The Speed of Innovation Paired with Heightened Security Regulations. The evolution of technology allows utility organizations to provide customers with improved services and increased reliability, but often times security gets in the way of adopting a cloud-first business model. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of standards aimed at regulating, monitoring, and managing the security of the Bulk Electric System (BES) in North America. To ensure cloud operations are monitored properly, utility organizations need their cloud provider to understand the standards imposed upon their industry.

In-Country Solution Deployment. NERC-CIP requires BES Cyber System Information (BCSI) to be restricted to authorized personnel and prohibited from unauthorized access, as the information is vulnerable to cybersecurity attacks. One critical element that ensures enhanced security is a local support model that includes exclusively U.S. resources who have been vetted through personnel risk assessments (i.e. background checks).

The utility industry provides necessary amenities to many, such as water, electricity, and natural gas. When it comes to their digital transformation, utility industries are required to maintain additional security standards that extend beyond commercial cloud solutions. The keys to a secure digital transformation are:

**The Roadblocks:** BARRIERS TO SECURELY ADOPTING CLOUD SOLUTIONS

The Speed of Innovation Paired with Heightened Security Regulations. The evolution of technology allows utility organizations to provide customers with improved services and increased reliability, but often times security gets in the way of adopting a cloud-first business model. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of standards aimed at regulating, monitoring, and managing the security of the Bulk Electric System (BES) in North America. To ensure cloud operations are monitored properly, utility organizations need their cloud provider to understand the standards imposed upon their industry.

In-Country Solution Deployment. NERC-CIP requires BES Cyber System Information (BCSI) to be restricted to authorized personnel and prohibited from unauthorized access, as the information is vulnerable to cybersecurity attacks. One critical element that ensures enhanced security is a local support model that includes exclusively U.S. resources who have been vetted through personnel risk assessments (i.e. background checks).

The Answer: SAP National Security Services

**Infrastructure Built to Support Regulated Workloads**
Our cloud infrastructure is built to protect utility organization’s confidential data. We deploy solutions on highly regulated hyperscalers, such as AWS GovCloud and Azure Government, who comply with the security regulations set forth by government agencies.

**Solutions Secured to Industry Standards**
Our defense in depth strategy ensures preventive and detective controls are in place to protect cloud systems and data. Customers can be assured the integrity and security of NERC CIP regulated entities’ BCSI, and other sensitive information, is protected.

**Local Support Model to Mitigate External Risk**
We support the utility’s compliance to NERC CIP by ensuring all cloud resources operate according to necessary compliance levels. All supporting personnel are located within the U.S., are U.S. persons, and have been approved through background checks and security screenings.

The Security Regulations We Deploy:
- International Traffic and Arms Regulations (ITAR) and Export Administration Regulations (EAR) compliant solutions
- Cloud environments built to the NIST 800-53 security standards
- Cloud solutions designed to support mission-critical workloads and protect BES Cyber System Information (BCSI)
WHY SAP NATIONAL SECURITY SERVICES: SECURE. LOCAL. SOVEREIGN.

We understand that utility organizations face different international threats and have unique compliance requirements surrounding their cloud operations. We are the solution for meeting and exceeding these challenges.

• We leverage tools such as vulnerability scanning, intrusion detection, and continuous monitoring to ensure your data stays protected with an automated security model.
• We enforce authentication and access rights to protect BES Cyber System Information (BCSI).
• Adherence to ITAR provides dedicated U.S. resources to support your cloud landscape through deep industry and regional compliance knowledge.
• We mitigate the risk of external threats by protecting system management, providing in-country deployment, and leveraging an enterprise strategy to control the data and resource access within your region.