanged
6-5-0661	Recommend deletion. Superseded by 0662 and NEW3.		Deleted
7-7-0662	Network Operators, Service Providers, and Property Managers should exercise power generators on a routine schedule in accordance with manufacturer's specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run.		Changed
7-5-0663	Network Operators, Service Providers, and Property Managers should coordinate scheduled power generator tests with all building occupants to avoid interruptions.		Unchanged
7-5-0664	Equipment Suppliers, Network Operators, and Service Providers should provide indicating type control fuses on the front of the power panels, including smaller distribution panels.		Unchanged
7-7-0665	Network Operators, Service Providers, and Property Managers should provide and maintain accurate single line drawings of AC switch equipment on-site.		Changed
6-5-0666	Recommend deletion. Superseded by 0665 .		Deleted
7-7-0667	Network Operators, Service Providers, Property Managers should keep circuit breaker racking/ratchet tools, spare fuses, fuse pullers, etc. readily available.		Changed
7-5-0668	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should clearly label the equipment served by each circuit breaker and fuse.		Unchanged

7-5-0669	Network Operators, Service Providers, and Property Managers should develop and/or provide appropriate emergency procedures for AC transfer.		Unchanged
6-5-0670	Recommend deletion. Superseded by 0635.		Deleted
7-5-0671	Network Operators, Service Providers, and Property Managers should design and implement a preventive maintenance and inspection program for electrical systems.		Unchanged
7-5-0672	Network Operators and Service Providers should provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.		Unchanged
7-5-0673	Network Operators and Service Providers should provide temperature compensation on the rectifiers (or some method to detect/prevent thermal runaway), when valve regulated batteries are used.		Unchanged
7-5-0674	Network Operators, Service Providers, and Property Managers should initiate or continue a modernization program to ensure that outdated power equipment is phased out of plant. They should consider the capabilities of smart controllers, local and remote monitoring, and alarm systems when updating their power equipment. Power monitors and smart controllers should be integrated into engineering and operational strategies.		Unchanged
7-5-0675	Network Operators, Service Providers and Property Managers should, for new installations, consider using multiple small battery plants in place of single very large plants, and consider using multiple battery strings in each plant.		Unchanged
7-7-0676	Network Operators and Service Providers should not use low voltage disconnects or battery disconnects at central office battery plants.		Changed
7-5-0677	Network Operators, Service Providers and Property Managers should only use rectifier sequence controllers where necessary to limit load on the backup power generator.		Unchanged
6-5-0678	Recommend deletion. Superseded by 5061.		Deleted
7-7-0679	Network Operators, Service Providers, and Equipment Suppliers should provide diverse power feeds for all redundant links (e.g., SS7, BITS clocks) and any components identified as "critical" single points of failure in transport and operations of the network.		Changed
7-7-0680	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should provide protective covers on vulnerable circuit breakers which power critical equipment.		Changed
7-5-0681	Network Operators, Equipment Suppliers, and Property Managers should ensure that fuses and breakers meet quality Level III reliability per Technical Reference (SR-332), "Reliability Prediction Procedure for Electronic Equipment".		Unchanged
7-5-0682	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should ensure that power wire, cable, and signaling cables used in communications locations meet NEBS.		Unchanged
7-5-0683	Network Operators, Service Providers and Equipment Suppliers should not mix DC power cables, AC power cables and telecommunications cables wherever possible.		Unchanged
7-7-0684	Network Operators, Service Providers, and Property Managers should verify DC fusing levels throughout the power supply and distribution system, especially at the main primary distribution board, to ensure that fuses and breakers are not loaded at more than 80% of their rated ampacity. Diode OR'ed arrangements require additional special overcurrent protection considerations. In addition, protector size should never exceed cable ampacity.		Changed

7-7-0685	Network Operators should have detailed methods and procedures to identify protection required around energized DC buses.		Changed
7-7-0686	Equipment Suppliers, Network Operators and Service Providers should verify front and rear stenciling on equipment during installation for accurate identification.		Changed
6-5-0687	Recommend deletion. Superseded by 0628, 0694.		Deleted
6-5-0688	Recommend deletion. Superseded by 0602, 0612, 0692, 0761, 5002, 5078, 5235.		Deleted
7-7-0689	Network Operators and Service Providers should provide a separate "battery discharge" alarm for all critical infrastructure facilities, and where feasible, periodically (e.g., every 15 minutes) repeat the alarm as long as the condition exists.		Changed
7-7-0690	Network Operators and Property Managers should consider providing power alarm redundancy so that no single point alarm system failure will lead to a network power outage.		Changed
6-5-0691	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0692	Network Operators, Service Providers, and Equipment Suppliers should consider using fail-safe, normally closed contacts that open for an alarm, for critical alarms produced by single contacts (one on one).		Changed
7-5-0693	Network Operators, Service Providers and Property Managers should emphasize the use of Methods Of Procedures (MOPs), vendor monitoring, and performing work on in-service equipment during low traffic periods.		Unchanged
7-5-0694	Network Operators and Service Providers should check for current flow in cables with AC/DC clamp-on ammeters before removing the associated fuses or opening the circuits during removal projects.		Unchanged
7-7-0695	Network Operators, Service Providers, and Property Managers should develop and test plans to address situations where normal power backup does not work (e.g., commercial AC power fails, the standby generator fails to start, automatic transfer switch fails).		Changed
7-7-0696	Network Operators, Service Providers, and Property Managers should use infrared thermography to check power connections and cabling in central offices when trouble shooting, during installation test and acceptance, and every 5 years.		Changed
7-7-0697	Network Operators, Service Providers, and Equipment Suppliers should employ an "Ask Yourself" program as part of core training and daily operations. This initiative is intended to reinforce the responsibility every employee has to ensure flawless network service. (See General Comments for additional details)	Employees should stop and resolve problems when they can't answer yes to any of the following questions: Do I know why I'm doing this work? Have I identified and notified everybody who will be directly affected by this work? Can I prevent or control a service interruption? Is this the right time to do this work? Am I trained and qualified to do this work? Are work orders, MOPs, and supporting documentation current and error-free? Do I have everything I need to quickly restore service if something goes wrong? Have I walked through the procedure?	Changed
6-5-0698	Recommend deletion. Superseded by 1067.		Deleted
7-7-0699	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should design standby systems to withstand harsh environmental conditions.		Changed
7-5-0700	Network Operators, Service Providers and Equipment Suppliers should consider the need for power expertise/power teams.		Unchanged

7-7-0701	Network Operators, Service Providers, and Property Managers should provide security for portable generators.		Changed
7-5-0702	Network Operators and Service Providers should minimize dependence on equipment requiring AC power feeds in favor of DC-powered components.		Unchanged
7-7-0703	Service Providers, Network Operators and Property Managers should secure remote power maintenance systems to prevent unauthorized use.		Changed
6-5-0704	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0705	Network Operators should use warning tape on buried facilities - place tape 12 in. above the cable system.		Changed
7-7-0706	Network Operators should use visible cable markings on buried facilities (unless prone to vandalism).		Changed
7-7-0707	Network Operators should ensure timely response once received from the One Call Center for all locate requests.		Changed
7-7-0708	Network Operators should use appropriate technologies for locating buried facilities and consider upgrading as technologies evolve.		Changed
7-7-0709	Network Operators should compare outside plant drawings relative to marking cable route maps when locating buried facilities and resolve any discrepancies.		Changed
7-7-0710	Network Operators should use 'dig carefully' concepts and utilize guidance from industry sources for the protection of underground facilities when excavation is to take place within the specified tolerance zone. (See "General" field for additional information)	Industry source example is the Common Ground Alliance. (www.commongroundalliance.com). Methods to consider, based on certain climate and geographical conditions include: hand-digging when practical (potholing), soft digging, vacuum excavation methods, pneumatic hand tools, other mechanical methods with the approval of the facility owner/operator, or other technical methods that may be developed and assign trained technical personnel to monitor activities at work sites where digging is underway.	Changed
6-5-0711	Recommend deletion. Superseded by 0710.		Deleted
6-5-0712	Recommend deletion. Superseded by 5067, 5115, 5244, 0629, 5096, 5116, 5296.		Deleted
6-5-0713	Recommend deletion. Superseded by 0697, 5096, 0589, 0629, 0588, 0650, 0511.		Deleted
6-5-0714	Recommend deletion. Superseded by 0697, 5096, 0589, 0629, 0588, 0650, 0511.		Deleted
7-7-0715	Network Operators should proactively communicate with land owners regarding rights-of-way or easements near critical buried facilities to prevent accidental service interruption.		Changed
7-7-0716	Network Operators should encourage employees to become proactive in preventing buried facilities damages.		Changed
6-5-0717	Recommend deletion. Superseded by 0709.		Deleted
6-5-0718	Recommend deletion. Superseded by 5026.		Deleted
7-7-0719	Network Operators should use 'dig carefully' concepts and utilize guidance from industry sources when installing underground facilities.	Industry source example is the Common Ground Alliance. (www.commongroundalliance.com). Methods to consider, based on certain climate and geographical conditions include: hand-digging when practical (potholing), soft digging, vacuum excavation methods, pneumatic hand tools, other mechanical methods with the approval of the facility owner/operator, or other technical methods that may be developed and assign trained technical personnel to monitor activities at work sites where digging is underway.	Changed

6-5-0720	Recommend deletion. Superseded by 0719.		Deleted
6-5-0721	Recommend deletion. Superseded by 0722.		Deleted
7-7-0722	Service Providers, Network Operators, and Property Managers should consider pest control measures to protect cables where appropriate.	Cables can be protected using armored cable or type "C" conduit in pest-infested areas.	Changed
6-5-0723	Recommend deletion. Superseded by 5011, 5046.		Deleted
6-5-0724	Recommend deletion. Superseded by 0725		Deleted
7-7-0725	Network Operators and Government should increase stakeholder coordination and cooperation to improve the effectiveness of state one-call legislation efforts.		Changed
7-7-0726	Network Operators should consider partnering with excavators, locators, and municipalities in a cable damage prevention program.		Changed
6-5-0727	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0728	Network Operators should use industry standard markings for outside plant cables.		Changed
7-7-0729	Network Operators should establish training, qualification and performance standards for internal utility locators and establish performance standards with external utility locators.		Changed
6-5-0730	Recommend deletion. Superseded by 0719.		Deleted
7-7-0731	Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis.		Changed
6-5-0732	Recommend deletion. Superseded by 0725.		Deleted
7-7-0733	Network Operators, when relocating buried facilities in a common right-of-way, should coordinate activities with other right-of-way occupants to minimize the potential for damage.		Changed
6-5-0734	Recommend deletion. Superseded by 0740.		Deleted
7-7-0735	Network Operators should evaluate the performance of their contracted excavators and internal excavators to foster improved network reliability.		Changed
7-5-0736	Network Operators should develop and implement a rapid restoration program for cables and facilities.		Unchanged
6-5-0737	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-5-0738	Network Operators and Service Providers should track and analyze facility outages taking action if any substantial negative trend arises or persists.		Unchanged
6-5-0739	Recommend deletion. Superseded by 0710, 0719.		Deleted
7-7-0740	Network Operators should implement internal processes needed to support the One-Call Notification legislation.		Changed
7-7-0741	Service Providers and Network Operators should review, and adopt as appropriate, best practices aimed at reducing damage to underground facilities that are maintained by the Common Ground Alliance (www.commongroundalliance.com).	The Common Ground Alliance best practices document provides comprehensive guidance in the areas of Planning & Design, One-Call Centers, Locating & Marking, Excavation, Mapping, Compliance, Public Education, Reporting & Evaluation, and Homeland Security. Many of the best practice are applicable to the activities of Service Providers and Network Operators.	Changed
6-5-0742	Recommend deletion. Superseded by 0741.		Deleted

6-5-0743	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-0744	Equipment Suppliers should periodically review the results of root cause analysis to ensure that the least impacting methods for fault recovery are being used.		Changed
7-7-0745	Equipment Suppliers should design equipment so that changes and upgrades are non-service impacting.		Changed
7-7-0746	Equipment Suppliers should emphasize human factors during design and development to reduce human errors and the impact of these errors. Automated systems should be considered to reduce operating errors.		Changed
7-7-0747	Network Operators, Service Providers and Equipment Suppliers should work together to establish reliability and performance objectives in the field environment.		Changed
7-7-0748	Equipment Suppliers should provide troubleshooting job aids, with updates as appropriate, to assist operations support personnel during fault isolation and recovery.		Changed
7-7-0749	Equipment Suppliers should prevent critical systems from accepting or allowing service affecting activity without appropriate confirmation.		Changed
7-7-0751	Equipment Suppliers should provide clear and specific engineering guidelines, ordering procedures, and installation documentation in support of their products.		Changed
7-7-0752	Service Providers and Network Operators should evaluate support documentation as an integral part of the equipment selection process.		Changed
7-7-0753	Service Providers and Network Operators should be familiar with support documentation provided with the equipment.		Changed
7-7-0754	Network Operators, Service Providers and Property Managers should have documented installation guidelines for equipment deployment in their network or buildings.		Changed
7-7-0755	Network Operators, Service Providers and Property Managers should clearly communicate their installation guidelines (e.g., MOP) to all involved parties.		Changed
7-7-0756	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider including a quality review based on the installation guidelines as part of the on-site installation acceptance.		Changed
7-7-0757	Network Operators, Service Providers and Equipment Suppliers should have procedures for pre-qualification or certification of installation vendors.		Changed
7-7-0512	Service Providers, Network Operators, and Property Managers should perform periodic inspections of fire and water stopping where cable ways pass through floors and walls (e.g., sealing compounds).		Changed
7-7-0513	Service Providers and Network Operators should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration for inter-connected networks. Where appropriate, this information should be shared with Public Safety Service and Support providers.	For example, provider contacts are listed in the NENA company ID registration webiste is http://www.nena.org/companyid/index.htm	Changed
6-6-0586	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted

7-7-0599	Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness through planned drills or simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.	While the staff should be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified. Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service. It is particularly important to coordinate disaster exercises with other Service Providers, Public Safety Providers and vendors. It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.	Changed
7-7-0619	Service Providers, Network Operators, Property Managers and Public Safety Providers should coordinate with fire agencies in emergency response preplanning efforts for communications equipment locations.		Changed
7-7-0655	Network Operators and Service Providers should coordinate hurricane and other disaster restoration work with electrical and other utilities as appropriate.		Changed
7-7-0759	Network Operators and Service Providers should ensure that engineering, design, and installation processes address how new network elements are integrated into the office and network synchronization plan(s).		Changed
7-7-0760	Network Operators and Service Providers should maintain records that accurately track the diversity of internal wiring for office synchronization, including timing leads and power.		Changed
7-6-0761	Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds and alarms.		Unchanged
7-7-1001	Service Providers, Network Operators, Equipment Suppliers, and Property Managers should formally document their business continuity processes in a business continuity plan covering critical business functions and business partnerships. Key areas for consideration include: Plan Scope, Responsibility, Risk Assessment, Business Impact Analysis, Plan Testing, Training and Plan Maintenance.	Critical business processes and support functions could include IT, sourcing, logistics, network and real estate.	Changed
7-7-1002	Service Providers, Network Operators, and Equipment Suppliers should consider establishing a business continuity executive steering committee (composed of executive managers and business process owners) to ensure executive support and oversight.		Changed
6-6-1003	Recommend deletion. Superseded by 1001.		Deleted
7-6-1004	Network Operators, Service Providers, Equipment Suppliers and Property Managers should review their Business Continuity Plan(s) on an annual basis to ensure that plans are up-to-date, relevant to current objectives of the business and can be executed as written.		Unchanged
7-7-1005	Service Providers, Network Operators, and Equipment Suppliers should perform a Business Impact Analysis (BIA) to assess the impact of the loss of critical operations, support systems and applications.	Related BP is 5072.	Changed
7-6-1006	Service Providers, Network Operators and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.		Unchanged

7-6-1007	Service Providers, Network Operators and Equipment Suppliers should consider establishing a geographically diverse back-up Emergency Operations Center.		Unchanged
7-7-1008	Service Providers, Network Operators, and Equipment Suppliers should use the Incident Command System Standard for incident coordination and control in the emergency operations center and at the incident site.	See National Fire Protection Association (NFPA) Standard 156, and National Incident Management System (NIMS).	Changed
7-7-1009	Service Providers, Network Operators and Equipment Suppliers should regularly conduct exercises that test their Disaster Recovery Plans. Exercise scenarios should include natural and man-made disasters. (e.g., hurricane, flood, nuclear, biological, and chemical)	The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.While the staff must be well prepared, the actual exercise should be conducted unannounced in order to test the responsiveness of the team members and effectiveness of the emergency processes. Also, callout rosters and emergency phone lists should be verified. Early in the exercise, make sure everyone understands that this is a disaster simulation, not the real thing! This will avoid unnecessary confusion and misunderstandings that could adversely affect service.It is particularly important to coordinate disaster exercises with other Service Provider, Public Safety Providers and vendors.It is very important immediately following the drill to critique the entire procedure and identify "lessons learned". These should be documented and shared with the entire team.	Changed
7-7-1010	Service Providers, Network Operators and Equipment Suppliers should designate personnel responsible for maintaining Business Continuity and Disaster Recovery Plans.		Changed
7-7-1011	Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should establish alternative methods of communication for critical personnel.		Changed
6-6-1012	Recommend deletion. Superseded by 5095.		Deleted
7-6-1013	Service Providers, Network Operators and Equipment Suppliers should review their insurance requirements in order to maintain business continuity in the event of massive property damage or loss, incapacitation of senior officers, and other interruptive situations.		Unchanged
6-6-1014	Recommend deletion. Superseded by 5072, 1001, 1005, NEW6		Deleted
7-7-1015	Network Operators and Service Providers should make available to the disaster recovery team "as-built" drawings of network sites.		Changed
7-6-1016	Service Providers and Network Operators should develop processes or plans to quickly account for all employees (e.g. field techs) in or near the impact area of a disaster.		Unchanged
7-6-1017	Service Providers and Network Operators should have documented plans or processes to assess damage to network elements, outside plant, facility infrastructure, etc. for implementation immediately following a disaster.		Unchanged
7-7-1018	Service Providers, Network Operators, and Equipment Suppliers should emphasize employee and public safety during a disaster and all phases of disaster recovery.		Changed
6-6-1019	Recommend deletion. Superseded by 5135.		Deleted
7-7-1020	Service Providers, Network Operators, and Equipment Suppliers should assess the need for Chemical, Biological, Radiological and Nuclear (CBRN) response program to safely restore or maintain service in the aftermath of fuel/chemical contamination or a Weapons of Mass Destruction (WMD) attack.		Changed
6-6-1021	Recommend deletion. Superseded by 8066.		Deleted

7-6-1022	Service Providers, Network Operators, and Equipment Suppliers should consider the development of a vital records program to protect vital records that may be critical to restoration efforts.		Unchanged
7-7-1023	Service Providers, Network Operators, and Equipment Suppliers should identify essential staff within their organizations that are critical to disaster recovery efforts. Planning should address the availability of these individuals and provide for backup staff.		Changed
7-7-1024	Service Providers, Network Operators, and Equipment Suppliers should plan for the possibility of a disaster occurring during a work stoppage.		Changed
7-7-1025	Service Providers and Network Operators should consider using a team to quickly determine appropriate actions both pro-active or re-active to address potential or real threats.		Changed
6-6-1027	Recommend deletion. Superseded by 1028, 5058, 5204, 0662, 0672 and 0675.		Deleted
7-7-1029	Service Providers and Network Operators should periodically review their portable power generator needs to address changes to the business.		Changed
6-6-1030	Recommend deletion. Superseded by 5207, 0658		Deleted
7-7-1031	Service Providers and Network Operators should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.	www.ncs.gov/ncc/main.html and www.nric.org/meetings/meeting20020913.html	Changed
7-7-1032	Service Providers and Network Operators should document their critical equipment suppliers, vendors, contractors and business partners in their Business Continuity Plans along with an assessment of the services, support, and capabilities available in the event of a disaster.		Changed
7-7-1034	Network Operators should ensure that the emergency mobile assets are maintained at a hardware and software level compatible with the existing network infrastructure so that the emergency mobile assets will be immediately available for deployment.	Experience has shown that hardware and software maintenance of emergency mobile assets should be assigned to designated technicians.	Changed
7-7-1035	Service Providers and Network Operators should include trial deployment of emergency mobile assets in disaster response exercises to evaluate level of personnel readiness.		Changed
7-7-1036	Network Operators should determine in advance if they will use line of sight systems (microwave radio, free space optics, and satellite communications systems) to re-establish communications. If these technologies are to be deployed it is recommended that path designs be developed for each critical area in advance with personnel trained to install and optimize the systems.		Changed
7-7-1037	Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should use a disaster recovery support model that provides a clear escalation path to executive levels, both internally and to business partners.		Changed
7-6-1038	Service Providers, Network Operators and Equipment Suppliers should consider during times of disaster, communicating the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response.		Unchanged

7-7-1039	Equipment Suppliers should develop support processes that include interfaces with those internal organizations (e.g., sales, logistics, manufacturing) that have a potential role in assisting Network Operators and Service Providers in disaster response efforts.		Changed
7-7-1040	Service Providers, Network Operators and Equipment Suppliers should consider using lab, demonstration or training equipment if replacement equipment is unavailable in disaster situations.		Changed
7-6-1041	Equipment Suppliers should consider providing a "Disaster Information Checklist" to all of the Service Providers they support. The checklist should provide a set of questions which the Service Provider would address immediately after a disaster and then promptly inform the Equipment Supplier to facilitate equipment delivery.		Unchanged
6-6-1042	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-6-1043	Equipment Suppliers should consider, during their response to major disasters, editing the support "hotline" calling tree by adding a specific entry for disaster events.		Unchanged
7-6-1044	Equipment Suppliers should consider providing a "Disaster Recovery Services Checklist" to all of the Service Providers they support. The checklist would provide a listing of the Equipment Supplier's professional services which the Service Provider may require during an event.		Unchanged
7-7-1045	Service Providers and Network Operators should use their escalation process, as needed, to address resource issues identified through damage and resource assessments.	Internally from separate regions, vendors, through mutual-aid partners, or state emergency operations centers.	Changed
6-6-1046	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-1047	Service Providers and Network Operators should develop a process to routinely archive critical system backups and provide for storage in a "secure off-site" facility which would provide geographical diversity.		Changed
7-7-1048	Service Providers and Network Operators should consider supplementing media backup storage with full system restoral media and documented restoration procedures that can be utilized at an alternate "hot site", in case of total failure of the primary service site.		Changed
6-6-1049	Service Providers should consider utilizing multiple network carriers for internet backbone connectivity to prevent isolation of service nodes.		Changed
7-6-1050	Network Operators and Service Providers should consider tertiary carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as "hot transport" backup facilities.		Unchanged
7-6-1051	Service Providers and Network Operators should work with Equipment Suppliers and Government entities to identify criteria and procedures for handling network elements affected by nuclear attack or nuclear accidents (e.g., shock wave, Electro-magnetic Pulse (EMP), Thermal, Fallout, fiber darkening of phosphorous based fiber cable).		Unchanged
7-7-1052	Service Providers and Network Operators should periodically assess the functionality of business critical systems during a disaster exercise.		Changed
6-6-1053	Recommend deletion. Superseded by 5026.		Deleted

7-7-1054	Network Operators, Service Providers, and Property Managers should install fire detection systems and consider the use of suppression systems or devices at buildings supporting network functionality.	Function, size and occupancy need to considered. This is not intended to include CEVs, tower sites, huts, regens, temporary or mobile facilities.	Changed
6-6-1055	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-6-1056	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-6-1057	Recommend deletion. Superseded by 5127.		Deleted
7-7-1058	Service Providers, Network Operators and Equipment Suppliers should work collectively with local, state, and federal governments to develop relationships fostering efficient communications, coordination and support for emergency response and restoration.		Changed
6-6-1059	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
6-6-1060	Recommend deletion. Not a best practice: -Too vague -Obsolete/Impractical -Required by law, regulation, etc. -Recommendation for company		Deleted
7-7-1061	Service Providers and Network Operators should ensure that Telecommunication Service Priority (TSP) records and data bases are reconciled annually.		Changed
6-6-1062	Recommend deletion. Superseded by 1058		Deleted
7-7-1063	Service Providers and Network Operators should set Initial Address Messages (IAMs) for congestion priority in accordance with applicable ANSI standards. This will ensure government emergency calls (911, GETS) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111.	The Network Interconnection Interoperability Forum (NIIF) (www.atis.org/niif/pots.asp), is tracking implementation as part of NIIF Issue 0095 in coordination with the Office of the Manager, National Communications System.	Changed
7-7-1064	Service Providers, Network Operators, and Equipment Suppliers should implement minimum network management controls in order to promote reliability of the interconnected network.	NIIF Reference Document is available at http://www.atis.org/niif/index.asp. NIIF Document 5001 Reference Document, Part VI, Section 2.	Changed
7-7-1065	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity.	Functional redundancy could include having employees telecommute when a center is affected as opposed to having an alternative center.	Changed
6-6-1066	Recommend deletion. Superseded by 0504		Deleted
7-6-1067	Network Operators, Service Providers and Property Managers should consider, in preparation for predicted natural events, placing standby generators on line and verifying proper operation of all subsystems (e.g., ice, snow, flood, hurricanes).		Unchanged
7-7-5281	Service Provider, Network Operators and Property Managers with buildings serviced by more than one emergency generator, should design, install and maintain each generator as a stand alone unit that is not dependent on the operation of another generator for proper functioning, including fuel supply path.		Changed

7-7-0771	Service Providers, Network Operators and Equipment Suppliers should consider a procedure for pre-notification of visits to critical facilities.		New
7-7-0772	Collocated Service Providers should coordinate with Network Operators and Property Managers on equipment moves, adds or changes (MACs) which could impact other occupants.		New
7-7-0773	Network Operators, Service Providers, and Property Managers should perform annual capacity evaluation of power equipment, and perform periodic scheduled maintenance, including power alarm testing.		New
7-7-0774	Network Operators, Service Providers and Equipment Suppliers should provide warning signs to indicate precautions to be taken when powering on circuits that require special procedures.		New
7-7-0775	Service Providers and Network Operators should consult and update the synchronization plan whenever facility (e.g., intra-/inter-office or inter-provider interconnect circuits) rearrangements, additions, deletions, or consolidations are planned. Verify the completed changes against the synchronization plan.		New
7-7-0776	Service Providers, Network Operators and Equipment Suppliers should conduct and periodically re-validate physical security assessments on critical network facilities.		New
7-7-0777	Equipment Suppliers should optimize equipment initializations to minimize service impact.		New
7-7-0778	Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that handling installation/interconnection of circuit and signal paths continues to be performed by qualified communications technicians.		New
7-7-0779	Service Providers, Network Operators and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	Related Best Practices are 5092 and 8548.	New
7-7-0780	Network Operators and Service Providers should consider including coordination information of Public Safety Authorities when developing disaster restoration and prioritization plans.		New
7-7-0781	Service Providers, Network Operators, and Property Managers should evaluate the use of automatic notification mechanisms to the local fire department at critical facilities.		New