

Government network security equipment



AI Overview

Government secure network equipment includes approved server racks, secure cabinets, network infrastructure, and cybersecurity-compliant solutions designed to protect sensitive data and critical services. Physical Security Solutions Government-approved secure cabinets and enclosures are designed to protect sensitive information and IT equipment from unauthorized access and physical threats. These units often feature integrated locking systems, electronic access controls, and audit trail capabilities, and are built to meet NPSA, CPNI, and UK Government security standards. They can be customized for multi-user workstations, conference setups, or high-demand environments, ensuring both robust security and operational flexibility . Modular designs allow for configurable shelving, LED screens, and power monitoring for server racks, enhancing both security and efficiency . Network and Connectivity Equipment Secure network equipment for government use includes highly resilient network infrastructure that supports critical services. Providers like hSo deliver ISO 27017/18-certified network solutions, ensuring encrypted data in transit and compliance with National Cyber Security Centre (NCSC) guidelines. These solutions are designed for public sector frameworks, including NHS Digital-approved HSCN connectivity, and support cloud hosting, secure remote access, and critical national infrastructure operations . Cyber Essentials Plus accreditation ensures that network services meet stringent security requirements. Cybersecurity and Compliance Government network equipment must comply with cybersecurity regulations, such as the Network and Information Systems (NIS) Regulations and the Cyber Security and Resilience Bill, which mandate risk-based security measures for essential and digital services . This includes protection against hacking, malware, ransomware, and data breaches, as well as incident reporting to competent authorities. The Government Cyber Coordination Centre (GC3) and the Government...

Article Content

Cisco Government: Digital Government Solutions

Cisco understands government customers face complex regulations to innovate securely and comply. On Cisco's Trust Portal, you'll find tailored trust packages, Cybersecurity programs and policy | GSA

Cybersecurity programs and policy We manage many IT security programs, and help agencies implement IT policy that enhances the safety and resiliency of the government's systems

Enhanced Visibility and Hardening Guidance for Communications

This guide provides network engineers and defenders of communications infrastructure with best practices to strengthen their visibility and harden their network devices against successful

Network Security: Safeguarding Government Sectors Against Evolving ...

Abstract The digital landscape has fundamentally altered government operations, introducing efficiencies alongside heightened vulnerability to sophisticated cyber threats. This article examines the critical

Israel installed security at Epstein's Manhattan

Investigation reveals the Israeli government installed surveillance equipment at a Jeffrey Epstein-managed residence.

NSA Details Network Infrastructure Best Practices > National Security ...

The National Security Agency (NSA) released the "Network Infrastructure Security Guidance" Cybersecurity Technical Report today. The report captures best practices based on the

Government Security Solutions: A Complete Guide

A complete guide to government security solutions — covering access control, surveillance, compliance standards, and how to choose and

Approved Products List

The Department of Defense Information Network (DoDIN) Approved Products List (APL) is the single consolidated list of products that affect communication and collaboration across the DoDIN.

List of Equipment and Services Covered By Section 2 of The Secure ...

Section 1.50002 of the US Federal Communications Commission's rules directs the Public Safety and Homeland Security Bureau to publish a list of communications equipment and services (Covered

Network Infrastructure Security Guide

Guidance for securing networks continues to evolve as adversaries exploit new vulnerabilities, new security features are implemented, and new methods of securing devices are

DA 25-644 Released: July 23, 2025

Pursuant to section 2 of the Secure and Trusted Communications Networks Act of 2019¹ (Secure Networks Act), and sections 1.50002 and 1.50003 of the Commission's rules,² the Federal

IoT in Government Network Security Solutions | IT

Lantronix offers a comprehensive suite of innovative products tailored specifically for federal, state, and local government agencies, designed to enhance connectivity,

Cisco Cybersecurity Solutions for Government

Empower your government agency with solutions to enhance cybersecurity and support compliance efforts. Deliver an AI-driven, cloud-native security fabric for modern IT environments. Secure

Device security guidance

Case studies If you're looking for some ideas on how to make small, tangible improvements in your network security, the NCSC has worked with several

Klever: export controls on advanced semiconductor manufacturing ...

On 1 April 2025 the Netherlands will modify its national export control measure for advanced semiconductor manufacturing equipment. As of that date more types of technology will be subject to

Network Infrastructure Security Guide

An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications, and information on the network.

Securing Networks | Cybersecurity and Infrastructure Security ...

Improve your security posture with CDM program cybersecurity tools, integration services, and dashboards designed to dynamically fortify the cybersecurity of government networks

Recent travel guidance for using government devices gives best ...

Stephens said the Federal Mobility Group's guidance was an intergovernmental collaboration effort and it applies to government-furnished equipment, smartphones and tablets. The

Cyber Awareness Challenge 2025 Telework and Home Computer

IoT devices can be compromised within two minutes of connecting to the Internet, and default passwords are currently the biggest security weaknesses of these devices. When using your home

NCSC advice on high risk vendors in UK telecoms

The Government has therefore asked the NCSC to consider publishing non-binding technical advice to operators in respect of their use of

FACT SHEET: FCC Updates Covered List to Include Foreign-Made

In other words, the Commission cannot update this list on its own and is required to implement determinations that are made by our national security agency experts. • Equipment on the Covered

Prohibition on Authorization of "Covered" Equipment

The Commission's prohibition on authorization of "covered" equipment concerns such equipment as identified on the Commission's Covered List, which the Commission periodically updates. Covered

FCC List of Equipment and Services That Pose National Security Threat

FCC's Public Safety and Homeland Security Bureau publishes a list of communications equipment and services that are deemed a threat to national security, consistent with requirements in

10 Best Network Security Providers for Government Sectors

Pursuant to the Commission's rules, the Public Safety and Homeland Security Bureau will maintain this list on the Commission's website, and will monitor the status of any determinations in

Government Secure Network Solutions

ZPE Systems provides governments with secure network solutions that combine Zero Trust protection with unified control, automation, and resilience.

Meeting digital and technology standards in schools and colleges

Use the latest wireless network standards for performance, coverage, management and security in your school or college.

Government Networks: Security Frameworks and Requirements

Government Networks: Security Frameworks and Requirements A practical look at how federal agencies secure their networks, from Zero Trust and FedRAMP to encryption standards and

New plans to safeguard country's telecoms network and

The National Cyber Security Centre has issued advice to telecoms network operators to help with the industry rollout of 5G and full fibre networks in

Securing Network Infrastructure Devices

Government agencies, organizations, and vendors supply a wide range of guidance to administrators—including benchmarks and best practices—on how to harden network devices.

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: <https://www.dknconsulting.co.za>

Email: info@dknconsulting.co.za

Phone: +31 6 2948 7351

Address: Herengracht 123, 1015 BT Amsterdam, Netherlands

This document is for informational purposes only. Specifications subject to change without notice.

