Everyone in your organization needs to take responsibility for security - even those for whom IT/OT security is not an explicit role. Be sure to take the following steps to reduce your risk:

Remote Desktop Protocol (RDP) Risks

Remote Desktop Protocol (RDP) sessions over the Internet to compromise identities, steal login credentials, and ransom other sensitive information.”

As described in a public service announcement released on September 27, 2018, by the Federal Bureau of Investigation (FBI), malicious cyber actors have developed methods of identifying and exploiting vulnerable systems to gain unauthorized access. These attacks, which are facilitated by exposing RDP endpoints via dark markets selling RDP Access, have the potential to introduce significant risk if not properly secured.

NERC GUIDANCE

Remote Desktop Protocol (RDP) Risks

Developments at FERC

In June 2019, NERC announced that the ERO Project Team is continuing to develop and test Release 1 of the Align Project, which is designed to improve the alignment between wholesale and retail reliability standards. The project team is seeking input from stakeholders to help guide the development and testing of the new requirements.

Recent NERC News

Standards Efficiency Review (SER) Retirements Filed

On October 1, 2010, FERC granted approval of CIP-008-6 (Cyber Security - Incident Reporting and Response Requirements for Critical Entities) and CIP-008-7 (Cyber Security - Incident Reporting and Response Requirements for Critical Entities). The revised standards were developed to address reliability issues concerning the study of single points of failure of protection systems.

Remote access wherever it is not absolutely necessary;