NERC-CIP’S MOST WANTED

The Top Three Most Violated NERC-CIP Standards

“What you need to know to stay off the list.”
NERC-CIP’s Most Wanted

The Top Three Most Violated NERC-CIP Standards

CONTENTS:
Overview ................................................................. 4
Top Ten All Time Violated NERC Standards ........................................... 5
CIP-001: The Most Prominent .................................................. 6
CIP-002: The Newest Addition ...................................................... 7
CIP-004: A Recurring Problem ...................................................... 8
Why the Prevalence of CIP-001, CIP-002 & CIP-004 on the Top Ten List .... 10
AlertEnterprise delivers ............................................................... 11
A Next-Generation NERC-CIP Solution ........................................... 11
OVERVIEW

For three years, electric utilities across North America have been engaged in NERC Critical Infrastructure Protection (CIP) compliance, which includes Sabotage Reporting, Critical Cyber Asset Identification, Security Management Controls, Personnel Training, Physical Security of Critical Cyber Assets, among four other standards. For each of those three years, a minimum of three NERC CIP standards have made appearances on NERC’s Top 10 All Time Violated Standards¹ list, including at least two of them as recurrent violators.

As you recall, the North American Electric Reliability Corporation (NERC) is an international, self-regulatory, not-for-profit authority governed by the Federal Energy Regulatory Commission (FERC). At its core stands an important goal: to ensure the reliability of the Bulk Electric System (BES)² in North America. In 2007, NERC approved Critical Infrastructure Protection (CIP) standards CIP-001 through CIP-009 for new and improved regulatory accountability. NERC CIP carries two primary purposes. The first purpose is to provide a cyber-security framework to ‘identify’ Critical Cyber Assets³ and the second is to ‘protect’ those assets.

AlertEnterprise, Inc. works closely with companies across the utility spectrum to address and resolve all areas of NERC CIP compliance. Our objective in this paper is to increase awareness of three most violated NERC CIP standards: CIP 001, CIP 002, CIP 004, and the one step you can take to effectively avoid blame as part of NERC’s Most Wanted⁴.

---

¹ The Top 10 All Time Violated Standards are chosen from nearly 100 NERC standards, which also include NERC CIP standards.
² As defined by the Regional Reliability Organization, the Bulk Electric System is the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100kV or higher.
³ Critical Cyber Assets are cyber assets essential to the reliable operation of Critical Assets.
⁴ NERC’s Most Wanted is the list of CIP standards we have determined to be the most critical to resolve.
CIP-001, -002, -004:

AMONGST THE TOP TEN ALL TIME VIOLATED NERC STANDARDS

Each year, NERC issues a report of the Top 10 All Time Violated Standards. These ‘Top 10’ are chosen from nearly 100 NERC standards that range from NERC PRC to NERC CIP. NERC CIP standards: CIP-001, CIP-002, CIP-003, CIP-004, CIP-006 and CIP-007 have each ranked in the top ten of this list at least once since the inception of NERC CIP standards. Over the past three years, there has been a recurrent trend with CIP-001, CIP-002, CIP-004, and CIP-007’s presence on the list. The two standards that deal specifically with cyber and physical security are CIP-002 and CIP-004. The standard specific to sabotage and most often put on the back-burner is CIP-001. The standard intended to ensure management of system security is CIP-007.

It is crucial to delve into a discussion individually for CIP-001, CIP-002 and CIP-004 to explore where the violations arise, and what you can do to significantly reduce your chances of falling victim to the most common violations in the CIP-001, CIP-002 and CIP-004 categories. CIP-007, the standard to ensure methods, processes and procedures of asset securement, is not of any lesser importance and is covered in a separate whitepaper.

Now, let’s briefly discuss the requirements of CIP-001, CIP-002 and CIP-004.
CIP-001: THE MOST PROMINENT
Sabotage Reporting

Responsible for almost a quarter of all ‘Top 10’ violations just one year after the NERC CIP standards became effective, CIP-001 has been unable to escape an appearance on this list.

CIP-001 requires the reporting of disturbances or unusual occurrences, suspected or determined to be caused by sabotage. The key mandates of CIP-001 compliance as determined by NERC apply to transmission operators, generator operators, reliability coordinators, balancing authorities, and load serving entities. They are as follows:

- **Recognition Procedures**
  Each responsible entity mentioned above shall have a procedure in place for recognition of sabotage events, and for relaying awareness of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection, to its operating personnel.

- **Communication Procedures**
  Each responsible entity shall have procedures whereby information about concerning sabotage events is communicated to appropriate parties in the Interconnection.

- **Response Guidelines**
  Each responsible entity shall provide its operating personnel with sabotage response guidelines for the purpose of reporting disturbances due to sabotage events.

- **Communications Contact Establishment**
  Each responsible entity shall establish communications contacts with applicable local FBI or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

CIP-001 also details the Compliance Monitoring Process and Levels of Non-Compliance. The Compliance Monitoring Process places compliance monitoring in the hands of Regional Reliability Organizations, provides methods of verification, and details a Data Retention Policy as evidence and proof of compliance.
**CIP-002: THE NEWEST ADDITION**

“Critical Cyber Asset Identification”

NERC CIP-002 has not always been a member on NERC’s ‘Top 10’ list. When NERC issued its first evaluation of the top ten violators in 2008, NERC CIP-001 and CIP-004 were the two CIP standards to make noticeable appearances on the list. Since then, CIP-002 has become another unfortunate CIP standard to make the list.

CIP-002 requires the identification and documentation of Critical Cyber Assets associated with the Critical Assets\(^5\) that support the reliable operation of the BES. In simpler terms, this standard requires the responsible unit\(^6\) to figure out what items are essential to the operation of its substations, including to its control, transmission and distribution systems. CIP-002 makes it a priority for you to understand who has access to your assets and the effects of access on your assets.

To meet the requirements of CIP-002, the first step involves a multi-pronged approach to identify, evaluate, and document a risk-based methodology that will be used to identify Critical Assets. The next step is to consider the multitude of systems and substations that correlate to the reliability and operability of the BES, and develop a list of an entity’s assets. Once this list is developed, an entity must isolate those assets deemed critical as the Critical Cyber Assets, and perform a review on those assets on at least an annual basis. This procedure appears simple, doesn’t it? But remember, CIP-002 is on that ‘Top 10’ list.

---

\(^5\) Critical Assets are those systems, equipment or facilities that, if affected by destruction or otherwise, would affect the reliability or operability of the Bulk Electric System.

\(^6\) The Responsible Entity shall mean
CIP-004: A RECURRING PROBLEM
“Insider Threat”

At the center of CIP-004 is a perpetrator identified as Insider Threat that manifests itself in the intelligent minds of employees, sabotages entire systems, and exposes an entity’s vulnerabilities. The purpose of CIP-004 is to safeguard weaknesses within company practices and ultimately, to protect the electric grid from incident. CIP-004 has a primary focus on proper training for personnel. Specifically, CIP-004 requires that personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets have an appropriate level of personnel risk assessment, training, and security awareness.

The key mandates of CIP-004 compliance determined by NERC are as follows and apply to contractors and vendors, in addition to employees:

- **Personnel Awareness Program**
  This mandate requires that a utility establish an awareness program whereby authorized cyber or authorized unescorted physical access to Critical Cyber Assets is monitored and documented on at least a quarterly basis by the utility. This program should take into consideration practices including direct and indirect communications, and management support and reinforcement.

- **Personnel Training**
  This mandate requires a utility to establish an annual cyber security training program for the personnel documented in the awareness program. This program ensures that all personnel with access to Critical Cyber Assets are trained within ninety calendar days of authorization to such assets. This training must include: (1) the proper use of Critical Cyber Assets, (2) physical and electronic access controls to Critical Cyber Assets, (3) the proper handling of Critical Cyber Asset information; and (4) action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

  It is important that a utility maintain documentation on the training conducted, including specifics on date of training completion, as well as a record of attendance.
Motivation for insider threat can entail greed, revenge for negative work-related events, or a number of other reasons. For instance, technical employees have used their specific abilities to sabotage an employer’s critical assets and systems.

Personnel Risk Assessment
This mandate requires a documented personnel risk assessment program in accordance with and subject to all applicable jurisdictional laws, and existing collective bargaining unit agreements. At a minimum, a utility must include identity verification and a seven-year criminal check in each assessment, and each component of the risk assessment at least every seven years after the initial assessment, or when need arises.

Personnel Access
This mandate requires a utility to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including electronic and physical access rights. This list must documented, evaluated and updated within seven calendar days of any change in personnel with access to Critical Cyber Assets, and reviewed quarterly.

While the sum total of these requirements will increase an entity’s awareness to existing or potential hazards, an entity cannot expect to be provided with a safety net against all incidents through manual processes. For instance, validation of contractor access through manual processes is full of risk, and in a number of cited cases, contractors were given inadvertent access. Automated software through AlertEnterprise provides a central repository for identity information for all contractors, including management of access to applications, systems, and facilities across the enterprise. For instance, contractor access requests, modification of contractor identity information, or termination of a contractor, are all automated tasks managed through AlertEnterprise Software.
WHY THE PREVALENCE OF CIP-001, CIP-002 AND CIP-004 ON THE TOP TEN LIST?

There are four key reasons why CIP-001, CIP-002 and CIP-004 have landed on the ‘Top 10’ list, but only ONE KEY SOLUTION to reduce their prevalence on this list.

Key Reason One: The Missing Pieces
While NERC-CIP standards outline an approach to identifying Critical Cyber Assets, they do not identify what a particular company’s Critical Assets are. An individual company must determine what aspects of its infrastructure are critical and how to safeguard those areas from incident. Unsurprisingly, this task has not proven easy for companies to do since NERC CIP standard CIP-004 is one of NERC’s Most Wanted.

Furthermore, many regulated entities have expressed that the NERC CIP-002 definition of what constitutes Critical Assets and Critical Cyber Assets is not well defined; these ambiguities in interpretation have led to heightened exposure of compliance violations.

Key Reason Two: Requirements are Ever-Changing and Growing
The expansion of NERC Compliance-Monitoring self-certifications, audits and spot-checks continue to grow in size and scope. Along with this expansion, we’ve continued to observe an increase in the amount of documentation required by NERC-CIP. Electric Utilities are far from mastering these requirements and will never have a chance to do so with current approaches to compliance, especially with newly proposed NERC-CIP standards on track for approval.

Key Reason Three: A Need for a Paradigm Shift
Existing approaches to NERC-CIP compliance are overloaded with endless manual tasks, and employees simply cannot keep up with these tasks while also balancing other areas of concern. Security, risk and compliance is managed in silos today even in the best of organizations, and organizations are relying on purely manual processes to bridge gaps between IT security, control systems engineers, and physical security teams. In order to thoroughly monitor operational thresholds as well as correlate threats related to SCADA networks, companies need to take part in a new generation paradigm shift to their current approach. To truly safeguard vulnerabilities in an entity’s systems will require an automated risk management solution.

Key Reason Four: The Need for Higher Priority on the Management Agenda
It is easy for management to place revenue, economic, and other compliance issues at the forefront of their agenda, leaving NERC compliance to trail behind. This fact is unsurprising considering the multitude of corporate issues continually addressed by management from ethics and social responsibility to environmental and ecological adherence. Management frequently gets weighted down with those items placed at the top of their list and occasionally need to
AlertEnterprise delivers:

- Total compliance management for NERC-CIP (CIP 001 to CIP 009)
- Mapping of Critical Assets and Cyber Assets to IT Security Controls and Physical Access Controls
- Powerful risk modeling to bring to light potential compliance violations, and control system risks and IT security gaps before a NERC violation comes knocking.
- Automation of assessments for NERC CIP, NIST SP800-53, ISO 27000, SOX, HIPAA, and many other regulations.

A NEXT-GENERATION NERC-CIP SOLUTION

True security can only be achieved with a combination of compliance and active policy enforcement. For the compliance piece, no company can expect to be truly compliant without an all-encompassing, next-generation solution. The AlertEnterprise NERC-CIP Solution delivers a unique risk management capability following a three-step process that aggregates blended threats from IT systems, Physical Access Control Systems and Critical Control Systems to uncover previously undetectable risks. The unique ability to correlate risks across IT and other systems provides the best protection from acts of sabotage and theft. AlertEnterprise automates removal of physical access following employee termination, or determines which terminated employees still have SCADA access.

ABOUT ALERTENTERPRISE

AlertEnterprise hides the complexity of integration across ERP, GRC, IAM and Security applications. AlertEnterprise uncovers blended threats that exist across IT applications, Physical Access Control Systems and Industrial Controls systems to deliver true prevention of fraud, theft and acts of sabotage.