North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

Version 5 CIP Cyber Security Standards

NERC CIP Version 5 is now fully enforced, with many more electric companies seeking to implement NERC CIP measures and looking to the market for automated solutions to help. For those that have been subject to the standard for years already, now is a good time to review solutions implemented at the time and re-evaluate the options for simpler and less expensive alternatives that are now available.

Demonstrating compliance can be a costly and time-consuming exercise, but Netwrix can help: Netwrix Change Tracker Enterprise 7.5 is the leading alternative to Tripwire, providing an easier to use and less expensive solution that provides a perfect solution to most NERC CIP controls.

Key Facts About NERC CIP v5

- The Critical Infrastructure Protection initiative of the North America Electric Reliability Corporation has helped protect Bulk Electric Systems (BES) and keep the lights on since its initial introduction in 2008.
- The increased proliferation of network-accessible Operational Technology (OT) and Industrial Control Systems (ICS) presents a much larger and more vulnerable attack surface than ever before.
- Cyber Security threats to BES generating facilities are now more widespread and with the growing sophistication of malware, APTs, ransomware and social-engineered Spear Phishing attacks, the need for robust operation of all security best practices is critical.
- Identity and Access Management, Configuration Hardening, Vulnerability Management, File Integrity Monitoring, Firewalling, Anti-Virus, Audit Trail Monitoring, Change and Configuration Management and Disaster Recovery along with Physical Security and documented processes and procedures are all mandated. Core security best

practices mandate the development of authorized baseline configurations for devices, against which any drift from this baseline can be reported. Approved changes must be authorized with a business justification documented. The key intent of this approach is to regularly review and question the configuration of all devices to ensure vulnerabilities are removed and the attack surface of all devices minimized.

- Networked SCADA, ICS and Intelligent electronic devices (IEDs), such as PLCs, Sensors, Controllers, and Relays are all potentially vulnerable to tampering and a cyber-attack. Access to these devices must, therefore, be carefully restricted and as such, monitoring of all open network ports is an essential dimension of NERC CIP compliance.

Find out which specific NERC CIP v5 requirements you can address with Netwrix Change Tracker

Netwrix Change Tracker 7.5 has been designed from the ground up to automatically operate these key security controls, recording configuration baselines for all devices then continuously monitoring and reporting any drift. Built-in Intelligent Change Control allows approval of changes recorded for all devices, whether in advance of changes being made or as a post-implementation review process. It is equipped with a distributed network port scanning capability specifically developed to address the exact requirements of the NERC CIP standard. Having the option to distribute scanning vantage points is important to both minimize network traffic but more critically to preserve internal firewalling integrity. Full port scans can be operated without compromise and without any need to make any special allowances in firewalling rules.

NERC CIP v5	Purpose	Netwrix Solution	Product		
			Change Tracker	Greenbone Enterprise	Log Tracker
CIP-002-3 R1, R2, R3	NERC Standards CIP-002-3 through CIP-009-3 provide a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.	Automated Network Discovery is provided by NNT Vulnerability Tracker to identify any Cyber Assets using a routable protocol. Any devices discovered will then be more deeply interrogated to establish other identification attributes and then, in turn, active Network Vulnerability Tests will be run to simulate Hacker activity and expose any exploitable vulnerabilities.		✓	
CIP-003-5 R1, R2, R3 and R4	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to mis operation or instability in the BES.	Monitoring and logging, Strategies for system hardening, Password policies including length, complexity, enforcement, prevention of brute force attempts, Recognition of Cyber Security Incidents, among others	✓	✓	✓

NERC CIP v5	Purpose	Netwrix Solution	Product		
			Change Tracker	Greenbone Enterprise	Log Tracker
CIP-004-3 R4	Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.	All User and System activity will be tracked and audit trails provided to ensure access is in-line with authorized privilege. Any new accounts or increased privilege will also be reported for review and approval.	✓		✓
CIP-005-5 R1, R2	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to mis operation or instability in the BES.	Use Netwrix Change Tracker to apply a secure and hardened configuration baseline. Netwrix is a Certified Vendor for CIS Benchmark Checklists and an Official OVAL Adopter, ensuring the most secure and effective configuration settings are used for firewalls and all other perimeter devices. Any changes are validated as approved, planned and accurately implemented, and any other drift from the secure baseline is reported in line with CIP 010-3.	✓		

NERC CIP v5	Purpose	Netwrix Solution	Product		
			Change Tracker	Greenbone Enterprise	Log Tracker
CIP-006-3c R1, R2	Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. The Responsible Entity shall maintain a physical security plan and implement the technical and procedural controls for monitoring physical access at all access points.	Physical access controls can be audited using automated audit trails and correlation rules. Configuration assessment and change control is automated using Netwrix Change Tracker. Any systems used to operate physical access controls will also need configuration hardening, change control and breach detection/anti-tampering measures to be enforced for the cyber elements	✓		✓
CIP-007-3 R1, R2, R3, R4, R5	Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing systems within the Electronic Security Perimeter(s). The Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets do not adversely affect existing cyber security controls. Changes include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	With Netwrix Change Tracker monitoring in place all changes are reported then analyzed and validated. Changes are assessed for risk based on knowledge within the system drawn from a range of trusted sources, such as your ITSM system planned change details, previously observed change patterns and file reputation whitelists like Netwrix F.A.S.T. Cloud. In addition, network and device changes can be actively tested using Greenbone Enterprise to probe for exploitable vulnerabilities. And finally, because new attack methods are always being derived by the cyber criminals, Netwrix also provides real-time breach detection, vital for the detection of any Stuxnet-style APT attacks.	✓	✓	

NERC CIP v5	Purpose	Netwrix Solution	Product		
			Change Tracker	Greenbone Enterprise	Log Tracker
CIP-008-3 R1, R2	Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.	Anomalous behaviors are detected via both change detection and log analysis. Changes are reviewed automatically against expected, planned and previously approved change patterns. Any Unplanned Changes are reported as potential security incidents and an investigation and review process is provided. All system and user activity are also baselined and analyzed using automated log correlation algorithms to identify unusual and suspicious behaviors. Audit trails are securely archived in line with NERC requirements for retrospective analysis and investigation.	✓		✓
CIP-010-3 R1, R2, R3, R4	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to mis operation or instability in the Bulk Electric System (BES).	Initial vulnerability assessments are performed using Certified CIS Benchmark hardening checklists and these can be tailored to match exactly the required hardened build standard for BES Cyber Systems. Any other source of automated compliance content such as OVAL or SCAP can also be used. This encompasses CIP-005 and CIP-007 Requirements. Greenbone Enterprise will then identify any missing patches and further remediation work necessary to maximize security.	✓	✓	

NERC CIP v5	Purpose	Netwrix Solution	Product		
			Change Tracker	Greenbone Enterprise	Log Tracker
CIP-011-1 R1	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to mis operation or instability in the BES.	Secure configuration standards can be assessed and records produced using Netwrix Change Tracker for BES Cyber System Information, including storage, transit, and use.	✓		

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social