SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

The Australian Energy Sector Cyber Security Framework (AESCSF)

Dragos and NP-View Provide an Integrated Approach to Energy Sector Cybersecurity

The AESCSF is a cybersecurity framework developed and tailored to the Australian energy sector. The purpose of the framework is to enable energy participants across the electricity, gas and liquid fuels subsectors to assess, evaluate, prioritise, and improve their cybersecurity capability and maturity. It comprises a set of security practices relevant to Australia's energy sector and a methodology for organisations to assess their criticality with respect to the Australian energy system and their maturity against the security practices. The AESCSF is focused on cybersecurity maturity and describes what your organisation should strive to achieve, not how it should be achieved.

Dragos offers a suite of OT-specific security solutions, including threat detection, response, and actionable intelligence, while the NP-View software provides powerful network visualization and segmentation analysis tools. Together, these solutions enable energy companies to meet AESCSF guidance across key domains such as risk management, threat detection, and incident response, significantly enhancing their overall cybersecurity posture and resilience against evolving cyber threats.

AESCSF applies to a broad spectrum of entities in the Australian energy sector, encompassing electricity generation, transmission, distribution, gas production, energy retail, market operations, and critical service providers.

AESCSF Requirements: How Dragos and NP-View Support Australian Energy Sector Cybersecurity

This table provides an overview of the Australian Energy Sector Cyber Security Framework (AESCSF) domains, their relevance to operational security, and how the Dragos suite of offerings and NP-View software can help meet these requirements.

1 RISK MANAGEMENT (RISK)

Description	Relevance to Operational Security	Dragos Capabilities

Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risks to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.	Effective risk management is foundational to operational security, ensuring that resources are allocated appropriately to address the most critical threats and vulnerabilities.	• **Dragos Platform:** Provides comprehensive asset visibility and vulnerability assessment, helping identify and prioritize risks in OT environments.
		• **NP-View:** Network segmentation analysis to identify potential vulnerabilities in network architecture. Firewall rule analysis to ensure proper segmentation and access controls are in place, reducing overall risk.
		• **Dragos Intelligence/WorldView:**
		  • Offers threat intelligence specific to industrial control systems, informing risk assessments and mitigation strategies.
		  • Provides tailored OT threat intelligence reports and insights to inform a risk management strategy, including understanding adversary behaviors, emerging vulnerabilities, and industry-specific risks.
		  • Integrates with asset visibility in the Dragos Platform to correlate vulnerabilities with active threats, identifying risks tied to adversary tactics and providing tailored recommendations to mitigate high-impact vulnerabilities.

		• Includes analysis of threat prevalence, adversary capabilities, and vulnerabilities impacting OT, enabling organizations to prioritize risks based on operational and safety impacts. • Provides actionable intelligence, including indicators of compromise (IOCs) and risk-based mitigation strategies, helping organizations select the most effective responses aligned with operational needs. • **Dragos Services:** Risk assessments and tabletop exercises to help organizations identify and address cybersecurity risks.

2 ASSET, CHANGE, AND CONFIGURATION MANAGEMENT (ASSET)

Description	Relevance to Operational Security	Dragos Capabilities
Manage the organization's operational technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.	Maintaining an accurate inventory of assets and their configurations is crucial for identifying vulnerabilities, managing patches, and responding to incidents effectively.	• **Dragos Platform:** Provides automated asset discovery and inventory management for OT environments. • **NP-View:** Automated network topology mapping to visualize and manage OT network assets. Configuration analysis to ensure assets are properly configured according to security best practices. • **Dragos Services:** Offers asset inventory and management services to help organizations establish and maintain accurate asset databases.

3 IDENTITY AND ACCESS MANAGEMENT (ACCESS)

Description	Relevance to Operational Security	Dragos Capabilities
Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.	Proper identity and access management prevents unauthorized access to critical systems and helps maintain the principle of least privilege.	• **Dragos Platform:** Monitors for unauthorized access attempts and provides visibility into user activities within OT environments. • **NP-View:** Access path analysis to identify and validate authorized communication paths between network zones. Firewall rule analysis to ensure access controls are properly implemented and maintained. • **Dragos Services:** Offers guidance on implementing effective identity and access management practices in industrial environments.

4 THREAT AND VULNERABILITY MANAGEMENT (THREAT)

Description	Relevance to Operational Security	Dragos Capabilities

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the organization's infrastructure and organizational objectives.	Proactive threat and vulnerability management helps organizations stay ahead of potential attacks and minimize the impact of successful breaches.	• **Dragos Platform:** Provides continuous threat detection and vulnerability assessment for OT environments.
		• **NP-View:** Vulnerability assessment through network configuration analysis. Identification of potential attack paths through the network.
		• **Dragos Intelligence/WorldView:**
		  • Offers actionable threat intelligence specific to industrial control systems.
		  • Continuously monitors the global OT threat landscape and delivers intelligence to organizations, ensuring they are aware of and prepared for emerging threats.
		  • Tracks OT threat groups and their tactics, techniques, and procedures (TTPs), delivering

		detailed profiles to help organizations develop comprehensive threat models and defense strategies. • Provides prioritized intelligence, highlighting the most critical threats to industrial operations, including ransomware trends and state-sponsored adversaries targeting specific sectors. • Facilitates threat information sharing through curated reports, IOCs, and participation in information-sharing networks like ISACs, ensuring stakeholders stay aligned. • **Dragos Neighborhood Keeper:** Enables anonymous threat sharing among peers in the energy sector.

5 SITUATIONAL AWARENESS (SITUATION)

Description	Relevance to Operational Security	Dragos Capabilities

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from other model domains, to form a common operating picture (COP).	Situational awareness enables organizations to quickly detect and respond to potential threats or anomalies in their operational environment.	• **Dragos Platform:** Provides real-time monitoring and alerting for OT environments, contributing to a comprehensive common operating picture.
		• **NP-View:** Real-time network visualization to maintain awareness of network state and changes. Continuous monitoring of network configurations and segmentation.
		• **Dragos Intelligence/WorldView:**
		  • Offers contextual threat intelligence to enhance situational awareness.
		  • Delivers actionable intelligence that integrates with the Dragos Platform and existing third-party tools, providing a clear understanding of OT cybersecurity state across the organization.

		• Supplies OT-specific IOCs and threat intelligence insights for integration into third-party monitoring tools, enabling effective detection of early-stage threats before they pivot to OT networks. • Provides regular updates to adversary profiles and emerging threats to ensure monitoring activities stay relevant to current threats. • **Dragos Neighborhood Keeper:** Enables anonymous sharing of threat data to improve collective situational awareness across the energy sector.

6 EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS (RESPONSE)

Description	Relevance to Operational Security	Dragos Capabilities
Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.	Effective incident response and continuity planning ensure that organizations can quickly detect, contain, and recover from cybersecurity incidents while maintaining critical operations.	• **Dragos Platform:** Provides incident detection, investigation, and response capabilities for OT environments. • **NP-View:** Rapid analysis of network configurations to support incident investigation and response. Identification of potential attack paths to aid in containment and mitigation efforts. • **Dragos Services:** Offers incident response planning, tabletop exercises, and on-call incident response support. • **Dragos Academy:** Provides training on incident response in industrial environments. • **Dragos Intelligence/WorldView:** Provides actionable intelligence, including IOCs and mitigation strategies, to support effective incident response.

7 SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT (THIRD-PARTIES)

Description	Relevance to Operational Security	Dragos Capabilities

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives..	Managing supply chain risks is crucial for maintaining the integrity and security of industrial control systems and their components.	• **Dragos Platform:** Helps identify and monitor third-party connections and activities within OT environments.
		• **NP-View:** Analysis of network connections and data flows to identify and monitor third-party access points. Verification of proper network segmentation for external connections.
		• **Dragos Intelligence/WorldView:**
		  • Provides intelligence on supply chain threats and vulnerabilities specific to industrial control systems.
		  • Enriches organizational data by integrating insights from third-party sources and ISACs.

8 WORKFORCE MANAGEMENT (WORKFORCE)

Description	Relevance to OT Security	Dragos Capabilities
Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.	A well-trained and security-aware workforce is essential for maintaining operational security and preventing human-error-induced incidents.	• **Dragos Academy:** Offers comprehensive training programs on industrial cybersecurity. • **Dragos Services:** Provides customized training and workforce development services. • **Dragos Intelligence/WorldView:** Offers regular threat briefings and intelligence updates to keep the workforce informed about current OT threats and trends.

9 CYBERSECURITY PROGRAM MANAGEMENT (PROGRAM)

Description	Relevance to Operational Security	Dragos Capabilities
Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.	A well-managed cybersecurity program ensures that security efforts are aligned with business objectives and that resources are allocated effectively to protect critical assets.	• **NP-View:** Comprehensive reporting and analytics to support cybersecurity program management and decision-making. • **Dragos Services:** Offers strategic consulting to help organizations develop and mature their industrial cybersecurity programs. • **Dragos Intelligence/WorldView:** Provides strategic threat intelligence to inform program planning and resource allocation.

10 CYBER SECURITY ARCHITECTURE (ARCHITECTURE)

Description	Relevance to Operational Security	Dragos Capabilities
Establish and maintain a cybersecurity architecture that provides a framework for the organization's cybersecurity activities and aligns with industry standards and best practices.	A well-designed security architecture provides a foundation for implementing effective security controls and maintaining operational resilience.	• **Dragos Platform:** Supports the implementation of defense-in-depth strategies for OT environments. • **NP-View:** Network architecture visualization and analysis to support the design and implementation of secure network architectures. Continuous monitoring of network segmentation and zoning to ensure adherence to architectural standards. • **Dragos Services:** Offers architectural review and design services to help organizations implement secure OT architectures. • **Dragos Intelligence/WorldView:** Provides insights on emerging threats and attack vectors to inform the development and evolution of security architectures.

11 AUSTRALIAN PRIVACY MANAGEMENT (APM)

Description	Relevance to Operational Security	Dragos Capabilities
Manage personal information in a way that is consistent with Australian Privacy Principles and the Office of the Australian Information Commissioner's privacy management framework.	Proper management of personal information is crucial for maintaining compliance and protecting sensitive data from unauthorized access or breaches.	• **Dragos Platform:** Provides data protection capabilities and access controls to support privacy requirements. • **NP-View:** Network segmentation analysis to ensure proper isolation of systems containing personal information. Access path analysis to verify that personal information is only accessible to authorized entities. • **Dragos Services:** Offers guidance on implementing privacy controls in industrial environments. • **Dragos Intelligence/WorldView:** Provides insights on privacy-related threats and best practices specific to the energy sector.

How to Use the Framework

The AESCSF implementation process involves several key steps:

1. **Assess your organization's criticality:**
   Determine your importance within the energy sector and the potential impact of a cybersecurity incident.
2. **Select the appropriate assessment model:**
   Based on your organization's criticality, choose the most suitable assessment approach.
3. **Determine the assets in scope for the assessment:**
   Identify and prioritize the critical assets and systems that need to be evaluated.
4. **Complete the assessment:**
   Conduct a thorough evaluation of the organization's cybersecurity practices against the AESCSF requirements.
5. **Review and improve:**
   After the assessment, analyze the results and identify gaps. Book a demo with Dragos to develop improvement plans.

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