Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:131 **31-03-2021**

Name: Data Center Power systems Guidelines

Threat Classification: Power attack, Black outs, Brown outs, Electromagnetic interference

Summary:

Power system such as Generators (DGs), Uninterrupted power supply (UPS), Industrial control systems (ICS), and supervisory control and data acquisition (SCADA) systems, are the most critical infrastructure of data centers and must be well protected against any type of cyber threats. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters as well as malicious or accidental actions by insiders. Security objectives typically follow the priority of availability, integrity and confidentiality.

Recommended Sources:

Please visit the following links for detailed guideline:

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Recommendations: Minimize opportunities for Power system failures by following not limited to the below guidelines:

- Developing security policies, procedures, training and educational material that applies specifically to the data center power systems.
- Continuous monitoring of data center power systems through network monitoring system (NMS) and Security Incident and Event Management system (SIEM).
- Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks).
- Ensuring that critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Restricting physical access to the Data center power systems.
- Tracking and monitoring audit trails and logs on power systems.
- Employing reliable and secure network protocols and services where feasible.
- Update all Software/firmware of data center power systems to the latest and stable versions with appropriate patches (where applicable).
- In case of any cyber incident, please immediately report to this office.