RedTeam Security

NERC-CIP Compliance Checklist

Is your organization in compliance with Critical Infrastructure Protection standards? Use this checklist to analyze your information security posture.

RedTeam Security
redteamsecure.com
sales@redteamsecure.com
twitter.com/redteamsecure

214 4th Street E., #140
St. Paul, MN 55101

Table Of Contents

About NERC

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority focused on assuring "the effective and efficient reduction of risks to the reliability and security of the grid." NERC develops and enforces Reliability Standards for bulk power system players in the continental United States, Canada, and the northern portion of Baja California, Mexico.

About This Checklist

This checklist was developed using cybersecurity guidelines provided by NERC's Critical Infrastructure Protection Committee (CIPC) and supported by RedTeam's broad utilities cybersecurity expertise. In line with the NERC's efforts to educate, train, and certify industry personnel, this checklist represents baseline cybersecurity requirements to meet compliance-driven objectives required by law.

For more information on NERC's standards as well as additional resources for cultivating a robust infrastructure security posture, visit **nerc.com**.

LEGEND

Wherever you see a blue callout, you'll find additional resources and helpful tips from RedTeam.

Wherever you see a red callout, the requirement is directly related to one of RedTeam's services. Click on the link provided for more information on how we can help you fulfill the requirement.

Part I: Categorization

- ☐ Is there an inventory of systems and their associated assets?
- ☐ Is a categorized inventory maintained which clearly identifies as high, medium, or low the adverse impact that loss, compromise, or misuse of these systems or assets could have on the bulk electric system (BES)?
- ☐ Does the inventory consider Electronic Access Control or Monitoring Systems (EACSM), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA) in addition to the Systems themselves?
- ☐ Is appropriate protection in place against compromises that could lead to mis-operation or instability in the BES?
- ☐ Has the entity taken into consideration the operational environment and scope of management when defining its BES Cyber System boundaries?
- ☐ Is there a security plan in place for each of its BES Cyber Systems (which can include a grouping of Critical Cyber Assets)?
- ☐ Are cyber system identifications and impact categorizations reviewed at least every 15 months?
- ☐ Are electronic or physical dated records kept as evidence of requirement review?
- ☐ Is evidence retained for the standard three calendar years?
- ☐ Are procedures in place for coordination and communication between entities working in tandem to ensure BES reliability and operability?

BES Cyber Assets are those that, if they were degraded, misused, or otherwise became unavailable, would have an adverse impact on the BES operation within 15 minutes.

Part II: Risk Management

- ☐ Have specific, consistent, and sustainable security management controls been established to mitigate risk to the Bulk Electric System (BES)?
- ☐ Is responsibility and accountability identified in order to protect BES Cyber Systems against compromise that could lead to mis-operation or instability?
- ☐ Do policies establish an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards?
- ☐ Do controls meet requirements for high, medium, and low impact BES Cyber Systems?

How we can help:
Red Team Operations from RedTeam Security

- ☐ Are documented cyber security policies reviewed at least once every 15 months?
- ☐ Are policy documents, records or review, revision histories or workflows from a document management system (for example) kept as evidence of requirement review?
- ☐ Is a CIP Senior Manager identified by name?
- ☐ If CIP Senior Manager changes is this documented within 30 days of the change?
- ☐ Is delegation of authority clearly documented if delegations are used?
- ☐ Is evidence retained for the standard three calendar years?
- ☐ Are methods to control physical access in place and documented?
- ☐ Are methods in place and documented to control access to Electronic Access Control or Monitoring System?
- ☐ Has one or more Cyber Security Incident Response Plan been implemented and documented?
- ☐ Is the plan tested and kept up-to-date?
- ☐ Is management commitment to the protection of its BES Cyber Systems periodically reaffirmed with annual review and approval of cyber security policies?

Learn how to strengthen your cybersecurity incident response plan here.

Part III: Cybersecurity Awareness

- ☐ Is a documented cyber security awareness program in place with security practices reinforced each calendar quarter for high and medium impact BES systems?
- ☐ Are presentations, instructor notes, handouts or other materials (for example) retained as evidence of training programs?
- ☐ What process is in place to confirm identity of personnel with access to BES cyber systems and their associated assets?
- ☐ Is a seven-year criminal history record check done to assess risk for personnel with access to BES cyber systems and their associated assets?
- ☐ Are contractors or service vendors with access to BES cyber systems and their associated assets also put through identity confirmation and criminal check procedures?
- ☐ Is documentation kept as evidence of personnel risk assessments?
- ☐ Is access to BES cyber systems and their associated assets authorized according to a process based on need?

How we can help:
Full Force Red Team Training and **Social Engineering Training**

- ☐ Are authorization records verified at least once each calendar quarter for those individuals with active electronic access or unescorted physical access?
- ☐ Does a process weigh the need for individuals' access to the designated storage locations for BES Cyber System Information at least once every 15 calendar months?
- ☐ Is a process established to remove an individual's unescorted physical access, interactive remote access, and access to designated storage locations within 24 hours of a termination action?
- ☐ Do reassignments or transfers revoke authorized electronic access to individual accounts and authorized unescorted physical access which are not deemed necessary by the end of the next calendar day?
- ☐ Is evidence of compliance retained for three calendar years?

While 24 hours is generally a sufficient window for revoking access, NERC-CIP recommends the "timeliest revocation of access possible." In other words, the sooner the better!

Part IV: Creating and Managing Perimeters

- ☐ Have electronic security perimeters been defined for all cyber assets connected to a network via routable protocol?
- ☐ Is external routable connectivity all through an identified Electronic Access Point (EAP)?
- ☐ Do both inbound and outbound network traffic require access limitations?
- ☐ Is authentication performed when establishing dial-up connectivity where technically feasible?
- ☐ Are there methods in place to detect known or suspected malicious inbound or outbound communications?
- ☐ Does network architecture utilize an intermediate system to prevent direct access to applicable cyber assets from a cyber asset initiating interactive remote access?
- ☐ Is encryption, terminating on the intermediate system, utilized for all interactive remote access sessions?
- ☐ Do all interactive remote access require multi-factor authentication?
- ☐ Does the entity maintain documented evidence of compliance?
- ☐ Is evidence retained for three calendar years?

This is one of the easiest but most under-used security measures. Passwords can be shared, stolen or guessed. Requiring a one-time token in addition to a password dramatically improves their effectiveness.

Part V: Protecting Physical Assets

- ☐ Is there a specific physical security plan to manage physical access to Bulk Electric System (BES) Cyber Systems?
- ☐ Do operational or procedural controls (such as card keys, special locks, security personnel) restrict physical access?
- ☐ Has at least one physical access control been implemented to restrict unauthorized, unescorted physical access into each applicable Physical Security Perimeter?
- ☐ Where technically feasible, have two physical controls been utilized?
- ☐ What systems are in place to monitor (such as alarm systems or human personnel) for unauthorized access through a physical access point or to a physical access control point?
- ☐ Will an alarm or alert issue within 15 minutes of detection in response to unauthorized access through a physical access or physical access control point?
- ☐ Are the individuals who should be notified of unauthorized access clearly identified in the incident response plan?
- ☐ Is there a log (computerized, video recording, or manually completed by personnel) recording entry into each Physical Security Perimeter identifying the individual, date and time of entry, and contact responsible for individual?
- ☐ Is the log retained for at least 90 calendar days?
- ☐ Is physical access to cabling and other nonprogrammable communication components (used for connection between cyber assets) located outside of a Physical Security Perimeter restricted and protected?
- ☐ Are all physical access control systems maintained and tested once every 24 calendar months?
- ☐ Is evidence of each requirement retained for three calendar years?

How we can help:
Physical Penetration Testing from RedTeam Security

Requirements Specific To Transmission Owners

- ☐ If a transmission owner, has an initial risk assessment of stations and substations been performed?
- ☐ Have subsequent risk assessments been performed at least once every 30 calendar months (if it has been identified that damage or inoperability at one or more of stations and substations could result in instability, uncontrolled separation, or cascading within an interconnection) or at least once every 60 calendar months (when damage or inoperability risk was not identified)?

- ☐ Has an unaffiliated third party verified the risk assessment performed by the transmission owner?
- ☐ Has transmission owner implemented procedures, such as the use of non-disclosure agreements, to protect sensitive or confidential information with the unaffiliated third-party verifier?
- ☐ Has transmission owner conducted an evaluation of the potential threats and vulnerabilities of a physical attack to each of its respective stations, substations, and primary control centers?
- ☐ Has owner developed and implemented a documented physical security plan?
- ☐ Are resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during transmission station, substation, primary control center evaluations?

Part VI: Protecting Systems

- ☐ Have steps been taken to disable or restrict network accessible ports only allowing those deemed necessary?
- ☐ Are protections documented against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media?
- ☐ Does a clear process manage patch tracking, evaluating, and installing cyber security patches?
- ☐ Are the sources of cyber security patches for applicable cyber assets identified?
- ☐ Is a process in place to ensure that cyber security patches for applicable cyber assets are consistently updated?
- ☐ Are security patches evaluated for applicability at least once every 35 calendar days?
- ☐ If applicable patches are not applied, is a dated mitigation plan created or an existing mitigation plan revised?
- ☐ Does the plan specify a timeframe for mitigation?
- ☐ Is the mitigation plan implemented within the timeframe specified in the plan?
- ☐ Are methods deployed to deter, detect, or prevent malicious code?
- ☐ Are processes in place for testing, installing, and update of signature and patterns?

At RedTeam, our motto is **ABP:** Always Be Patching! Security patch management is a proactive way to monitor and address security vulnerabilities in software before they can be exploited.

How we can help:
Network Penetration Testing from RedTeam Security

- ☐ Are successful login attempts, failed access and login attempts, and malicious code detected and logged?
- ☐ Are alerts generated for malicious code or failed access and login attempts detections?
- ☐ Are event logs retain, where technically feasible, for at least 90 consecutive calendar days?
- ☐ Are logged events reviewed or sampled at intervals no greater than 15 days to identify undetected cyber security incidents?
- ☐ Is authentication of interactive user access enforced?
- ☐ Are all known enabled, default, or other generic account types identified and inventoried?
- ☐ Are all individuals authorized to access shared accounts identified?
- ☐ Are all known default passwords changed?
- ☐ Is authentication for interactive user access enforcing password complexity?
- ☐ Are interactive uses obliged to change their passwords at least once every 15 calendar months?

Part VII: Incident Reporting and Response

- ☐ Is one or more process established to identify, classify, and respond to cyber security incidents?
- ☐ Are there one or more processes in place to determine if an identified cyber security incident is a reportable cyber security incident?
- ☐ Does procedure for reportable cyber security incidents require notification of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law, within one hour of the determination?
- ☐ Are rules and responsibilities for cyber security incident response groups or individuals defined?
- ☐ Have incident handling procedures been established?
- ☐ Are cyber security incident response plans tested at least once every 15 calendar months?
- ☐ Are documents related to reportable cyber security incidents (such as security logs, police reports, emails, forensic analysis results, restoration records, and post-incident review notes) retained?
- ☐ Are lessons learned and any updates made after a cyber security incident response plan or actual implementation documented and reported to each person or group with a defined role in the response plan?

While very important, an incident response plan is not set in stone. The best plan allows leeway for the incident responders to make the best tactical decisions under the specific circumstances of the incident.

- ☐ Is any change in role or responsibility for person or group defined in the response plan updated and reported to all those with defined roles within 60 days of the change?

Part VIII: Incident Recovery

- ☐ Have conditions for activation of a recovery plan been defined?
- ☐ Are responders' roles and responsibilities in recovery identified?
- ☐ Is there one or more process for the backup and storage of information required to recover BES Cyber System functionality?
- ☐ Is the successful completion of the backup verified using one or more processes?
- ☐ Are there procedures for data preservation which would not impede or restrict recovery?
- ☐ Are each of the recovery plans tested once every 15 calendar months?
- ☐ Does a test of a representative sample of information used to recover BES Cyber System functionality occur at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations?
- ☐ Are lessons learned and any updates made after a cyber security incident recovery documented and reported to each person or group with a defined role in the response plan?
- ☐ Is any change in role or responsibility for person or group defined in the recovery plan updated and reported to all those with defined roles within 60 days of the change?

Part IX: Change Management and Vulnerability Assessment

- ☐ Are changes that deviate from the existing baseline configuration authorized and documented?
- ☐ If a change deviates from the existing baseline configuration, is the baseline configuration updated as necessary within 30 calendar days of completing the change?

In a real-world context, these "changes to the baseline configuration" might include removable media like USB drives, which are frequently used to transfer information.

- ☐ Prior to implementing a change that deviates from the existing baseline configuration are potential impacts on cyber security controls determined?
- ☐ Are potential impacts on cyber security controls from change that deviates from the existing baseline configuration verified following the change?
- ☐ Are results of the verification documented?

- ☐ Where technically feasible is each change that deviates from the existing baseline configuration in the production environment tested in a test environment then production environment to ensure minimization of adverse effects?
- ☐ Are results of the testing and its environment documented?
- ☐ Are changes to the baseline configuration monitored at least once every 35 calendar days?
- ☐ Does entity document and investigate detected unauthorized changes once every 35 calendar days?
- ☐ Is a paper or active vulnerability assessment conducted at least once every 15 calendar months?
- ☐ Are results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments, including the planned date of completing the action plan, documented?

According to best practices, this vulnerability assessment should also be verified by an unaffiliated third party.

Part X: Information Protection

- ☐ Is BES Cyber System information identified and documented?
- ☐ Are procedures for secure handling of BES Cyber System information (including storage, transit, and use) recorded?
- ☐ Is action taken to prevent the unauthorized retrieval of BES Cyber System information from cyber asset data storage media prior to the release for reuse of applicable cyber assets?
- ☐ Prior to the disposal of applicable cyber assets is action taken to prevent the unauthorized retrieval of BES Cyber System information or to destroy the data storage media?

Part XI: Supply Chain Risk Management

- ☐ Has one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems been developed?
- ☐ Do processes for procuring BES Cyber Systems require vendor notification of vendor-identified incidents, coordinated responses to vendor-identified incidents, notification by vendors when remote or onsite access should no longer be granted to vendor representatives and disclosure by vendors of known vulnerabilities related to the products or services provided?

- ☐ Is software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System verified?
- ☐ Are controls coordinated for vendor-initiated interactive remote access and system-to-system remote access with vendors?
- ☐ Does entity review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) at least once every 15 calendar months?

About RedTeam Security

RedTeam Security has been a premiere provider of offensive information security services since 2008. In today's marketplace, companies are overwhelmed by security threats from hackers originating from all over the world. Studies show that the number of attacks against companies are increasing and at the same time becoming more complex. As a result of these attacks, the number of data breaches have cost companies tens of millions of dollars as well as grave reputational damage.

The security experts at RedTeam Security have years of experience helping organizations of all sizes identify and mitigate security vulnerabilities. Our highly trained consultants are published authors, hold multiple security certifications and speak at security conferences around the world.

Our portfolio of services includes:

Red Teaming
Network Penetration Testing
Application Penetration Testing
Physical Penetration Testing
Social Engineering
Compliance

It's easy to receive a customized security proposal for your financial institution. Just **fill out our scoping questionnaire**. You can also **schedule a consultation** with our team of experts or call us at **612-234-7848** for more information.

RedTeam
SECURITY CONSULTING

We educate. We identify. We inform. We reduce your attack surface.