NERC-CIP compliance card

SOPHOS

TThe North American Electric Reliability Corporation (NERC) is an international regulatory organization that develops and enforces standards to reduce risks to the reliability and security of the power grid infrastructure. In 2008, NERC developed the Critical Infrastructure Protection (CIP) standards compliance framework to mitigate cybersecurity attacks on the Bulk Electric System (BES). The NERC-CIP standards were developed to protect the physical and cyber assets of North America's power bulk system, essential for its security and infrastructure protection. Non-compliance with NERC-CIP standards may lead to penalties of up to $1 million per day; which is why most industrial control system organizations invest substantial time and critical resources into maintaining compliance with the standards.

STANDARD	REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
CIP-002-5.1a **Cyber Security - BES Cyber System Categorization**	*To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cybersecurity requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.*	**Sophos Cloud Optix**	Provides accurate inventories and network topologies visualizations of an organization's cloud resources across all production environments including hosts, containers, serverless, IAM, network security groups and more while adding additional visualizations for traffic flows, and deployment of Sophos Cloud workload agents and Sophos virtual firewalls within the environment. With inventory in place, Cloud Optix scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
CIP-003-7 **Cyber Security - Security Management Controls**	*To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)*	**All Sophos products**	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Intercept X with XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
CIP-004-6 **Cyber Security - Personnel & Training**	*To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.*	**All Sophos products**	Sophos' user-identity based policy technology allows user level controls over network resources and other organization's assets.
		Sophos Central	Configurable role-based administration provides granular control of administrator privileges. Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Zero Trust Network Access	Continuously validates user identity, device health, and compliance before granting access to applications and data.

CIP-005-5 **Cyber Security - Electronic Security Parameters**	*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 misoperation or instability in the BES.*	**Sophos Firewall**	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Email **Sophos Firewall**	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam. Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
		Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
		Security Consulting	Sophos offers penetration testing and vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.
		Sophos Intercept X Advanced with EDR **Sophos Intercept X for Server**	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Get a root cause analysis of an attack with complete visibility on the how and where of the attack along with recommendations on what your next steps should be.
		Sophos Managed Threat Response	Proactive 24/7 threat hunting by elite team of threat analysts initiates actions to remotely disrupt, contain, and neutralize threats on your behalf to stop even the most sophisticated threats. Investigates detections from Sophos-protected endpoints, networks, and cloud platforms on customers' behalf to validate if adversarial activity or an active threat exists. Depending on the customer preference, notification of findings and recommendations are shared or an immediate response to the threat is initiated. Performs thorough investigations of detections, telemetry, and other datasets (observables) to derive indicators for use in threat hunts and targeted response actions. Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.
		Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.

CIP-007-6 **Cyber Security - System Security Management**	*To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).*	Sophos Cloud Optix	AI-powered monitoring instantly identifies suspicious console login events, API calls, and assumed-role API calls that suggest shared or stolen user credentials are being used by an attacker remotely to gain unauthorized access. Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Sophos Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Administrators are instructed to change the default password of the "admin" user immediately after deployment. An alert is displayed when the default password for the super administrator is not changed.
		Sophos Intercept X for Server	Prevents unauthorized applications from running with Server Protection, automatically scanning your system for known good applications, and whitelisting only those applications.
		Sophos Managed Threat Response	Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.
		Sophos Device Encryption	Complete data protection solution that is effective across multiple platforms and devices, including mobile and traditional endpoints. Protect data at rest with full disk encryption. Location-based file encryption protects data in motion and follows the file wherever it may go – for example, via email, uploaded to cloud storage, or copied to removable devices. Application-based (synchronized) encryption encrypts data by default as soon as it is created.
		Sophos Intercept X Advanced with EDR Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications. Device Control allows admins to control the use of removable media through policy settings. Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code.
		All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response. All administrative actions are logged and available for reporting and audits.
CIP-008-5 **Cyber Security - Incident Reporting and Response Planning**	*To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements*	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response. All administrative actions are logged and available for reporting and audits.
		Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
		Sophos Intercept X Advanced with EDR Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.
		Sophos Cloud Optix	Establishes guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities.
CIP-009-6 **Cyber Security - Recovery Plans for BES Cyber Systems**	*To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.*	Intercept X with XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or master boot record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos Managed Threat Response	Monitors and investigates detections from Sophos endpoint, network, and cloud platform solutions to identify, investigate, contain, and neutralize active threats.

CIP-010-2 **Cyber Security -Configuration Change Management and Vulnerability Assessments**	*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 misoperation or instability in the Bulk Electric System (BES).*	**Sophos Central**	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Sophos Mobile	Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Cloud Optix	AI-powered monitoring instantly identifies suspicious console login events, API calls, and assumed-role API calls that suggest shared or stolen user credentials are being used by an attacker remotely to gain unauthorized access. Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.
		All Sophos products	All administrative actions are logged and available for reporting and audits.
		Security Consulting	Sophos offers penetration testing and vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.
CIP-011-2 **Cyber Security – Information Protection**	*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 misoperation or instability in the Bulk Electric System (BES).*	**Sophos Zero-trust Network Access**	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Firewall	Sophos XG Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
		Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection safeguards your users and devices from malicious content and apps.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance. Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Email	Delivers data loss prevention and content control that provide advanced data breach prevention with policy-based email encryption.
CIP-012-1 **Cyber Security – Communications between Control Centers**	*To mitigate the risk of unauthorized disclosures and respond to attempts to modify the real-time assessment and monitoring data transmitted between control centers.*	**Sophos Email**	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos SafeGuard Encryption	Encrypts data on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted remains encrypted as files move across the network.

CIP-013-1 **Cyber Security - Supply Chain Risk Management**	*To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.*	Sophos Intercept X with EDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful EDR functionality enables automatic identification of suspicious activity, prioritizes threat indicators, and quickly searches for potential threats across endpoint and servers.
		Sophos Managed Threat Response (MTR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
		Sophos Zero-trust Network Access	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2021-07-08 RC-NA (MP)