SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

Securing Australia's Critical Infrastructure

Mapping Dragos and NP-View Capabilities to SOCI Act 2024 Requirements

The Security of Critical Infrastructure (SOCI) Act 2018, recently updated in 2024, is an Australian legislation designed to enhance the security and resilience of critical infrastructure across 11 sectors, introducing risk management obligations and government assistance provisions.

Dragos, with its comprehensive OT security platform and threat intelligence capabilities, helps organizations meet SOCI requirements by providing asset visibility, threat detection, and incident response for industrial control systems. NP-View complements these efforts by offering network segmentation analysis and policy verification, enabling companies to demonstrate compliance with SOCI's security governance requirements and enhance their overall cybersecurity posture.

Latest SOCI Act Updates

The Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 introduced several key changes:

1

Expanded Scope

Clarified that data storage systems holding business-critical data for critical infrastructure assets are part of the critical infrastructure asset.

2

Broadened Government Powers

Extended government assistance powers to include non-cyber incidents, such as terrorist attacks and natural disasters.

3

Enhanced Information Sharing

Updated protected information and disclosure provisions to facilitate more effective information sharing.

4

Risk Management Program Oversight

Introduced powers for regulators to direct entities to address serious deficiencies in their risk management programs.

5

Telecommunications Security

Consolidated security requirements for critical telecommunications assets into the SOCI Act.

6

Simplified Notifications

Streamlined the process for notifying declarations of systems of national significance (SoNS).

Dragos Capabilities Mapped to SOCI Requirements

The following information outlines the domains of the Security of Critical Infrastructure (SOCI) Act 2018 in Australia, incorporating the latest amendments introduced by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024. It describes their relevance to operational security and how the Dragos suite of offerings can help customers meet SOCI requirements.

1 CRITICAL INFRASTRUCTURE ASSET IDENTIFICATION

Description	Relevance	Dragos Capabilities
Identifying and classifying assets that are critical to national security and economic prosperity, including data storage systems holding business-critical data.	Essential for prioritizing protection efforts and resource allocation.	• **Dragos Platform:** Provides comprehensive asset identification and inventory for OT environments, including data storage systems. • **NP-View:** Offers network visualization to identify critical assets and their connections, helping to map data flows.

2 RISK MANAGEMENT

Description	Relevance	Dragos Capabilities
Implementing processes to identify, assess, and mitigate risks to critical infrastructure, with new regulatory powers to address serious deficiencies.	Crucial for maintaining the resilience and security of critical systems.	• **Dragos Platform:** Offers vulnerability assessment and risk scoring for OT assets, aligning with enhanced risk management requirements. • **Dragos Services:** Provides risk assessments and mitigation strategies, helping to address potential deficiencies proactively. • **NP-View:** Assists in identifying network-related risks and segmentation issues, supporting comprehensive risk management.

3 CYBERSECURITY AND ALL-HAZARDS APPROACH

Description	Relevance	Dragos Capabilities
Protecting critical infrastructure from cyber threats and other hazards, including non-cyber incidents.	Essential for maintaining the integrity and availability of critical systems across various threat scenarios.	• **Dragos Platform:** Provides threat detection, incident response, and vulnerability management for OT environments, adaptable to various types of incidents. • **NP-View:** Offers network visualization to identify critical assets and their connections, helping to map data flows.

4 INFORMATION SHARING AND COLLABORATION

Description	Relevance	Dragos Capabilities
Facilitating the exchange of threat intelligence and best practices among critical infrastructure operators, government agencies, and across industries.	Enhances collective defense capabilities and promotes a coordinated response to threats.	• **Dragos Neighborhood Keeper:** Enables anonymous information sharing among participants, aligning with the Act's enhanced information sharing provisions. • **Dragos Intelligence/WorldView:** Provides actionable threat intelligence that can be shared within organizations and across sectors, supporting the new disclosure framework.

5 INCIDENT RESPONSE AND RECOVERY

Description	Relevance	Dragos Capabilities
Developing and implementing plans to respond to and recover from security incidents, including non-cyber events.	Ensures rapid and effective response to minimize the impact of security breaches and other hazards.	• **Dragos Platform:** Offers incident response capabilities and playbooks, adaptable to various types of incidents. • **Dragos Services:** Provides incident response support and tabletop exercises, including scenarios for non-cyber incidents.

6 TELECOMMUNICATIONS SECURITY

Description	Relevance	Dragos Capabilities
Implementing enhanced security measures for critical telecommunications assets, as consolidated in the SOCI Act.	Ensures the resilience and security of vital communication infrastructure.	While Dragos and NP-View primarily focus on OT environments, their network analysis and security capabilities can support the overall security posture of organizations operating critical telecommunications assets.

7 COMPLIANCE AND REPORTING

Description	Relevance	Dragos Capabilities
Meeting regulatory requirements and reporting on the security posture of critical infrastructure assets, including addressing regulator-identified deficiencies.	Ensures adherence to legal obligations and promotes transparency.	• **Dragos Platform:** Generates reports on security posture, incidents, and compliance status, helping to address regulatory requirements and demonstrate ongoing compliance. • **NP-View:** Provides documentation and visualization of network segmentation for compliance purposes, supporting the demonstration of security measures.

Enhanced Cybersecurity Requirements for SOCI SoNS in Australia

Systems of National Significance (SoNS) Qualification

Systems of National Significance (SoNS) represent a critical subset of Australia's infrastructure assets, identified based on their paramount importance to national security and economic stability. The qualification process for SoNS is rigorous and considers several key factors:

- **Asset Type:**
  Must be classified as a critical infrastructure asset
- **Sector Coverage:**
  Spans 11 essential sectors including communications, financial services, data storage, defence, energy, and healthcare
- **Interdependence:**
  The nature and extent of the asset's connections with other critical infrastructure
- **Ministerial Declaration:**
  The Minister for Home Affairs must be satisfied of the asset's national significance

Organizations operating within these sectors should conduct a thorough self-assessment against these criteria to determine their potential SoNS status.Amendment (Enhanced Response and Prevention) Act 2024. It describes their relevance to operational security and how the Dragos suite of offerings can help customers meet SOCI requirements.

Enhanced Cyber Security Obligations (ECSO) Framework

SoNS are subject to Enhanced Cyber Security Obligations (ECSO), a comprehensive framework designed to bolster the cybersecurity posture of these critical assets. The ECSO framework comprises four core components, each with specific requirements:

- Enhanced Cyber Security Obligations (ECSO) Framework
- SoNS are subject to Enhanced Cyber Security Obligations (ECSO), a comprehensive framework designed to bolster the cybersecurity posture of these critical assets. The ECSO framework comprises four core components, each with specific requirements:
- Cyber Security Incident Response Plans
- Develop and maintain comprehensive response protocols
- Integrate with existing business continuity plans
- Submit plans to the Secretary of the Department of Home Affairs
- Conduct regular reviews and updates *(at least annually)*
- Cyber Security Exercises
- Undertake regular testing of response capabilities
- Exercises may be discussion-based, tabletop, or operational
- Submit an evaluation report within 30 days of exercise completion
- Implement improvements based on exercise outcomes
- Vulnerability Assessments
- Conduct systematic identification of system weaknesses
- Assessments can be documentation-based, hands-on, or use automated scanning tools
- Submit a vulnerability assessment report within 30 days of completion

- Develop and implement remediation plans for identified vulnerabilities
- System Information Provision
- Establish mechanisms for real-time threat monitoring
- Comply with periodic or event-based reporting as specified
- Potentially install government-provided software for information sharing
- Ensure all shared information excludes personal data as per the Privacy Act 1988
- The application of ECSO is tailored to each SoNS based on factors such as compliance costs, reasonableness, and existing regulatory obligations.

Book a Demo Today: Leverage the Dragos Platform and NP-View to Meet SOCI Requirements

The 2024 amendments to the SOCI Act represent a significant evolution in Australia's approach to critical infrastructure protection. The Dragos suite of offerings provides comprehensive capabilities to address the key domains of the updated SOCI Act. By leveraging Dragos, organizations can enhance their critical infrastructure protection, meet the new regulatory requirements, and improve their overall security posture in line with the all-hazards approach emphasized in the latest legislation.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo   Contact Us