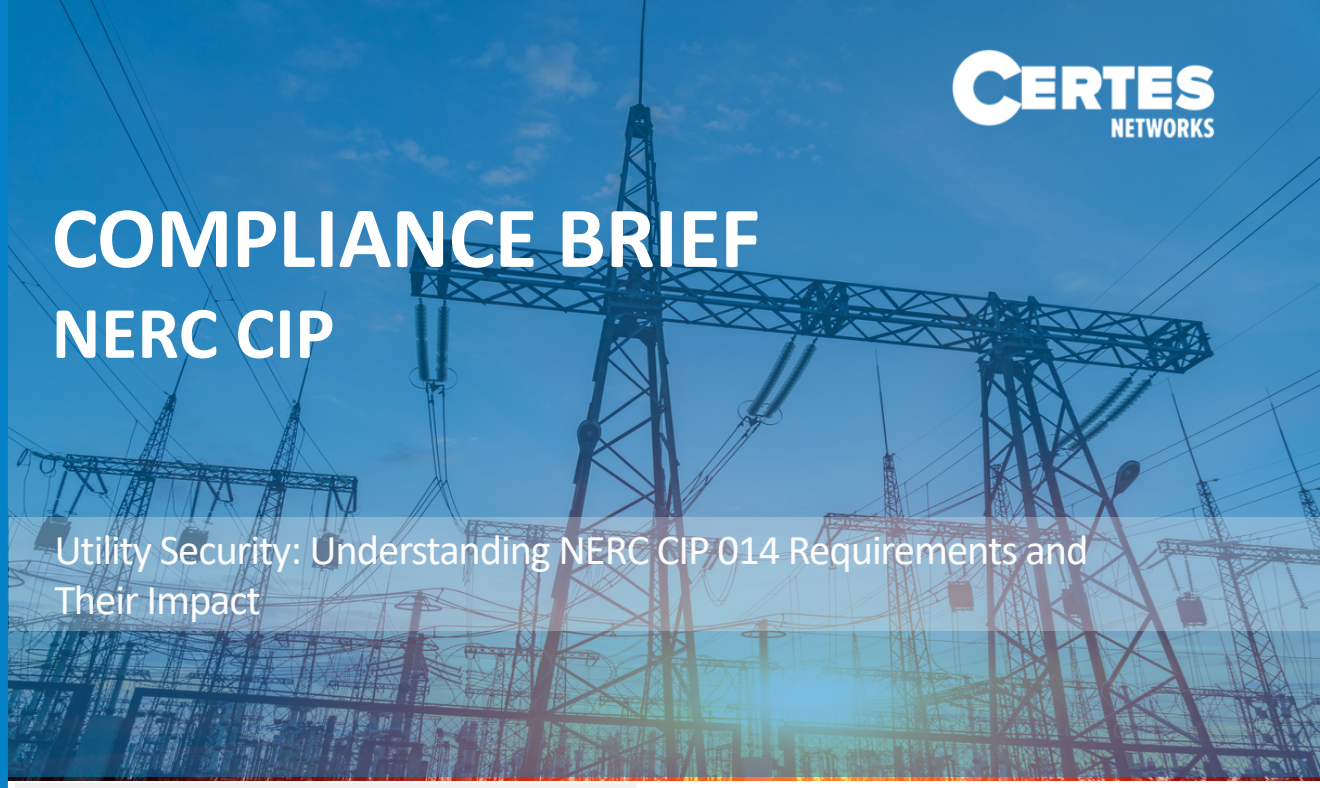


COMPLIANCE BRIEF
NERC CIP

Utility Security: Understanding NERC CIP 014 Requirements and Their Impact

What is NERC CIP and Why It's Important

In the U.S. energy market, the ownership breakdown is a mix of regulated investor-owned utilities, municipal electric utilities, rural electric cooperatives, federal power marketing agencies and independent power producers. According to the U.S. Department of Energy, investor-owned utilities account for more than 50 percent of net generation and almost 80 percent of transmission. Public-owned utilities and cooperatives, along with the Federal power agencies, account for approximately 25 percent of net generation and almost all of the remaining transmission. Independent power producers account for the remaining 25 percent of net generation.

These entities are responsible for utility security, and they have a vast array of assets that require safeguarding. The three grids in the U.S. (Eastern, Western and Texas) are composed of more than 9,000 generation assets, 200,000 miles of transmission lines at 230 kV or above and 2,100 HV transformers. The high degree of interconnectivity within the grid reduces exposure to major failures. A single equipment component failure is unlikely to cause a cascading effect on a significant portion of the grid. No region in the U.S. has ever experienced simultaneous high-voltage transformer failures – just singular failures. However, the large and growing number of critical infrastructure assets and the ever-expanding list of threat profiles make single or multiple failures a significantly greater concern to overall grid reliability.

The environment in which utilities operate is also changing – ever-evolving and creating more areas where the grid is vulnerable to disruption. These changing areas can be viewed from both an internal and external standpoint, and both threat profiles require utilities to carefully plan and coordinate efforts across their organization. These profiles also include threats that could be physical or cyber-related (or both) in nature, further increasing the grid's vulnerability and the need for enhanced security to safeguard reliability.

NERC and Critical Infrastructure Protection

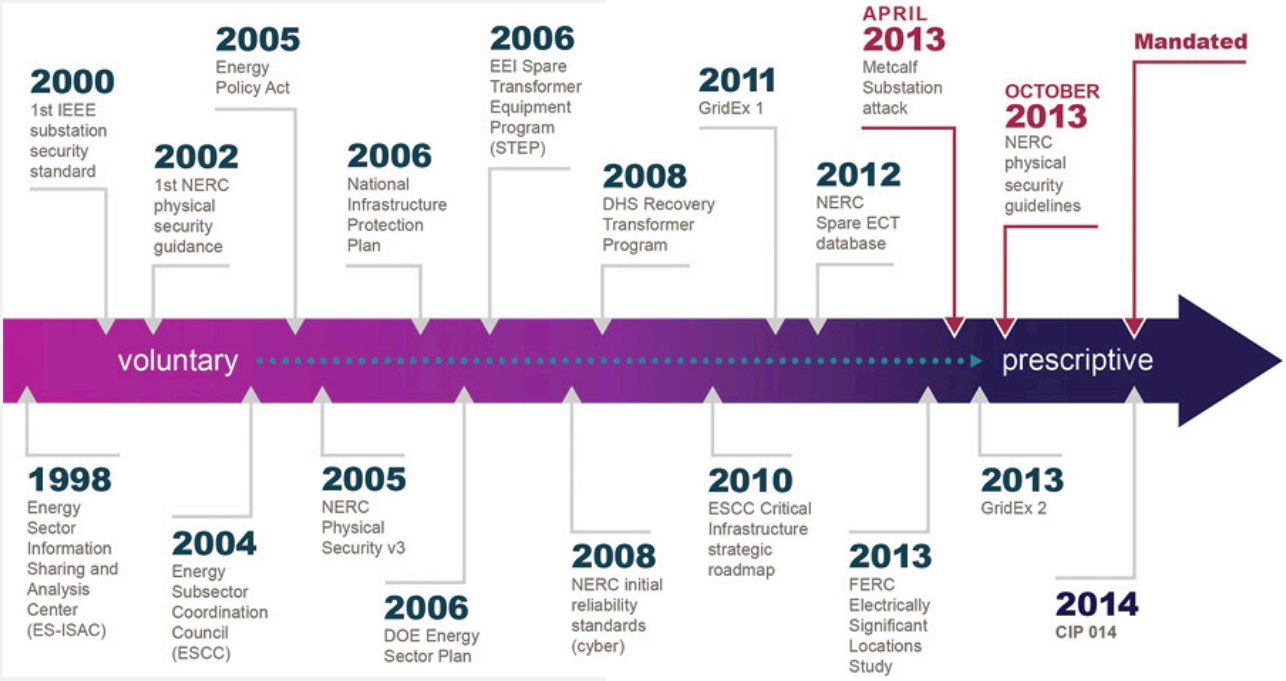
Utility security can be viewed as the integration of national security into the power and electricity sectors. The protection of the largest machine ever designed, built and operated is critical to the quality of life and the economic future of everyone in North America.

Utilities are not alone in their effort to protect the reliability of the power grid. The North American Electric Reliability Corporation (NERC) is the regulatory authority with responsibility for the reliability of service to more than 334 million people. NERC's standards are directly aimed at encouraging or mandating steps for utilities in protecting their operations, helping to ensure overall grid reliability.

NERC's authority has led to critical infrastructure protection (CIP) standards that guide utilities' planning and activities to eliminate or mitigate the the many internal and external threat profiles. The CIP standards have evolved over time both in the scope

of their focus and in the level of their authority. While cybersecurity continues to be an area of intense scrutiny and need for protection, focus has shifted in recent years toward the need for more intense physical security.

As shown in Chart 1, the U.S. government and NERC's approach to critical infrastructure protection stems from the National Infrastructure Protection Plan issued by the Department of Homeland Security. This plan was first released in 2006, revised in 2009 and revised again in 2013. The plan outlines how government and private sector participants in the critical infrastructure community can work together to manage risks and achieve security and resilience. The chart also shows the shift from primarily voluntary guidelines to more prescriptive standards in recent years.



A CIP 014 Standard Overview

Due to finite financial resources, utilities may not have all of the physical security protection they might otherwise like for their assets. This reality requires both appropriately prioritizing what assets are critical and then protecting them in light of the CIP 014 standard.

In general, the CIP 014 standard for physical security is a high-level threat and vulnerability analysis to uncover potential threats, weaknesses and the corresponding risks should an attack take place on a critical grid juncture. The standard provides a structured framework whereby utilities must perform an initial risk assessment. This assessment must be reviewed by an independent third party. The standard also then requires utilities to perform a tailored assessment and evaluation of potential threats and the associated vulnerabilities related to each identified critical location. And finally, the utility must develop and implement a plan to protect those identified assets from physical threat and have the plan verified by an independent third party.

REQUIREMENT ONE

The first requirement under the CIP 014 standard is for utilities to identify transmission stations, substations and control centers that – if rendered inoperable or severely damaged – could result in widespread instability, uncontrolled separation or cascading failures within an interconnection. This initial risk assessment covers existing and planned facilities within the next two years. Subsequent analyses have a 30- or 60-day timeframe, depending on whether transmission stations or substations were identified in the initial or previous follow-up assessments.

For the most part, generation plants and control centers are well-protected, leaving substations and transmission lines as the most potentially vulnerable assets. These assets are therefore measured against the criterion of their critical importance – what would happen if they were rendered inoperable or severely damaged. If the subsequent interconnection instability would be significant, then the assets must be included in the assessment. NERC has identified these assets as transmission stations or substations operated at or above 500 kV. Also included are substations between 200 and 499 kV that have three connected substations.

It should be noted that one of the two revisions directed by FERC applies under this requirement. The revision would allow applicable authorities to edit a utility's critical facility list, even if the facility doesn't meet the stated criteria. This provides insight that the critical list will continue to evolve based on new criteria or evolving threats. While centered on overall grid stability, additional considerations by government authorities could include the ease of replacing a transformer or whether a substation serves critical customers such as emergency or healthcare providers.
The timing of the initial risk assessment is dependent on the timing of the final regulation being announced (at press time, it is still pending). The standard would then include an effective date, and the deadline for the first assessment would be clear.

Requirement	Goal
R1	Initial risk assessment– critical facility identification
R2	Independent review of initial risk assessment of R1
R3	Coordination between operator and owner
R4	Threat and vulnerability assessment
R5	Development and implementation of physical security plan
R6	Third-party assessment of plan of R4 and R5

REQUIREMENT TWO

Under the second requirement of the standard, NERC requires utilities to have their initial risk assessment verified by an unaffiliated third party. NERC requires utilities to select either a registered planning coordinator, transmission planner, reliability coordinator or an entity that has transmission planning or analysis experience.
As NERC notes, it's critical for utilities to work with a third party that has transmission experience. It could also be recommended that the third party have a broader depth of utility knowledge along with cybersecurity capabilities to approach security in a holistic way.

Utilities may also considering a third party that is capable of working collaboratively on planning and assessing, as NERC allows for the third-party verifier in requirement two to assist the utility with the processes outlined in requirement one. This collaborative approach to the first two requirements can increase the efficiency and effectiveness of the overall process.

The CIP 014 standard's second requirement must be finished within 90 days of the completion of the initial risk assessment in requirement one.

REQUIREMENT THREE

The standard's third requirement mandates the sharing of assessment information and the critical nature of assets between transmission owners and operators. If the owner of a critical asset is not the operator, NERC requires communication between the two regarding the identification (requirement one) and verification (requirement two) of the particular station or substation's status as a critical asset.

This notification must take place within seven days of the completion of requirement two, and must include the date on which requirement two was completed, because that date serves as the beginning point for the operator to complete requirements four, five and six.

It is also required that the transmission owner inform the transmission operator within seven days should any assets be removed from the critical asset list during subsequent assessments.

REQUIREMENT FOUR

After assessing and identifying critical transmission stations or substations, verifying their status and communicating that information to the operator if needed, requirement four of the CIP 014 standard mandates an evaluation of the potential threats and vulnerabilities of a physical attack to each transmission station, substation and control center identified under the first requirement.

According to NERC, the evaluation should include any unique characteristics of the location, any prior history of attack or past physical security events on similar facilities and any intelligence or threat warnings received from sources such as law enforcement, NERC, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) or U.S. federal and/or Canadian governmental agencies.

This evaluation is the basis of the strategic plan for physical security and should also inform a utility's infrastructure investment planning. It is critical to get this step right. Threat and vulnerability assessments combined with risk assessment are the foundation for a risk management plan. With the 'where' established through previous requirements, the idea behind the assessment is to analyze:

- Who or what can hurt us?
- How can we be hurt?
- When are we most vulnerable?
- What is the probability of that happening?

Answering these questions will lead to a wide range of responses among utilities, highlighting the importance for a customized evaluation approach for each utility and in some cases each critical location on a utility's list. Several current methodologies based on defense or emergency management agency protocols are available to make these evaluations. It can be helpful to work in conjunction with a third-party consultant during this phase of the standard as well to contribute to the efficiency of the next two steps. The third party should have a strong knowledge of the full spectrum and impact of this process – the overall utility industry, physical and cybersecurity, stakeholder and customer impacts, etc.

There is no definitive timetable or deadline specifically for requirement four. However, utilities should be aware that requirement five hinges on this evaluation and does have a deadline based on the completion date of requirement two. The two stages can be completed concurrently.

REQUIREMENT FIVE

The fifth requirement from the NERC standard is for utilities to develop and implement a documented physical security plan that covers the identified and evaluated transmission stations, substations and primary control centers.

According to NERC, the plan should address resiliency or security measures designed collectively to deter, detect, delay, assess, communicate and respond to the potential physical threats and vulnerabilities identified during the previous evaluation. The plan should also include law enforcement contact and coordination information, a timeline for executing the physical security enhancements and modifications specified in the physical security plan and provisions to evaluate evolving physical threats and the necessary security measures to mitigate them.

Utilities may look beyond just a plan for NERC compliance and integrate these concepts as part of the their overall security programs, which should include physical and cybersecurity approaches, as well as accounting for other utility goals related to asset investment, growth and resiliency. The timelines contained in the plan should be realistic and coordinated with investment capabilities.

Requirement five must be finished within 120 days of the completion of the verification process in requirement two.

REQUIREMENT SIX

The final requirement in the CIP 014 standard is similar to the second in that it requires an unaffiliated third party to verify the utility's information and activities, except that the validation in this step is for the threat and vulnerability evaluation and subsequent security action plan. As with requirement two, NERC allows the flexibility to work with the same third party throughout the evaluation and plan development steps. This teaming approach allows utilities to complete requirement six at the same time as requirements four and five.

Under the standard, requirement six must be completed no later than 90 days following the completion of requirement five.

CONCLUSION

In working with utilities for on-going security measures and in preparation for the CIP 014 standard, a holistic approach is recommended to utility security that is both proactive and reactive. Deterring threats – both physical and cybersecurity – and minimizing vulnerabilities is a proactive approach while mitigating the consequences of attacks is reactive.

Although utilities will continue to be confronted with new types of challenges followed most likely by new regulations, it's important for utilities to take a flexible, long-term view to utility security and position themselves to meet both anticipated and unforeseen events.

Long-term utility security planning focuses on the people who design, operate and maintain electric grids; the processes employed for developing plans, measures and operating procedures; the physical security materials and hardening measures; and integration of appropriate cybersecurity system technologies and applications. The long view of the future may start with CIP standards, but it should recognize that existing regulations will evolve as new needs and requirements arise.

Diligent preparation for an audit is essential. NERC has published worksheets to help organizations prepare for their next audit, which can be found at: https://www.nerc.com/pa/comp/Pages/Reliability-Standard-Audit-Worksheets-(RSAWs).aspx

A copy of the latest NERC CIP Reliability Standards as it relates to cyber security can be found at: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com