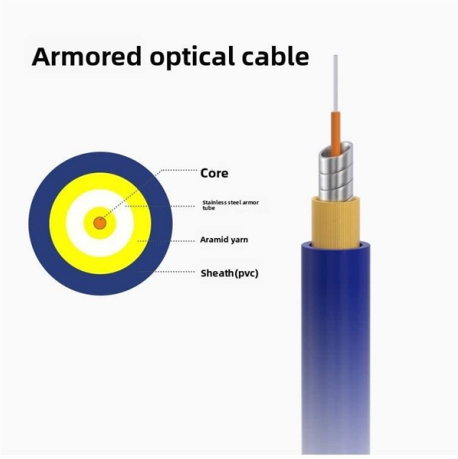
Network Security Equipment Confidentiality Bureau Authorization



AI Overview

Network security equipment authorization and confidentiality are managed through FCC regulations, Telecommunication Certification Bodies (TCBs), and DoD COMSEC policies to protect sensitive technical information and national security.FCC Equipment Authorization and ConfidentialityThe Federal Communications Commission (FCC) oversees the authorization of telecommunications and network equipment in the United States. Equipment that poses a potential national security risk is identified on the FCC's Covered List, which includes products from companies such as Huawei, ZTE, Hytera, Hikvision, and Dahua when used for public safety or critical infrastructure purposes . Equipment on this list is prohibited from marketing, importation, or authorization in the U.S., ensuring that high-risk devices do not compromise network security .Telecommunication Certification Bodies (TCBs) and Confidentiality RequestsApplications for equipment certification are processed by Telecommunication Certification Bodies (TCBs). When submitting a Form 731 application, applicants can request confidentiality for specific exhibits, such as internal photos or user manuals, to protect proprietary technical information . Confidentiality can be short-term (with an expiration date) or long-term, often requiring that sensitive equipment be serviced only by designated professionals under a Non-Disclosure Agreement (NDA). Properly associating confidentiality with each exhibit is critical; otherwise, the information may become publicly available .Department of Defense (DoD) Communications Security (COMSEC)For DoD network security equipment, the DoD Components follow DoDI 8523.01, which mandates the protection of communications through COMSEC measures, including transmission security (TRANSEC) and safeguarding cryptographic items . This ensures the confid...

Article Content

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

What is the CIA Triad? | Definition from TechTarget

The CIA triad (confidentiality, integrity and availability) guides data security policies. Learn why it''s important, and check out some examples.

A Framework for Designing Cryptographic Key Management Systems

A Key Security Policy would state the policy for confidentiality, integrity and source authentication for the key and its metadata over the entire key lifecycle.

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

List of companies that produce equipment and services covered by section 2 of the Secure Networks Act.

Data Confidentiality: Detect, Respond to, and Recover from Data

Network protection provides protection for security architecture and enterprise components, as well as providing additional network and authentication logging data for analysis.

October 7, 2025

Prohibit authorization of devices that include modular transmitters that are covered equipment. Provide a procedure to limit previously granted authorizations of covered equipment to prohibit the continued

PUBLIC NOTICE

Pursuant to sections 2(a) and (d) of the Secure and Trusted Communications Networks Act of 2019,1 and sections 1.50002 and 1.50003 of the Commission''s rules,2 the Federal Communications

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

Below is the list of covered equipment subject to importation and/or marketing prohibitions.

Promoting the Integrity and Security of

The following outlines how the People''s Republic of China (PRC) is manipulating and can exploit the FCC''s equipment authorization process to harm

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

PUBLIC NOTICE

WC Docket No. 18-89 Pursuant to section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act),1 and section 1.50002 of the Commission''s rules,2 the Federal

What''s The CIA Triad? Confidentiality, Integrity,

Key Takeaways The CIA Triad — Confidentiality, Integrity, and Availability — is a foundational model for information security, guiding

FCC Bans Equipment Authorizations for Chinese Telecommunication,

The Report and Order applies to future authorizations of equipment identified on the Covered List published by the FCC''s Public Safety and Homeland Security Bureau pursuant to the

Network Security

Network security protects networks and the data they carry from unauthorized access, misuse, and cyberattacks. It ensures systems remain confidential, available, and trustworthy across

Protecting Against National Security Threats to the Communications ...

In this document, the Commission seeks further comment on potential additional revisions to the rules and procedures associated with prohibiting the authorization of "covered" equipment in

NIST SP 800-122, Guide to Protecting the Confidentiality of Personally ...

The document explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy using the Fair Information Practices, which are the

15 CFR Part 791 -

(1) No specific authorization issued under this subpart, or otherwise issued by BIS, permits or validates any prohibited transaction effectuated prior to the issuance of such specific authorization unless

Microsoft Word

Information Assurance: The overall effort taken by an organization to ensure the availability, authentication, confidentiality, integrity, and non-repudiation of its sensitive data and the supporting

Protecting Against National Security Threats to the Communications ...

In November 2022, as part of the Commission''s ongoing efforts to protect the security of America''s communications networks and equipment supply chains, the Commission adopted the

FCC Releases Item Amending Equipment Authorization Rules to

Wiley has a strong bench of expertise on issues related to federal supply chain oversight and national security. We have particularly deep experience with the FCC''s equipment authorization

Protecting Against National Security Threats to the Communications ...

In this document, the Federal Communications Commission (Commission) amends its rules related to equipment authorization to further secure our communications networks and supply

Network Security Principles

Learn the key principles of network security with a focus on authorization. This tutorial covers what authorization is, why it''s essential, and how to implement it with simple examples.

Data Confidentiality: Identifying and Protecting Assets Against ...

Specifically, data confidentiality remains a challenge as attacks against an organization''s data can compromise emails, employee records, financial records, and customer information—impacting

FCC bans equipment authorization for Chinese

The U.S. Federal Communications Commission (FCC) has adopted new rules, under the Bipartisan Secure Equipment Act of 2021, which prohibit

47 CFR Part 2 Subpart J -

In addition to the technical standards provided, the rules governing the service may require that such equipment be authorized under Supplier''s Declaration of Conformity or receive a grant of certification

Federal Communications Commission FCC 22-84 Before the Federal ...

3 (NPRM),1we adopt revisions to our equipment authorization program to prohibit authorization of equipment that has been identified on the Commission''s Covered List – published pursuant the

Protecting Against National Security Threats to the Communications ...

The FCC''s equipment authorization process requires all telecommunications and electronic devices legally marketed in or imported to the United States to receive certification. These authorizations

Federal Register :: Securing the Information and Communications ...

This final rule, published by the Department of Commerce''s (Department) Bureau of Industry and Security (BIS), sets forth regulations and procedures to address undue or unacceptable

FedRAMP | FedRAMP.gov

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment.

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.