The procurement of network security equipment should be undertaken by the relevant authority organization

Article Overview

The procurement of network security equipment should be undertaken by the organization responsible for the network or service, guided by relevant regulatory authorities and security frameworks.

Responsible Authority

The primary responsibility for procuring network security equipment lies with the organization or entity operating the network, such as a telecommunications provider, critical infrastructure operator, or enterprise IT department. These organizations must ensure that equipment meets security requirements, aligns with risk management policies, and supports the continuity of critical services . Regulatory and advisory bodies provide guidance and oversight:

o National Cyber Security Centre (NCSC): Offers guidance for assessing the security of network equipment, particularly for critical services, and recommends ongoing evaluation of vendor security practices .
o European Union Agency for Cybersecurity (ENISA): Provides practical guidelines for ICT procurement, helping organizations manage security risks in procured products or outsourced services .
o GSMA NESAS (Network Equipment Security Assurance Scheme): Establishes an industry-wide security assurance framework for network equipment, ensuring compliance with global security standards .
o Information Commissioner's Office (ICO): Advises on due diligence, risk assessment, and contractual enforcement of information and cyber security requirements when engaging IT suppliers .

Key Responsibilities in Procurement

Organizations undertaking procurement should:
o Conduct risk assessments to identify potential security threats associated with vendors and equipment .
o Perform due diligence on suppliers, including reviewing security policies, certifications, and past performance .
o Include enforceable security requirements in contracts, ensuring vendors comply with the organization's security objectives .
o Monitor and audit vendor security throughout the lifecycle of the equipment to maintain ongoing compliance and resilience .
o Align with regulatory frameworks such as the Telecommunications (Security) Act, Electronic Communications Security Measures, or other national and international standards .

Conclusion

The procurement of network security equipment should be undertaken by the relevant authority organization

While the organization operating the network is directly responsible for procurement, it should do so under the guidance of regulatory authorities and industry standards to ensure security, compliance, and resilience. This collaborative approach mitigates risks, enforces vendor accountability, and supports the secure operation of critical networks and services .

This guidance details how procurement and commercial practitioners operating in government should manage security

Streamline your IT procurement process in 2025 with smart strategies, best practices, and a

The goal of this Security Guide for ICT Procurement is to support primarily electronic communications service providers but also ICT

Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktop Computers Executive summary

The security policy framework describes the standards, best-practice guidelines and approaches that are required to

NIS2 Directive procurement 2026: Regulation 2022/2555/EU mandates cybersecurity upgrades for public bodies.

DHS and CISA have broad authority to secure the networks and IT equipment utilized by civilian federal agencies. As a result, CISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise

Generally, contracting authorities awarding defence and security contracts must use the same procurement

This week"s update provides an overview of the importance of "information security" (which includes but is not limited to

The procurement of security equipment is a critical component of public safety strategies, requiring meticulous planning

This Procurement Policy Note (PPN) sets out the actions in-scope organisations should take to identify and

The procurement of network security equipment should be undertaken by the relevant authority organization

mitigate

The contracting authority can strengthen the cyber integrity of the award process and the following performance of the contract by

This document summarizes security principles that should be considered when designing and procuring control systems products

Do you have what it takes to be a network equipment purchasing manager? Being a purchasing manager is a multi

The cloud security principles are designed to help you choose a cloud provider that meets your security

Web: https://in-au.co.za