NRIC VII Draft (New/Changed/ Unchanged)	NRIC VII Best Practice Number	NRIC VII Best Practice Draft	NRIC VII General/Comments Draft
Revised	**7-6-8061**	**IR (Incident Response) Procedures:** Service Providers and Network Operators should establish a set of standards and procedures for dealing with computer and network security events. These procedures can and should be part of the overall business continuity/disaster recovery plan. Where possible, the procedures should be exercised periodically and revised as needed. Procedures should cover likely threats to those elements of the infrastructure which are critical to service delivery/business continuity. See appendix X and Y.	IETF RFC2350, US-CERT. Also, NRIC BP 7-P-8074, and 7-P-8075, 6-5-0561, 5239, 1001, 1002, 1004, 1006, 1009, 1010, 1016, 6-5-0599. Supersedes NRIC BP 6-5-0500.
Revised	**7-6-8066**	**Sharing Information with Industry & Government:** Service Providers, Network Operators, and Equipment Suppliers should participate in regional and national information sharing groups such as the National Coordinating Center for Telecommunications (NCC), Telecom-ISAC (Information Sharing and Analysis Center), the ISP-ISAC (when chartered), Network Security Information Exchange (NSIE), and the National Infrastructure Protection Center (NIPC). Formal membership and participation will enhance the receipt of timely threat information and will provide a forum for response and coordination. Membership will also afford access to proprietary threat and vulnerability information (under NDA) that may precede public release of similar data. Because of the critical nature of this information, 24x7 coverage should be considered.	Related to NRIC BP 7-P-8553. Supersedes NRIC BP 6-5-0585, 6-5-5102 & 6-5-5147
Revised	**7-7-8068**	**Incident Response Communications Plan:** Service Providers, Network Operators, and Equipment Suppliers should develop and practice a communications plan as part of the broader Incident response plan. The communications plan should identify key players and include as a minimum - contact names, business telephone numbers, home tel. numbers, pager numbers, fax numbers, cell phone numbers, home addresses, internet addresses, permanent bridge numbers, etc. Notification plans should be developed prior to an event/incident happening where necessary. The plan should also include alternate communications channels such as alpha pagers, internet, satellite phones, VOIP, private lines, blackberries, etc. The value of any alternate communications method needs to be balanced against the security and information loss risks introduced.	NRIC BP 0561, 0609, 8066 and 8055.
New/revised	**7-P-8132**	**Leverage Business Impact Analysis for Incident Response Planning:** Service Providers and Network Operators should leverage the BCP/DR Business Impact Assessment (BIA) efforts as input to prioritizing and planning Information and/or Physcial Security Incident Response efforts.	Related to NRIC BPs 7-6-8061, 6-6-1003, and 6-6-1001.
Changed reference/comment	**7-6-8548**	**Incident Response (IR) Procedures:** When a service outage or security incident occurs, Service Providers and Network Operators should follow processes similar to Appendix X.	IETF RFC2350, US-CERT NRIC BP 7-P-8074, 7-P-8075, 6-5-0561, 6-5-0599, 6-5-5092, 5239, 1001, 1002, 1004, 1006, 1009, 1010, 1016
Delete	**7-6-8564**	**Recovery Incident Response (IR) Post Mortem Checklist:** After responding to a security incident or service outage, Service Providers and Network Operators should follow processes similar to Appendix Z, to capture lessons learned and prevent future events.	Deleted Superseded by 5227.