TIA QuEST Forum
Telecommunications Industry Association
TECHNICAL BULLETIN
TIAonline.org / @TIAonline

How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Operationalizes the United Kingdom Telecommunications (Security) Act of 2021

July 19, 2022

Executive Summary

This Technical Bulletin provides an overview of the United Kingdom Telecommunications (Security) Act of 2021 (the 'Act') and benefits provided by the Telecommunications Industry Associations (TIA) SCS 9001 Supply Chain Security Standard in operationalizing the Act.

Matt Warman, Minister for Digital Infrastructure, described the Act as bringing in "*one of the strongest telecoms security regimes in the world, a rise in standards across the board, set by the government rather than the industry*". The Act amends the existing security duties under the Communications Act, 2003, which are applicable to Providers of Public Electronic Communications Networks ("PECNs") and Public Electronic Communications Services ("PECSs").

For the purposes of this bulletin, PECNs and PECSs will be referred to as 'Providers'.

Introduction to the Telecommunications Industry Association (TIA)

The Telecommunications Industry Association (TIA), the trusted industry association for the connected world, represents more than 400 global companies that enable high-speed communications networks and accelerate next-generation ICT innovation. Through leadership in U.S. and international advocacy, technology programs, standards development, and business performance solutions, TIA and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI) and is active in developing and promoting international standards.

TIA QuEST Forum brings together companies from around the world who manufacture, deploy and operate cutting edge networks, to develop process-based industry standards and tools to improve business performance and to address the challenges that come with digital transformation, new business models, innovation, and increasing competition.

TIA's QuEST Forum community built and maintains the ICT industry's most prominent quality standard – TL 9000. As part of our commitment to ensuring global networks are reliable, trusted and secure, TIA QuEST Forum has released the "SCS 9001 Supply Chain Security Management System", a process-based standard focused on supply chain security for the global Information and Communication Technology (ICT) industry.

SCS9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry and benchmarks performance to drive continuous improvement. This standard provides value to network operators of all types and developers and manufacturers of products and services used within those networks.

Overview of the United Kingdom Telecommunications (Security) Act of 2021

The Act was developed in close collaboration with the National Cyber Security Centre (NCSC) following the publication of the UK Telecoms Supply Chain Review Report in July 2019.[1] The NCSC provides technical advice on cyber security matters to the government and in support of Ofcom, the U.K.'s telecommunications regulatory body.

The Act became law on November 17, 2021. It creates a new regulatory framework imposing a wide range of cyber security obligations on the telecom industry with Ofcom responsible for the oversight and enforcement of the law.

The Act creates new and stronger security responsibilities on Providers. Ofcom has oversight responsibility for ensuring Provider compliance.

A high-level summary of the provisions of the Act follows:

- Providers must have measures in place to identify and reduce security risks.
- Providers must prepare for future risks.
- Providers are required to take appropriate and proportionate action after a security compromise, to limit damage and take steps to remedy and mitigate the damage.

The Act gives the government powers to set out specific security requirements that Providers must meet. This includes making sure that Providers securely design, construct and maintain networks with special focus on the handling of sensitive data; reduce supply chain risks; carefully control access to sensitive parts of the network; and make sure the right processes are in place to understand the risks facing networks and services.

Ofcom's authority under the Act is substantial. Specifically, Ofcom is empowered to:

- Ensure Providers comply with their security duties.
- Work with Providers to improve their security.
- Monitor and enforce Providers' ongoing compliance.
- Ensure that Providers share information for the security assessment of their networks.
- Take enforcement action in the cases of non-compliance.

Ofcom can impose a fine of up to a maximum of ten percent of relevant turnover, or in the case of a continuing failure to comply, penalties of up to £100,000 per day. If a provider fails to

[1] Both documents can be accessed with the provided links in the References section of this bulletin.

provide information or refuses to explain a failure, Ofcom can impose fines of up to a maximum of £10 million, or in the case of a continuing failure to do this, £50,000 per day.

The Act further provides for the Government to issue Designated Vendor Directions in respect of High-Risk Vendors (HRVs) where these HRVs are deemed to be a threat to national security. This means the government can control the extent to which equipment provided by these companies are deployed in UK networks. In certain cases, this also means the government can require Providers to remove existing equipment that has been sourced from these companies.

The Act has now received royal assent and creates a strong new regulatory framework imposing a wide range of cyber security and supply chain obligations on the U.K. telecoms industry. However, the Act itself is not prescriptive and does not provide great detail on how Providers should meet the requirements. The Act provides for additional security measures to be included in ancillary legislation, and it is within this legislation that the comprehension of the Act becomes clear.

There are two additional legislative activities and deliverables in support of the Act:

- *Electronic Communications (Security Measures) Regulations"* (the 'Regulations') details a range of specific requirements considered as part of the Act.[2] The Regulations have been the subject of extensive consultation, are currently available in draft form, and changes are likely prior to the final version.
- *Draft Telecommunications Security Code of Practice* (the "Code of Practice") was first made available in March 2022. This document provides practical guidance and examples of how to achieve the requirements detailed within the Regulations.

An overview of the requirements described within the Regulations is provided in the following table, along with provisions within SCS 9001 that Providers and their vendors can use to operationalize the requirements of the Act and the Regulations.[3]

The SCS 9001 capabilities are intended to be representative and not inclusive of all SCS 9001 capabilities.

[2] A link to the draft document is available in the References section of this bulletin.

[3] The SCS 9001 capabilities are intended to be representative and not inclusive of all SCS 9001 capabilities. Numbering used within the table is not taken from the Act, Regulations or SCS 9001, it is used to simply map example requirements of the Regulations and the corresponding response of SCS 9001 capabilities.

The Electronic Communications (Security Measures) Regulations

The following table explains how SCS 9001 assists both network operators and their vendors in operationalizing the TSA and Regulations. The Regulations are consolidated into the primary areas of interest and corresponding representative capabilities of SCS 9001 in how they address the Regulations are provided.

Please Note: the numbering in the table is independent of any regulations and SCS 9001 and is provided only to simplify referencing correlating data points in each column of the table.

TSA 2021 Regulations	TIA QuEST Forum SCS 9001 Alignment
Network architecture The Regulations require that Providers: 1. Implement, redesign as necessary and operate and maintain networks to reduce the risk of security compromise 2. Properly handle sensitive data 3. Assess network vulnerability to the exposure of 'external signals' 4. Provide network segregation of critical functions with such segregation being physical or logical 5. Take appropriate measures in the procurement, configuration, management and testing of equipment to ensure the security of the equipment before being placed into the network 6. Are self-sufficient in being able to assess risks to, and where necessary maintain the operation of, networks located in the U.K. without reliance on persons, equipment or stored data located outside the United Kingdom	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring that organizations conduct Secure Network and Systems Planning reviews to ensure that organizations plan, design, and implement networks and systems in a manner to assure a secure environment. 2. requiring that organizations perform a Security Risk Analysis which includes consideration of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure and limited access to such sensitive data to only those requiring such access to perform their job function. 3. requiring that organizations operate under a Secure Network and Systems Operations policy which include continuous monitoring of the network environment using advanced techniques such as deep packet analysis and traffic throttling in response to network-based attacks and implementing procedures to protect wireless network environments including the detection of unauthorized (rogue) wireless network devices for a timely disconnect from the network. 4. requiring the separation of production and non-production environments to prevent unauthorized access or changes to information assets as well as configuring network environments and virtual instances to restrict and monitor traffic between trusted and untrusted connections. 5. requiring processes for supply chain management, vendor management, training of personnel, proper operation of products, and extensive testing of acquired equipment including security testing such as vulnerability testing, periodic penetration testing, cyber-attack simulations, and regular monitoring for specific threats. 6. requires that organizations identify Statutory and Regulatory Processes to establish documented

	procedures to ensure compliance with legal, and regulatory obligations.
Protection of data and network functions The Regulations require that Providers: 1. Protect data based on its sensitivity 2. Protect network functions based on their sensitivity 3. Ensure that devices providing privileged access are not exposed to external networks 4. Provide network monitoring to reduce the risk of security compromises 5. Ensure that equipment supplied to customers as part of the extended network is secure 6. Ensure that tools enabling monitoring or audit cannot be accessed from outside the United Kingdom 7. Apply encryption to reduce security compromises 8. Monitor fraud related to SIM cards	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring that organizations establish Access Control and Least Privilege Policies to restrict access to data to only those with a need to have such access and ensuring that Cryptographic Control Policies are established to protect data in use (memory), at rest (storage) and in transit (over networks). 2. requiring that organizations implement Zero Trust Architectures which controls all communications sessions. 3. requiring that networks be designed with segregation as to function, adopt a Least Privileged Policy, network access be granted based on strong authentication, authorization, and accounting (AAA) rules, and implement an Access Control Policy to ensure appropriate identity, entitlement, and access management policies including multi-factor authentication as appropriate 4. requiring not only continuous network monitoring for anomalous behavior with a special focus at network boundaries, but also monitoring access control of all assets with logging. SCS 9001 requires that organizations deeply instrument their operations in areas such as monitoring asset access, creating logs of administrative actions, network traffic, and automated equipment identification be used as a method of connection authentication, amongst other requirements. 5. requiring that purchased products are verified and tested to ensure they meet specifications including security requirements 6. requiring that organizations comply with regulatory, legal, and statutory requirements. 7. requiring that the organization implement Cryptographic Control Policies to protect data in use (memory), at rest (storage) and in transit (over networks). 8. SCS 9001 doesn't explicitly call out fraud related to SIM cards but does provide for controls and policies for mobile devices through establishment of BYOD Control Policies for the use of employee supplied devices.

TSA 2021 Regulations	TIA QuEST Forum SCS 9001 Alignment
Monitoring and audit The Regulations require that Providers: 1. Monitor their networks for anomalous behavior and promptly analyze all activity related to anomalous behavior 2. Maintain a record of all access to the network or service 3. Generate alerts upon detection of security events 4. Archive all activity related to monitoring 5. Share information on detected anomalous activity with other Providers 6. Establish and maintain a management data base of all devices used within the network	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring a plan for networks to be designed under a Zero Trust model including the monitoring of traffic flows for anomalous behavior, potentially indicating a network attack. 2. requiring extensive monitoring and logging of all system asset and network access attempts and storing those records in audit logs which themselves are to be protected from unauthorized access, modification, and deletions. 3. requiring that the organization implement an Incident Reporting policy whereby all incidents detected shall be reported to appropriate personnel and that potential security events are managed by an Incident Response Team. Extensive alerting and incident data collection is required. 4. requiring that logging facilities and log information be protected against tampering and unauthorized access, and further that audit logging tools are prevented from unauthorized access, modification, and deletion. 5. requiring that organizations maintain documented information to notify all customers who may be affected by a critical problem and establishing methods for affected customers to obtain real time information about current critical service disruptions. Further, the organization is required to establish methods to ensure external providers meet security requirements including agreement to all relevant security, service, and capacity-level requirements by each supplier that can access, process, store, communicate, or provide infrastructure components. 6. requiring that organizations establish and maintain a Configuration Management Database (CMDB) to record all assets within the network. The data stored in a CMDB includes all assets and relevant information describing the assets and their relationships with one another. The CMDB is a key element in the establishment of an asset inventory and policies used in performing service management processes such as incident management, change management and problem management, as examples.

TSA 2021 Regulations	TIA QuEST Forum SCS 9001 Alignment
Supply Chain The Regulations require that Providers: 1. Reduce supply chain risk by vetting not only their own suppliers, but the supply chains of those suppliers as well. 2. Identify and reduce the risks of security compromises occurring as a result of the Provider outsourcing any aspect of the implementation or operation of their networks 3. Provide a risk assessment of their supply chain including contracts with their suppliers and those of their suppliers 4. Provide protections if a 3rd party supplier is itself a Provider and is given access to the primary Provider's network and/or sensitive data. Ensure that all integration points and data sharing are handled securely. 5. Co-operate amongst all parties for the resolution of incidents contributing to a security compromise. 6. Ensure that 3rd party Providers conform to equivalent policies and procedures in relation to the risks of security compromises.	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring through Provenance processes that the origins of all components in products have complete traceability to their source and that these requirements are extended to all suppliers within the supply chain including all contractors, and their subcontractors. 2. requiring that organizations perform a Business Impact Assessment (BIA) that determines the key factors on protections of assets and networks. The BIA shall include External Provider Input and that the organization implement methods for collaboration with external providers on supply chain and security planning activities. 3. requiring that organizations conduct a Supply Chain Risk Management and Security Risk Analysis reviewed with findings addressed through a Supply Chain Security Risk Mitigation process. These reviews and updates are to be conducted at least annually. Further, the organization is required to perform a Business Impact Assessment (BIA) that determines the key factors on protections of assets and networks. The BIA shall include External Provider Input and that the organization implement methods for collaboration with external providers on supply chain and security planning activities. 4. requiring that the organization establish Security Policies within the appropriate business processes supporting confidentiality, integrity, and availability across system interfaces, jurisdictions, and business functions. Additionally, the organization is required to develop a network architecture through Secure Network and Systems Planning that includes network diagrams identifying high-risk environments and data flows that may have legal compliance impacts and limiting access to sensitive data. 5. requiring that as part of vendor selection, that External Providers be allowed input into, and are aligned with required security policies and that all 3rd parties be involved in the Incident Management Process of responding to reported attacks and vulnerabilities. 6. requiring that the organization apply criteria for the evaluation, selection, monitoring of the performance of external providers based on their ability to provide products and services in accordance with requirements.

TSA 2021 Regulations	TIA QuEST Forum SCS 9001 Alignment
Prevention of security compromise and management of security permissions The Regulations require that Providers: 1. Take measures as appropriate and proportionate to prevent the occurrence of security compromises in their networks 2. Require two or more independent credentials to be present in order to access security critical functions 3. Avoid the use of default credentials 4. Ensure that data that could be used to cause a security compromise is stored securely 5. Ensure changes to the operations of security critical functions are approved by another suitably competent and authorized person 6. Undertake regular reviews of security measures 7. Deploy patches as they become available that mitigate security vulnerabilities in a timely manner (14 days based upon severity) 8. Isolate security critical functions from all signals believed unsafe. 9. Limit the number of persons given security permissions and that the extent of those permissions be restricted to the extent necessary to undertake authorized activities 10. Ensure that passwords and credentials are managed, stored and assigned securely	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring that organizations conduct a Security Risk Analysis with identified vulnerabilities addressed through Operational Risk and Technical Vulnerability Management processes. 2. requiring that organizations establish an Access Control Policy for ensuring appropriate identity, entitlement, and access management for all corporate assets and that users be established, documented, and evaluated at least annually for effectiveness. The Policy will include consideration for higher levels of assurance through multi-factor authentication as appropriate. 3. requiring that organizations reset all vendor provided passwords and provide account credential lifecycle management from instantiation through revocation of credentials. Further, passwords must be of high quality and sufficient complexity. 4. requiring the development of a network architecture through Secure Network and Systems Planning that includes network diagrams identifying high-risk environments and data flows that may have legal compliance impacts and limiting access to sensitive data. 5. requiring the establishment of a comprehensive Change Management process through which the organization maintains documented information ensuring all requirements and design changes to systems are managed and tracked in a systematic manner and that changes which impact mutually agreed conditions for quality, reliability, and functional intent are reviewed with the customer prior to approval and implementation. 6. requiring that organizations conduct Security Program Planning which requires that all security processes be documented, approved, implemented, maintained, and reviewed at least annually that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall, as appropriate, include, but is not limited to a) risk management, b) security program policy, c) organization of security, d) asset management, e) human resources security, f) physical and environmental security, g) communications and operations management, h) access control, i) information

	systems acquisition, development, and maintenance, j) ensuring the supply chain security program can achieve its intended outcome(s), k) preventing, or reducing undesired effects, l) creating, maintaining, and leveraging a security strategy and roadmap for organizational security improvement, m) system boundaries, n) system environments of operation, o) how security requirements are implemented, p) relationships with or connections to other systems, and q) achieving continual improvement. 7. requiring that organizations establish a Change Management Policy Policies, documented procedures, and measures shall be established to detect technical vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing). A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. The process shall include a) timely identification of information about technical vulnerabilities of information systems being used, b) evaluation of the organization's exposure to such vulnerabilities, c) appropriate measures taken to address the associated risk, d) a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software, 8. requiring that organizations move to a Zero Trust Network Architecture, which in of itself addresses many concerns. Additionally, the organization is required to implement secure networks and systems leveraging concepts such as Least Privileged Access and Access Control Policies. 9. requiring a Least Privilege Policy for denying network communications traffic by default, identification of privileged accounts, and physical and logical access controls 10. requiring minimum password complexities, use of a password generator, resetting default passwords, and account credential lifecycle management from instantiation through revocation. Additionally, organizations are required to protect passwords both during storage and transmission with strong cryptographic controls employing a NIST Federal Information Processing Standards-valid cryptography standard (or equivalent) when used to protect the confidentiality of assets.

TSA 2021 Regulations	TIA QuEST Forum SCS 9001 Alignment
Governance and accountability The Regulations require that Providers: 1. Ensure appropriate management of persons given responsibility for network security 2. Treat security as an essential business function and assign board level or equivalent responsibility for ensuring effective security management 3. Undertake at least once in any period of 12 months a review of the risks of security compromises to the network or service in order to produce a written assessment of the extent of the overall risk of security compromises 4. Ensure that business procedures include a post-incident review process in relation to all security incidents. 5. Have a standardized way of categorizing and managing security incidents. 6. Identify and prioritize network security updates and network equipment upgrades	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring that organizations establish Security Policies including a strategic business plan and security program inclusive of defined security roles and responsibilities for business leadership and that roles and responsibilities are documented for contractors, employees, and third-party users as they relate to supply chain assets and security. 2. requiring that Top Management be responsible for supply chain security including setting the strategy, regular annual assessment and review, and that all supply chain security responsibilities are defined, documented, assigned, and communicated at all levels of the organization. 3. requiring that the organization conduct a Supply Chain Security Risk Assessment at least annually to formally assess risks with consideration given to risk sources, and risk measurement criteria based on current and accumulated threat intelligence. The organization shall retain documented information about the security risk assessment process. Risk assessment should include not only the organization itself, but also the supply chain with recommendations that suppliers and customers engage in common threat intelligence exercises. 4. requiring the establishment of an Incident Management Process whereby the organization establishes and maintains a documented operational incident response process for products and services that includes preparation, detection, analysis, containment, recovery, and user or customer response activities. Additionally, the organization is required to establish an Incident Reporting Processes whereby all incidents are reported to the appropriate personnel and logged along with providing customer notifications on updates on critical problems including service disruptions with the ability for customers to obtain real-time updates. 5. requiring that organizations establish an Incident Reporting process with pertinent information collected and archived such as date of event, severity of event, person reporting the incident, description of the event, proposed resolution to the event, etc. 6. requiring that organizations establish effective Problem Resolution Processes which includes as examples documenting the event, provide options such as immediate patching, immediate source

	code corrections, deferring solutions to a planned release, and providing documented work-around(s) until a permanent resolution is provided within a designated timeframe based on the severity of the problem. Further, requirements are to be established when corrective action is required of an external provider when it is determined that the external provider is responsible for the nonconformity.
Competency The Regulations require that Providers ensure that persons with responsibility for meeting the Regulations, and those persons who support the operation of security critical functions are competent to discharge that responsibility.	SCS 9001 supports operationalizing this requirement including requiring that organizations determine the necessary competence of person(s) doing work under its control, ensures that these persons are competent on the basis of appropriate education, training, or experience, takes action to acquire necessary competence and retain evidence of such competence. Further, SCS 9001 requires annual Security Awareness Training for all employees, contractors, and 3rd party users with access to corporate assets.
Testing The Regulations require that Providers: 1. Carry out tests in relation to the network or service as are appropriate and proportionate for the purpose of assessing the resilience of the network or service to the risks of security compromises occurring. 2. Tests must involve simulating, so far as is possible, techniques that might be expected to be used by a person seeking to cause a security compromise.	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring that organizations implement a Secure Development Lifecycle process whereby security is considered at every phase of development and product delivery. A variety of recommended test approaches are described as appropriate such as unit, feature, integration, system, acceptance, field, migration, regression, functional, boundary, usability, performance, interoperability, stress, security, network vulnerability and penetration. 2. requiring organizations establish real-world test environment mimicking the user production and operational environments.
Assistance The Regulations require that Service Providers (those providing communication services over a Provider's network): 1. Must not do anything which impedes a Provider from complying with these Regulations 2. Must provide assistance to the Provider when requested for the Provider to fulfill the requirement of the Regulations. The Regulations require that Providers and Service Providers: 3. Share information about any security compromise with all other Providers and Service Providers whose network or communication service may be impacted.	Examples of how SCS 9001 provides support in operationalizing these requirements includes but may not be limited to: 1. requiring that organizations conduct a Business Impact Analysis which identifies all dependencies on business partners, suppliers, and third-party service providers. 2. requiring that the organization has documented corrective action processes to enact upon critical problem reports. These corrective action requirements may be executed by an external provider when it is determined that the external provider is responsible for the nonconformity. The organization is expected to take escalatory action when timely and effective corrective actions are not achieved.

4. Must seek appropriate assistance to reduce the risk of security compromises to the Provider's network or Service Provider's communications service.	3. requiring that the organization establish methods to ensure external providers meet security requirements. These methods can include as appropriate agreement to all relevant security, service, and capacity-level requirements, primary points of contact for the duration of the business relationship, references to detailed supporting and relevant business processes, measures implemented to enable effective governance, risk management, and legal, statutory, and regulatory compliance as examples. Further, SCS 9001 requires controls, processes, and policies that ensure requirements are extended to external providers as appropriate to mitigate and contain security risks, and that providers make security incident information available within defined timeframes for any incidents that they or their supply chain experience. 4. requiring that organizations determine the competence of employees performing functions which can access the network or other information assets and to take appropriate action of training or the hiring or contracting of competent persons.

Conclusion

The U.K. Telecommunications Security Act 2021 is significant legislation with deep impacts into the deployment and operation of networks in the United Kingdom. Ofcom has been provided new powers in the oversight, monitoring and assessment of penalties for network operators not complying with the law.

SCS 9001 is a Supply Chain security standard which provides assurance as to the proper operational hygiene of vendors in delivering products and services to organizations who operate networks, be they private or public.

The SCS 9001 Supply Chain Security Standard was developed in support of network operators in evaluating their vendors and providing higher confidence that those vendors:

- Operate their businesses with integrity and transparency
- Conduct all aspects of their operations and product development with a high level of consideration to security through-out product lifecycles
- Deliver products that are inherently higher in security and quality
- Make requisite investments to support products through their entire production lifecycle with the ability to more quickly identify, mitigate and resolve vulnerabilities

TIA will continue to track the legislative process and ratification of the Electronic Communications (Security Measures) Regulations 2021 and Telecommunications Security Code of Practice and issue updates to this bulletin as appropriate.

As demonstrated herein, SCS 9001 can be a powerful aid in driving security and supply chain security improvements to address the requirements of the Telecommunications Security Act of 2021.

Questions? Want more information about TIA QuEST Forum's SCS 9001?
Visit: https://bit.ly/SCS9001
Send us an email: supplychainsecurity@tiaonline.org

References

- United Kingdom Telecommunications Security Act of 2021
  newbook.book (legislation.gov.uk)
- Electronic Communications (Security Measures) Regulations 2021 (Draft)
  SI/SR Template (publishing.service.gov.uk)
- Telecommunications Security Code of Practice (Draft)
  Draft Telecommunications Security Code of Practice (publishing.service.gov.uk)
- Ofcom Press Release
  New powers for Ofcom to oversee security of telecoms networks - Ofcom
- UK Telecoms Supply Chain Review Report (2019)
  UK Telecoms Supply Chain Review Report (publishing.service.gov.uk)