SOLUTION BRIEF

Security of Critical Infrastructure Act (SOCI) 2018

The Security of Critical Infrastructure Act (SOCI) 2018 outlines the legal obligations for those who own, operate, or have direct interests in critical infrastructure assets. It is a legislative framework designed to promote and enhance the protection of critical infrastructure, which consists of 11 sectors, from cyber threats. The act is aimed to safeguard vital systems and assets that are essential for the functioning of a nation's economy, security, and public health.

Key provisions of the SOCI 2018 include:

1

Identification of Critical Infrastructure

The act outlines procedures for identifying and categorizing critical infrastructure sectors such as energy, transportation, communication, healthcare, and finance.

2

Risk Assessment and Management

Organizations must conduct regular and scheduled risk assessments to identify vulnerabilities and threats to critical infrastructure, and implement appropriate risk identification and mitigation strategies.

3

Cybersecurity Standards and Best Practices

SOCI 2018 establishes cybersecurity standards, best practices and specific actions that organizations must adhere to in order to protect critical infrastructure from cyber threats.

4

Incident Reporting and Response

The act outlines requirements for incident reporting and response protocols to ensure timely and effective handling of cyber incidents affecting critical infrastructure.

5

Information Sharing and Collaboration

Promotion of information sharing and collaboration among government agencies, private sector entities, and other stakeholders to enhance cybersecurity resilience across critical infrastructure sectors.

In the context of the SOCI Act, organizations are not only encouraged but may also be legally obligated to adopt an approved cybersecurity framework. These frameworks, such as the Essential Eight developed by the Australian Cyber Security Centre, NIST, ISO 27001 & ISO 27002, SOC2, NERC-CIP, HIPAA, GDPR, and FISMA, provide a structured approach to managing cybersecurity risks. They offer guidelines for protecting valuable assets, identifying and managing risks, and recovering from cybersecurity incidents.

Implementing these frameworks demonstrates an organization's commitment to cybersecurity, builds trust with stakeholders, and ensures compliance with relevant laws and regulations. While the adoption of a specific cybersecurity framework may not be officially mandated across all sectors, it is increasingly recognized as a best practice and may be required by industry-specific regulations. Therefore, organizations are strongly advised to select and implement a cybersecurity framework that aligns with their needs and ensures compliance with the SOCI Act.

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time. Armis Centrix™, the Armis cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, and manages billions of assets around the world in real time. It can help organizations align with the Security of Critical Infrastructure Act (SOCI) 2018 through its comprehensive cybersecurity solution tailored for critical infrastructure protection.

Aligning With SOCI 2018

Comprehensive Asset Inventory

- **Visibility** - Armis Centrix™ discovers and continuously monitors all assets across the organization, regardless of their location or connection type or whether the device is physical or virtual.
- **Deep Situational Awareness** - It provides detailed information on each asset, such as manufacturer, model, operating system, software, and firmware versions, crucial for understanding the attack surface and identifying vulnerabilities.

Vulnerability Assessment and Management

- **Continuous Monitoring** - Armis Centrix™ continuously assesses the security posture of all assets, identifying, deduplicating, assigning and mitigating vulnerabilities and risk in real-time.
- **Vulnerability Prioritization** - It helps organizations prioritize vulnerabilities and other security findings based on risk level, and criticality of the asset to business operations.

Threat Detection and Response

- **Threat Detection** - Armis Centrix™ leverages AI/ML to detect and alert on policy violations and anomalous behavior, such as unexpected network traffic, unauthorized access attempts, and suspicious activity.
- **Proactive Threat Identification** - Armis Early Warning capabilities can help find the vulnerabilities and threats while still in the formulation stage and ahead of CISA KEV. This proactive response preempts the attack and enables the next bullet to happen.
- **Rapid Response** - It enables organizations to quickly respond to security incidents, minimizing the impact and reducing downtime.

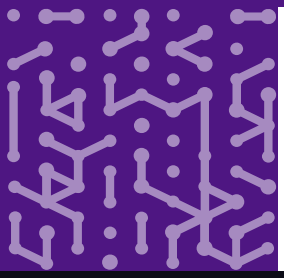
Compliance Monitoring & Reporting

- **Data Collection and Analysis** - Armis Centrix™ collects and analyzes detailed data related to asset inventory, behavior vulnerability management, and threats.
- **Reporting and Documentation** - It provides reports and documentation that can be used to proactively demonstrate compliance with the SOCI Act's requirements, such as asset registration and incident reporting.

Information Sharing and Collaboration

Armis facilitates collaborative threat intelligence sharing by pulling as well as sharing information with the other security products that are part of the organization's tech stack.This integrated approach eliminates security siloes and blind spots while also enabling the organization to benefit from collective insights and collective defense strategies. Furthermore, and as part of our threat intelligence engine, organizations will can benefit from information appending and expected behavior of each and every asset to bolster their cyber awareness and resilience.

By leveraging Armis Centrix™, organizations can strengthen their cybersecurity posture and align with the requirements of the Security of Critical Infrastructure Act (SOCI) 2018 to better protect critical infrastructure from cyber threats and unacceptable risk.



Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial