The North American Electric Reliability Corporation (NERC) has defined reliability standards to help maintain and improve the reliability of North America's bulk power system.

NERC has the legal authority to enforce compliance with NERC Reliability Standards, which it achieves through a rigorous program of monitoring, audits and investigations, and the imposition of financial penalties and other enforcement actions for non-compliance.

The Critical Infrastructure Protection (CIP) standard is one of the NERC reliability standards. CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets.

Below you will find the CIP requirements for which ByStorm FileSure can help you to be CIP compliant:

CIP-003 Access Control	R5.1	Authority to grant access privileges must be known and monitored at all times	Most organizations have deployed an event log monitoring system to capture privileged group changes in order to address this requirement. But if the events are not logged in the first place, they obviously are not collected and there is no way to respond. FileSure operates outside of, and in addition to, the native-Windows security model and provides both file access auditing and file access control. Having a comprehensive record of all file accesses, moves, deletes, and changes can be critical for general IT use as well as CIP compliance. FileSure also provides access control (DLP – Data Loss Protection - blocking attempts to read/write/copy/move/etc.). FileSure can ensure file integrity and also ensure that even if someone is accidentally or inappropriately granted privileges via the standard Windows security model, that they cannot access files they shouldn't be accessing.
	R5.2	Access privileges to protected information must be controlled and access policies must be enforced	FileSure can record ACL changes, but the larger issue is enforcing access policy altogether. FileSure operates 'outside' the Windows authentication model, which means Domain Administrators don't have any inherent privileges in FileSure. So, if you set up a rule that says 'No one but Bob in Accounting can read an excel spreadsheet on the Accounting share,' Domain Admin Sam can't read it, even if Windows says he can. FileSure DOES NOT override the native-Windows security model. So if Windows determines someone does not have access, yet if FileSure rules are set such that the person should have access, they will NOT be granted access. In other words, your existing user/group permissions and ACLs will continue to do what you intended when it comes to denying access, however, FileSure will

			complement that and can block users and/or administrators that might have “slipped through the cracks.” Furthermore, FileSure can control where data can be copied and moved, which native-Windows ACLs do not address whatsoever.
	R6	Change Control and Configuration Management – All software and hardware changes must be tracked	With FileSure, all software changes are spotted and logged without having to turn on native-Windows file auditing! Any change to any file can be audited; you just have to configure the appropriate rules to identify the file, folder, or even better, the type of file. There is no need to go and touch each and every file or folder ACL. Even if you did, it would get changed or altered later by another administrator. Simply by setting rules in FileSure about the types of files that can be accessed and changed or moved, or the processes or users/groups allowed to do so, FileSure can enforce the policy regardless of the ACLs.

CIP-004 Access Privileges	R4.1	Access to Critical assets – Privileges to access electronic information on sensitive assets must be tracked and validated	FileSure is independent of native-Windows limitations when it comes to file auditing and file access. The FileSure system both audits file access and controls file access based on defined policy via a customizable rule-set. Sensitive assets, folders, and/or shares can be identified and FileSure can audit all accesses to these assets and alert on the critical asset access (file read) or maybe just when the asset is copied, moved, changed, or deleted. This is all customizable via the rule-set and can by applied by user, process, or type of file being accessed, and much more. FileSure also provides automated alerting via email, but of course, FileSure logged events can be monitored for and responded to via SCOM or other existing event log monitoring systems in order to appropriately notify management or security personnel as desired.
CIP-005 Electronic Security Perimeters	R1.5	Securing the access control and security monitoring systems – Must treat the access control system and the security monitoring software/systems as extremely critical assets and must know when any changes are made to the versions or installed components, when security system user permissions change, when security policies or rules change, or when anything on a system that these components reside changes	FileSure self-audits. All changes within FileSure are logged and can be tracked. You can also use FileSure to protect programs from being accessed by privileged users by blocking read access to the console program. For example, Bob can start RegEdit but no one else can. Sam can use FileSure, but no one else can. Sally can run MMC but no one else can; etc. This is possible because FileSure operates OUTSIDE the native-Windows security model; So while Windows says Sally has the authority to run RegEdit, FileSure says she doesn't. FileSure always wins! ☺ Automated emails can be utilized to notify management or security when such changes occur, however, as mentioned above, FileSure logged events can be monitored for and responded to via SCOM or other event log monitoring systems.
	R3.2	Monitoring Electronic Access – Must monitor for failed access authorization attempts and must investigate all unauthorized accesses	Authorization attempts (failures and successes) are usually logged and monitored at the domain controller and SCOM or some other event monitoring system is probably monitoring them. A larger concern would be an authorized user accessing files that they SHOULDN'T be accessing. Using FileSure to monitor all sensitive file accesses would catch this for you and enable you to investigate such an unauthorized access.
	R5.3	Electronic Access Log Retention – must be kept	FileSure logs are compressed and encrypted and are NOT stored in a commercial database since a DBA could alter

		for at least 90 days and ensure logs are not altered	them. FileSure uses SQLite whereby monthly blocks of logs are stored in separate files and in most cases never need to be groomed. FileSure can ensure that logs are not altered by only allowing the FileSure application to write to the FileSure log. When it comes to non-FileSure logs from other systems, FileSure can enforce that only the system that owns the log can write to the log. All others attempts to change or alter any log will be rejected. FileSure can be utilized to collect and store not only its own logs but also any log event written to the Windows event log. FileSure can also be configured to write to the Windows security log, the Windows application log, and Syslog, for organizations that have other methods of collecting, securing, and storing various logs.
CIP-007 Systems Security Management	R2	Ports and Services – Must make sure only those ports and services required for normal and emergency operation are enabled; by default ports and services are disabled	FileSure can be utilized to identify when firewall rule/configuration changes occur by auditing the Firewall configuration files/folder. Additionally, FileSure can ensure that only desired services are allowed to be installed (written) as a file in the first place via its white-listing feature. Most products accomplish this by identifying a service started event in the event log and then shutting any unapproved processes/services down. This is extremely dangerous because a worm or unapproved service could have long-since done its damage before it is detected and forced to shut down. FileSure doesn't let the unapproved application/service get installed on the computer in the first place! And even if it were to get installed, or maybe it was there before FileSure was installed, for a service to start, the executable (a file) must be read from storage. FileSure can block unapproved services from being read from the drive thus preventing unapproved applications from ever getting started.
	R4.1	Malicious Software Prevention – Must use anti-virus and malware prevention where technically feasible; where not technically feasible must utilize a compensating method of some type	FileSure complements anti-virus and anti-malware systems in that it can prevent the zero-day attacks that signature based systems cannot. FileSure does this through the use of an executable white-list as described for the previous requirement. FileSure can also be used as a compensating method altogether. Also, as described above for CIP-007 R2, white-lists can be utilized to keep unknown or unapproved applications/services from ever getting started.
	R4.2	AV and Anti-Malware signature updates - Must	FileSure can audit when signature files change. Regularly scheduled reports can be retained to prove that they

		regularly update anti-virus and malware prevention signatures	have been updated/changed and email alerts can be utilized to notify others that these updates occurred.
	R5.1	User account access activity – Must be logged and saved for at least 90 days	SCOM/ACS, or your event log monitoring system, will typically handle much of what is needed to meet this requirement, however, session changes are not logged. FileSure does detect and audit session changes…for example, when a computer is connected to and remote controlled, locked or physically connected/unlocked, etc.. Of course, FileSure is also able to selectively pick out any event from the Windows event logs and will store them in with its own events in its encrypted and compressed data store for both short-term viewing and long term archival.
	R6	Security Status Monitoring – Automated systems must be used to monitor security events, alert on incidents, retain logs for 90 days, and review logs and retain proof of review	FileSure logs to its own private secure log for long-term retention of these logs, forensic search/review, threshold alerting, and reporting. FileSure can optionally be configured to write to the Windows application log, Windows security log, and via Syslog in order to integrate with and extend the value of existing event log collection, monitoring, and archival systems. FileSure can also be used to collect specific event(s), as desired, from the Windows security event log and store them in with its own events in its encrypted and compressed data store for both short-term viewing and long term archival. FileSure is able to alert via email when specific events (incidents) occur and can be used to review these events for forensic investigations.

About ByStorm Software

ByStorm Software, founded in 2003, provides IT organizations with low footprint, yet comprehensive file auditing, data loss protection, and compliance enabling alerting and reporting for the Microsoft Windows platform. ByStorm Software is committed to ensuring that our solutions install and begin providing value within minutes and that our customers are empowered to meet PCI, HIPAA, NERC/CIP, NIST, SOX, and other security and compliance mandates.

Some of our customers include: