Ministry of Defence

Defence Standard 05-138 Issue 4 Date: 14 May 2024

Cyber Security Standard for Suppliers

Section 1 Foreword

Defence Standard Structure

Section 1 (Generated by the StanMIS toolset)

- Revision Note
- Historical Record
- Warning
- Standard Clauses

Section 2 (Technical information provided by Subject Matter Expert)

- Title
- Introduction (optional)
- Table of Contents
- Scope
- Technical Information to include Tables and Figures
- Annexes (as required)

Section 3 (Generated by StanMIS toolset)

- Normative References
- Definitions
- Abbreviation

- Changes Since Previous Issue

REVISION NOTE

This substantive update details the move from five Cyber Risk Profiles of “N/A, Very Low, Low, Moderate and High” to four Cyber Risk Profiles of “Level 0, Level 1, Level 2 and Level 3” and introduces new cyber security control requirements at each level.

HISTORICAL RECORD

This standard supersedes the following:

Def Stan 05-138 Iss 3

WARNING

The Ministry of Defence (MOD), like its contractors, is subject both to United Kingdom law and any EUderived law that has been retained under the European Union (Withdrawal) Act 2018 regarding Health and Safety at Work. Many Defence Standards set out processes and procedures that could be injurious to health if adequate precautions are not taken. Adherence to those processes and procedures in no way absolves users from complying with legal requirements relating to Health and Safety at Work.

STANDARD CLAUSES

a) This standard has been published on behalf of the Ministry of Defence (MOD) by UK Defence Standardization (DStan).

b) This standard has been reached following broad consensus amongst the authorities concerned with its use and is intended to be used whenever relevant in all future designs, contracts, orders etc. and whenever practicable by amendment to those already in existence. If any difficulty arises which prevents application of the Defence Standard, DStan shall be informed so that a remedy may be sought.

c) Please address any enquiries regarding the use of this standard in relation to an invitation to tender or to a contract in which it is incorporated, to the responsible technical or supervising authority named in the invitation to tender or contract.

d) Compliance with this Defence Standard shall not in itself relieve any person from any legal obligations imposed upon them.

e) This standard has been devised solely for the use of the MOD and its contractors in the execution of contracts for the MOD. To the extent permitted by law, the MOD hereby excludes all liability whatsoever and howsoever arising (including, but without limitation, liability resulting from negligence) for any loss or damage however caused when the standard is used for any other purpose.

Section 2

Cyber Security Standard for Suppliers

Contents

Tables

0 Introduction

0.1 The Cyber Security Model (CSM) is a risk-based, proportionate approach to strengthening Supplier resilience, and protecting UK & Partner Data as it moves through, or is generated in, the supply chain.

0.2 The CSM seeks to adopt a whole enterprise/organisational approach to cyber resilience that ensures its continued operation and delivery of its contracted output and protection of Data, including that of the UK and its International Partners.

0.3 This Defence Standard defines the CSM Cyber Risk Profiles and associated minimum cyber security control requirements of a Supplier organisation.

1 Scope

1.1 The scope of this standard is the Supplier's overarching corporate or enterprise environment. All Supplier organisations, systems, processes, procedures and data necessary for its effective protection of Data and/or Functions are within the scope of this standard, going beyond the protection of just the information provided to the Supplier in support of that contracted output.

1.2 This standard is, therefore, intentionally broad, ensuring that a Supplier organisation, irrespective of any controls required for a specific contracted output, has the appropriate minimum levels of controls in place for the level of risk to which that Supplier organisation is expected more generally.

1.3 The requirements set out within this standard are derived from current international and industry best practices, as well as requirements placed upon the MOD as a UK Government department.

1.4 These requirements are intended to be considered as a 'minimum'. Individual contracts may specify greater levels of controls/protection (such as where specified within a Security Aspects Letter).

1.5 It is intended that this standard will be regularly reviewed and updated, to ensure its continued currency and fit for purpose.

1.6 This standard may not be taken as a basis to reduce or remove any other requirements placed upon a Supplier organisation, whether contractual or legal.

2 Cyber Risk Profiles

2.1 The CSM Risk Assessment Process assigns a Cyber Risk Profile (CRP).

2.2 The CSM Cyber Risk Profiles are:

Level 0 ('Basic') – 3 controls

The Level 0 'Basic' CRP is normally assigned where there is a very low level of assessed cyber risk to a Supplier delivering an output. It requires Supplier organisations to demonstrate basic cyber security practices.

Level 1 ('Foundational') – 101 controls

The Level 1 'Foundational' CRP is normally assigned where there is a low to moderate level of assessed cyber risk to a Supplier delivering an output. It requires Supplier organisations to demonstrate a comprehensive cyber security programme with good practices.

Level 2 ('Advanced') – 138 controls

The Level 2 'Advanced' CRP is normally assigned where there is a high level of assessed cyber risk to a Supplier delivering a contracted output. It requires Supplier organisations to demonstrate advanced cyber security oversight and planning which drives robust organisational and cyber practices.

Level 3 ('Expert') – 143 controls

The Level 3 'Expert' CRP is normally assigned where there is a substantial level of assessed cyber risk from a Supplier delivering a contracted output. It requires Supplier organisations to demonstrate expert cyber security capabilities that fully take advantage of the 'defence in depth' methodology to appropriately protect the organisation against new and evolving threats.

2.3 The control requirements for each CRP are detailed in Clause 3.

2.4 The supplier shall, for each control requirement referenced in Clause 3, ensure they have a documented and implemented control in place with auditable evidence.

2.5 Where specified controls are deemed inappropriate/impractical for specific circumstances this shall be documented by the Supplier and flagged to the Authority at the time of bidding or immediately to such if identified during the period of any contracted activity.

2.6 Where the term 'Functions' is used in Clause 3, it is helpful to consider this term as referring to both general business activities essential for ongoing operations and any specific activities related to delivering contracted outputs.

2.7 Where the term 'Data' is used in Clause 3, it is helpful to consider this term as encompassing any information generated, stored or handled by the supplier in support of its Functions.

2.8 Suppliers shall refer to contract documentation, including the latest version of DEFCON 658 and the Security Aspects Letter (where issued), for full contractual definition of these terms.

3 Cyber Risk Profile Requirements Table

Table 1 - Cyber Risk Profile Requirements Table

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
0001	Cyber Essentials	X	X	X	X	The Supplier shall have Cyber Essentials certification that covers the scope required for all aspects of the contract and commit to maintaining this for the duration of the contract.
0002	Cyber Essentials Plus			X	X	The Supplier shall have Cyber Essentials Plus certification that covers the scope required for all aspects of the contract and commit to maintaining this for the duration of the contract.
Objective A: Managing security risk The Supplier has appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to its network, and information systems, including all network and information systems that protect all Data.						
1100	Governance		X	X	X	The Supplier shall have appropriate management policies and processes in place to govern their approach to the security of the network and information systems supporting Functions and protection of Data.
1101	Board direction			X	X	The Supplier shall have effective organisational security management led at board level and articulated clearly in corresponding policies.
1102	Roles and responsibilities		X	X	X	The Supplier shall have established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.
1103	Decision-making			X	X	The Supplier shall have senior-level accountability for the security of networks and information systems, and delegates decision-making authority appropriately and effectively. Risks to network and information systems that protect all Data are considered in the context of other organisational risks.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
1200	Risk management		X	X	X	The Supplier shall take appropriate steps to identify, assess, understand and remediate security risks to the network and information systems that protect all Data. This includes an overall organisational approach to risk management.
1201	Risk management process			X	X	The Supplier shall have effective internal processes for managing risks (to the security of network and information systems that protect all Data) and communicating associated activities and solutions.
1202	Periodically assess risk		X	X	X	The Supplier shall periodically assess the risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, resulting from the operation of organisational systems and the associated processing, storage, or transmission of Data.
1203	Network diagrams		X	X	X	The Supplier shall create and maintain up to date network diagrams detailing the network boundaries, internal and external connection, and systems within the operational environment.
1204	Threat intelligence capabilities				X	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.
1205	Assurance			X	X	The Supplier shall gain validation for the effectiveness of the security of their technology, people, and processes in support of its Functions and which store and/or process Data.
1206	Internal controls assurance			X	X	The Supplier shall monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Any identified deficiencies should be recorded, reported to leadership, and mitigated within agreed timeframes.
1300	Asset management		X	X	X	The Supplier shall reasonably ensure everything required to deliver, maintain or support networks and information systems that support delivery of all Functions which protect all Data are determined and understood. This includes people and systems, as well as any supporting infrastructure (such as power or cooling).

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
1301	Automated asset inventory management			X	X	The Supplier shall employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of data, people, systems and supporting infrastructure used to support business Functions and protect Data.
1400	Supply chain		X	X	X	The Supplier shall understand and manage security risks to Functions and Data that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.
1401	External provider trusted relationships		X	X	X	The Supplier shall establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships.
1500	Physical access controls		X	X	X	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.
1501	Physical access device management		X	X	X	The Supplier shall manage and maintain an inventory of all physical access devices used on their premises. The inventory should contain a unique identifier for the device regardless of the type (e.g. RFID card, access fob or door key) as well as the named individual who it is assigned to.
1502	Physical access restrictions		X	X	X	The Supplier shall restrict physical access to sensitive areas within an organisation's premises to only those who are authorised to have access. The Supplier shall maintain and manage an inventory of those staff who have privileged physical access.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
1503	Visitor access management		X	X	X	The Supplier shall ensure the following controls are applied to all visitors visiting the organisation's premises: i) Visitor access and exit shall be logged ii) ii) All visitors shall wear visitor ID badges at all times. Visitor badges should visually differ from employee badges iii) All visitors should be appropriately escorted at all times while on the premises iv) Visitor badges should be returned to the organisation at the end of the day.
Objective B: Protecting against cyber attack The Supplier has proportionate security measures in place to protect the networks and information systems supporting all Functions from cyber attack.						
2100	Resilience policy and process development		X	X	X	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.
2101	Policy and process implementation			X	X	The Supplier shall implement security policies and processes that demonstrate the continuing security benefits to Functions and Data.
2200	Identity and access control		X	X	X	The Supplier shall understand, document and manage (i.e create, review and disable) access to networks, information systems, and removable storage media & devices supporting Functions and protection of Data. All accounts and identities, including users, system and automated functions that can access Data or systems are appropriately verified, authenticated and authorised.
2201	Access control - multi-factor authentication			X	X	The Supplier shall implement multi-factor authentication (MFA) mechanisms to control access to critical or sensitive systems, and organisational operations. Factors can include: i) Something you know (e.g. password/personal identification number (PIN)) ii) Something you have (e.g. cryptographic identification device, token) iii) Something you are (e.g. biometric).
2202	Device management			X	X	The Supplier shall fully understand and trust the devices that are used to access the network and information systems that support Functions and process Data.
2203	Privileged user management			X	X	The Supplier shall closely manage privileged user access and actions to networks and information systems supporting Functions and that protect Data.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2204	Principle of least functionality		X	X	X	The Supplier shall ensure that all information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, programmes and services that are not integral to the operation of that information system.
2205	Least privilege		X	X	X	The Supplier shall closely manage all user accounts and employ the principle of least privilege to networks and information systems supporting all Functions and protecting all Data.
2206	Least privilege - audit system		X	X	X	The Supplier shall limit access to systems' audit/security logging data and functionality to privileged user groups that have a confirmed requirement in accordance with the principle of least privilege.
2207	Separation of duties		X	X	X	The Supplier shall develop a policy and implement a separation of duties methodology for standard and privileged accounts which support Functions and protect Data.
2208	Identity and Access Management (IdAM)			X	X	The Supplier shall closely manage and maintain identity and access control for users/admins, devices and systems accessing their networks and information systems supporting business Functions and protecting all Data.
2209	Limit access to authorised entities				X	The Supplier shall implement automated mechanisms to support the management of system accounts, including processes acting on behalf of authorised users.
2210	Limit to authorised transactions		X	X	X	The Supplier shall issue, manage, verify, revoke, and audit identities and credentials to authorised transactions. users, and processes.
2211	Secure first-time password management		X	X	X	The Supplier shall employ secure practices for the secure storage, transmission, and management of first-time and one-time passwords. These practices include, but are not limited to: i) Secure storage of first-time password prior to use ii) Secure transmission of first-time and one-time passwords to their new user iii) Require first-time and one-time passwords are immediately changed after first logon.
2212	Automated password management			X	X	The Supplier shall employ automated mechanisms for the generation, protection, storage, rotation, transmission, cryptographic protection and management of passwords for staff and systems.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2213	Automated password quality check		X	X	X	The Supplier shall deploy technical controls to manage the quality of credentials across all identifiers. The technical controls should reflect industry standard requirements such as password length, complexity requirements (e.g. uppercase, lowercase, numbers and symbols), reuse history, prevent reuse of identifiers for a defined period, banned words and insecure pattern recognition (e.g. 1234), as appropriate.
2214	Repeated unsuccessful logon handling		X	X	X	The Supplier shall employ policies and processes to appropriately manage unsuccessful login attempts to standard and privileged accounts. The Supplier shall lock accounts after at most ten unsuccessful login attempts for a minimum of **15 minutes**; the duration of which should increase between multiple account lockouts.
2215	Replay-resistant authentication		X	X	X	The Supplier shall enforce technical control to protect against the capture of transmitted authentication or access control information and its subsequent retransmission i.e replay attacks.
2216	Privilege failure handling			X	X	The Supplier shall prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
2217	Service accounts		X	X	X	The Supplier shall inventory all generic, service and system accounts used on the network. Every account shall be owned by a single named individual who is responsible and accountable for the account and its usage.
2218	System users and processes		X	X	X	The Supplier shall identify system users, processes acting on behalf of users, and devices.
2300	Data security		X			The Supplier shall appropriately protect data stored or transmitted electronically from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on Functions or Data. Such protection extends to how authorised users, devices and systems access critical data necessary for the operation of Functions and use of Data. Additionally, covers information that would assist an attacker, such as design details of networks and information systems.
2301	Understanding data			X	X	The Supplier shall have a good understanding and classification of the data important to the operation of Functions and protection of Data, including where it is stored, where it travels, the application of protective markings to media. The Supplier shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of Functions and protection of all Data.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2302	Data in transit			X	X	The Supplier shall protect and control data in transit, including the use of encryption where appropriate, for data important to the operation of the Functions and all Data. This includes the transfer of data to third parties.
2303	Management of established network connections		X	X	X	The Supplier shall terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
2304	Wireless network access control		X	X	X	The Supplier shall ensure that the following controls apply to trusted organisational wireless networks: i) All users and devices must be authorised and authenticated prior to granting access to the network via the wireless network ii) The data transferred over the wireless network must be encrypted using WPA2 or above methodology.
2305	Remote Access - VPN (Virtual Private Network)		X	X	X	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.
2306	Remote access sessions		X	X	X	The Supplier shall employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
2307	Managed access control points		X	X	X	The Supplier shall route remote access via managed access control points.
2308	Stored data			X	X	The Supplier shall appropriately protect the confidentiality of soft and hard copies of data being stored for all Functions.
2309	Mobile data			X	X	The Supplier shall protect, such as through encryption, data important to the operation of Functions and all Data on mobile devices.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2310	Removable media		X	X	X	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.
2311	Authorised working locations		X	X	X	The Supplier shall maintain and update a list of authorised working locations which are not the organisation's premise and communicate these locations to all employees and contractors.
2312	Security at alternate working locations		X	X	X	The Supplier shall employ technical security controls and educate users to reduce the security risks to employees while working outside the organisation's premise. Technical security controls for consideration may include, but are not limited to: i) Always-on VPN to protect data in-transit ii) Screen privacy protector to prevent shoulder surfing iii) Disabling USB ports on devices iv) Full disk encryption User awareness topics may include, but are not limited to: i) Risks of using public Wi-Fi ii) Avoid taking confidential phone calls within earshot of unauthorised individuals. iii) Shoulder surfing iv) Avoid leaving devices unattended
2313	Media/equipment sanitisation			X	X	The Supplier shall appropriately sanitise before reuse and / or disposal the devices, equipment, and removable storage media & devices holding data important to the operation of business Functions and that protect all Data.
2314	Ensure UK GDPR compliance	X	X	X	X	The Supplier shall ensure that the processing of personal data is conducted in compliance with the General Data Protection Regulation.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2315	Email authentication methods		X	X	X	The Supplier shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source.
2316	Personal and/or Personally Identifiable Information (PII) processing/transparency - control flow		X	X	X	The Supplier shall employ systems to monitor and control the flow of all Personal and/or Personally Identifiable Information (PII) and all government information (e.g. OFFICIAL and above) provided or produced during the contract throughout the information lifecycle in accordance with approved authorisations, required legislation and contractual requirements.
2317	Endpoint encryption		X	X	X	The Supplier shall implement and maintain full disk level encryption on all endpoints to industry standard solutions, for example, full disk encryption solutions using AES-256 encryption algorithm or FIPS equivalent.
2318	Approved cryptographic methods		X	X	X	The Supplier shall employ appropriate nationally or departmentally approved cryptography when used to protect all Data (e.g. FIPS 140-2 or comparable standards)
2319	Securely manage cryptographic keys		X	X	X	The Supplier shall establish and manage cryptographic keys for cryptography employed in organisational systems using appropriate nationally or departmentally approved solutions (e.g. FIPS 140-2 or comparable standards)
2320	Data Loss Prevention (DLP)			X	X	The Supplier shall implement and maintain appropriate tooling to monitor and restrict the access and use of: i) Removable storage media and devices ii) External websites iii) Email
2321	Publicly accessible data		X	X	X	The Supplier shall: i) Designate individuals authorised to make information publicly accessible ii) Train authorised individuals to ensure that publicly accessible information does not contain non-public information iii) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included iv) Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2322	Mobile devices/Bring Your Own Device (BYOD)		X	X	X	The Supplier shall ensure that mobile devices accessing its corporate environment/data are appropriately configured and managed using industry recognised solutions such as Mobile Device Management (MDM) tooling.
2323	Secure destruction		X	X	X	The Supplier shall, where not otherwise stated explicitly by country, legislation or Authority instructions, implement procedures to ensure that all Data is securely destroyed when no longer needed, or at the expiration or termination of the Agreement. Supplier shall: i) Secure and confirm the erasure of Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal ii) Provide attestation of destruction, where specified by contract with Authority iii) Require that any third parties engaged to process the Data shall securely dispose of such Data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or Authority instructions.
2400	System security		X	X	X	The Supplier shall ensure that network and information systems and technology critical for the operation of business Functions and protection of Data are protected from cyber attack. An organisational understanding of risk to business Functions and protection of Data informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.
2401	Secure configuration		X	X	X	The Supplier shall securely configure the network and information systems that support the operation of business Functions and that protect Data.
2402	Vulnerability management		X	X	X	The Supplier shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by: i) Performing vulnerability scans on a **monthly** basis and during any major system or application updates ii) Implementing vendor patches or fixes prioritising using the CVSS v3 scoring iii) Developing a Risk Treatment Plan to address identified vulnerabilities. The Supplier shall address vulnerabilities in accordance with the Supplier's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2403	Penetration testing		X	X	X	The Supplier shall conduct penetration testing (minimum every **12 months**) against externally facing systems used to support the operation of Functions and that protect Data. The penetration testing programme shall be based upon industry standards and performed by subject matter experts. The Supplier shall ensure that any deficiencies identified are remediated in a timely manner in line with their risk to the network. The Supplier shall retain records including: i) The scope and methodology utilised ii) The number of critical, high, and medium severity findings iii) The name of the tester iv) The date of the testing v) Timelines and actions for a remedial plan.
2404	Change management		X	X	X	The Supplier shall formally document, publish and review (minimum every **12 months**) the change control procedures to manage changes to information systems, supporting infrastructure and facilities. The change management policy includes: i) Definitions of the types of change (e.g. standard, critical, emergency) with associated processes ii) Roles and responsibilities for those involved in the change or approving the change. Prior to implementing any changes, Supplier shall: i) Establish acceptance criteria for production change approval and implementation ii) Require stakeholder approval prior to any change implementation iii) Formally record the change in a centralised repository iv) Document business impact analysis outcomes and document back-out procedures should the change fail v) Keep a full audit trail of the change request, testing conducted, associated documentation, approvals and outcomes vi) Document and record security impact analysis outcomes along with any mitigating actions.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2405	Patch management		X	X	X	The Supplier shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Supplier shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline. The Supplier shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.
2406	Privacy warning notices - prior to access			X	X	The Supplier shall ensure that mechanisms are in place to ensure users accept appropriate warning notices prior to information system access. At a minimum users must be warned that: i) Use of the information system is monitored, recorded and subject to audit ii) Unauthorised usage of the information system is prohibited iii) Unauthorised usage of the information system use is subject to criminal and civil penalties iv) In continuing, the user affirms consent to monitoring and recording of their activities
2407	Privacy warning notices - specific handling		X	X	X	The Supplier shall ensure that users accept appropriate warning notices prior to information system access where information systems contain information with specific handling requirements imposed by the UK or its International Partners. Such warnings must only be provided to authenticated users. At a minimum users must be warned that: i) The information system contains information with specific requirements imposed by the UK and/or international partner nations. ii) Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.
2408	Screen locking/timeouts		X	X	X	The Supplier shall have controls in place to automatically lock user sessions after a predefined period. The lock screen shall conceal all information previously displayed on the screen and prevent unauthorised viewing of data.
2409	Identify allowed programs		X	X	X	The Supplier shall identify software programs authorised to execute on the corporate environment. For all other programs employ a block by default, permit-by-exception policy.
2410	Review the list of approved software		X	X	X	The Supplier shall review and manage the list of authorised software programs at least every **90 days**.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2411	Secured Internet access		X	X	X	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (eg malicious sites, inappropriate content etc) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)
2412	Voice over Internet Protocol (VoIP)		X	X	X	The Supplier should establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and ensure controls are in place to authorise, monitor, and control the use of VoIP within the information system.
2413	Mobile code management		X	X	X	The Supplier shall define acceptable and unacceptable mobile code, and ensure controls are in place to identify, authorise, monitor, review and control the use of mobile code within the organisation.
2414	Communication authenticity protection		X	X	X	The Supplier shall use secure network management and communication protocols to protect session authenticity addressing communications protection at the session level.
2415	Automatically identify and address misconfigurations and unauthorised components				X	The Supplier shall employ automated mechanisms to detect misconfigured or unauthorised system components.
2416	Shared system resources			X	X	The supplier shall prevent unauthorised and unintended information transfer via shared system resources (e.g. registers, cache memory, main memory, hard disks).
2417	Authorise remote execution of privileged commands		X	X	X	The Supplier shall ensure that all remote users acquire appropriate authorisation prior to accessing and/or executing privileged functions.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2418	Baseline configurations and inventories		X	X	X	The Supplier shall implement, update and document system hardening procedures. Implement, update and document baseline configurations settings for all information technology products deployed in organisational systems; this shall include the restriction of user actions and of unsupported software and hardware.
2419	Obscure authentication information		X	X	X	The Supplier shall configure systems to obscure authentication information, for example, passwords to ensure that they are not displayed as cleartext when a user is inputting their credentials.
2420	Authentication feedback		X	X	X	The Supplier shall configure systems to minimise feedback information from failed logons to ensure that the system does not provide any information that would allow unauthorised individuals to compromise authentication mechanisms. e.g. explicitly stating that the password is the incorrect authentication component.
2421	Network Time Protocol (NTP)		X	X	X	The Supplier shall implement a Network Time Protocol (NTP) to a recognised authoritative source, to synchronise the clocks of every network device to ensure accurate and consistent timestamps for audit records on associated system logs.
2422	Physical and logical access restrictions		X	X	X	The Supplier shall define, document, approve, and enforce physical and logical access restrictions associated with changes to organisational systems.
2423	Trusted source repository		X	X	X	The Supplier shall identify, register and maintain an inventory of system components using automated tooling for those assets that support business Functions and protect Data in an asset register, and at a minimum, include data location and asset ownership information.
2424	Implement audit for stored credentials outside policy			X	X	The Supplier shall ensure administrator credentials are stored through an approved and secured storage mechanism (process/location/tools etc.) and **quarterly** audits are performed to ensure the control is consistently applied and functions appropriately.
2425	Use integrity verification tools				X	The Supplier shall implement an integrity verification tool to detect unauthorised changes to webfacing, critical software and firmware. Upon discovering discrepancies, the tool should automatically trigger the incident response process.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2426	Anti-malware capabilities		X	X	X	The Supplier shall ensure that anti-malware capabilities are regularly audited, to verify they are up to date, functional (e.g. performing real-time scans as well as periodic scans), managed, detect malware, report detections and update both malware signatures and software when new releases are available.
2427	Monitor/protect communications at boundaries		X	X	X	The Supplier shall monitor, control, and protect communications (information transmitted or received by organisational systems) at the external boundaries except as prohibited by Applicable Law and key internal boundaries of those organisational systems. This includes all staff including all remote workers to carry out their duties.
2428	Verify/limit access to external system connections		X	X	X	The Supplier shall control and limit connections to external systems by an allow-list on the network boundary.
2429	Verify/limit access from external system connections		X	X	X	The Supplier shall block unauthorised inbound connections by default. Inbound firewall rules are approved and documented by an authorised person, and include the business need within the documentation.
2430	External system connection review			X	X	The Supplier shall promptly remove or disable unnecessary firewall rules when they are no longer required or fulfil no business need.
2500	Resilient networks and systems	X	X	X	X	The Supplier shall build resilience against cyber-attack and system failure into their design, implementation, operation and management of systems that support the operation of business Functions and protection of Data.
2501	Design for resilience		X	X	X	The Supplier shall design the network and information systems supporting their Functions and protect Data to be resilient to cyber security incidents and system failure. Systems shall be appropriately segregated and resource limitations mitigated.
2502	Resilience preparation		X			The Supplier shall develop recovery plans for all systems that deliver Functions and protect Data.
2503	Resilience preparation with testing			X	X	The Supplier shall develop recovery plans for all systems that deliver Functions and protect Data. Recovery plans must also be tested at least annually with any deficiencies being recorded, risk assessed and resolved within defined timelines.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2504	Backups		X			The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation.
2505	Resilient backups			X	X	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation iii) Secure offsite storage supporting availability requirements iv) Regular backup recovery testing.
2506	Physical transport of backups			X	X	The Supplier shall protect the physical movement of media containing Data in transit using the following methodologies: i) Store backup media within a secured and locked container prior to transport. ii) Utilise a certified backup courier to transport backup drives/tapes. iii) Maintain a full chain of custody record. iv) Ensure that tracking information is recorded for all drives being transported. v) Implement appropriate cryptographic mechanisms to protect confidentiality.
2507	Deny traffic by default at interfaces		X	X	X	The Supplier shall ensure that firewalls must block every network connectivity path and network service not explicitly authorised by the appropriate Change Advisory Board (CAB). Traffic flow policy exceptions that are no longer supported by an explicit business need must be removed.
2508	Separate public and internal subnetworks		X	X	X	The Supplier shall implement network segmentation for publicly accessible system components to ensure logical and/or physical separation from internal network components.
2509	Managed email filtering		X	X	X	The Supplier shall implement appropriate tooling or methods to detect, block and report malicious or spam emails coming into the network. Such tooling or methods may include learning capabilities for more effectively identifying legitimate communications.
2510	Diagnostic programmes		X	X	X	The Supplier shall check all media containing diagnostic and/or test programs for malicious code prior to use on the organisational network.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2511	Maintenance activities		X	X	X	The Supplier shall ensure that relevant good practice tooling, techniques and mechanisms are authorised or provided to maintenance personnel in order to carry out their duties
2512	MFA for remote maintenance activities		X	X	X	The Supplier shall require multi-factor authentication to establish non local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
2513	Maintenance personnel supervision		X	X	X	The Supplier shall designate authorised, suitably qualified and experienced personnel to supervise maintenance personnel who do not possess the required physical access authorisations.
2600	Staff awareness and training		X	X	X	The Supplier shall ensure that staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of business Functions and protection of Data.
2601	Cyber security culture			X	X	The Supplier shall develop and maintain a positive cyber security culture which encourages employees to make information security part of their day-to-day activities and incentivises them for doing so.
2602	Cyber security training			X	X	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every **12 months** to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every **12 months** or when there are significant changes to the threat.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2603	Staff risk awareness		X	X	X	The Supplier shall ensure that managers, systems administrators, and users of organisational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organisational information systems. The Supplier shall review and update these security risks at least every **12 months** or when there is significant change within the organisation or threat.
2604	Acceptable Use Policy		X	X	X	The Supplier's Acceptable Use Policy shall consider and include appropriate enforcement of restrictions on: i) Use of social media, social networking sites, and external sites/applications ii) Posting organisational information on public websites iii) Use of organisation-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications iv) Enforce clear desk and clear screen requirements v) Handling of physical corporate assets outside the office environment vi) Locations for conducting duties vii) Remote activation of collaborative computing devices viii) Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
2605	Annual threat focused training feedback			X	X	The Supplier shall conduct practical exercises in awareness training for their organisation that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.
2700	Personnel pre-employment checks		X	X	X	The Supplier shall, unless prohibited by Applicable Law, perform appropriate background verification checks on Personnel that have access to Data upon hire. The verification checks shall include: i) Verifying credentials ii) Employment history iii) Qualification checks iv) Application or verification of BPSS (Baseline Personnel Security Standard)

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
2701	Personnel security vetting*		X	X	X	The Supplier shall define and implement a policy for applying BPSS and National Security Vetting (NSV) checks as appropriate for employees that support Functions and the protection of Data. *(*It is recognised that application of NSV is normally only possible once a contract requiring such is in place. Potential suppliers who do not meet this requirement at time of submission must, however, be willing and be able to enforce their staff through appropriate levels of vetting within a timescale agreed with the project delivery team following contract award*).
2702	Joiners, movers and leavers		X	X	X	The Supplier shall define and implement a joiners, movers and leavers policy to secure organisational hardware, software and systems.
2703	Whistleblowing		X	X	X	The Supplier shall define and implement training and processes for employees and contractors to identify and report suspicious activities and/or behaviour including violations of information security policies and procedures without fear of recrimination. The Supplier shall define and implement a disciplinary process to take action against employees who violate information security policies or procedures.
2704	Environmental controls		X	X	X	The Supplier shall, where appropriate, implement, install, and maintain the following environmental controls supporting Functions and protection of Data: i) Fire suppression systems ii) Temperature and humidity controls within a data centre or server room environment iii) Backup power technology (e.g. uninterruptible power supply, diesel generator, separate grid connection, etc.).
	Objective C: Detecting cyber security events The Supplier has capabilities which enable security defences to remain effective and detect cyber security events affecting, or with the potential to affect, Functions and protection of Data.					
3100	Security monitoring		X	X	X	The Supplier shall monitor the security status of the networks and systems supporting the operation of business Functions and protection of Data in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
3101	Monitor security controls		X	X		The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) Security events covered ii) Frequency of monitoring iii) Clearly defined roles and responsibilities iv) Escalation matrix.
3102	Continuously monitor security controls				X	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24x7x365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring iv) Clearly defined roles and responsibilities v) Escalation matrix.
3103	Securing logs			X	X	The Supplier shall hold logging data securely and grant read access only to accounts with business needs. The Supplier shall protect audit tools from unauthorised access, modification and deletion. Logging data shall be retained and protected from deletion to a documented retention period, after which it shall be deleted.
3104	Security event triage			X	X	The Supplier shall provide evidence from their monitoring tool of security incidents to verify the reliability of identified and triggered alerts for triage.
3105	Identifying security incidents			X	X	The Supplier shall contextualise alerts with knowledge of the threat and their systems, and engage Incident Response when an incident (confirmed or otherwise) is identified.
3106	Monitoring tools and skills			X	X	The Supplier shall ensure that monitoring staff skills, tools and roles, including any that are outsourced, reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have contextual knowledge of the Functions and requirements for the protection of Data.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
3107	Create, retain and correlate audit logs		X	X	X	The Supplier shall generate event logs for systems that support the operation of Functions and protection of Data. The following criteria apply: i) Logs are archived for a minimum of **12 months** ii) Logs capture (as a minimum) date, time (from a single NTP source), user ID, device accessed and port used iii) Logs capture key security event types (e.g. critical files accessed, user accounts generated, multiple failed login attempts, logging failures from devices, events related to systems that have an internet connection) iv) Access to modify system logs is restricted v) Logs and security event logs can be made available upon request vi) Store audit records in a repository that is part of a physically different system vii) The Supplier shall ensure that systems logs are reviewed at least **weekly** to identify system failures, faults, or potential security incidents and corrective actions are taken to resolve or address issues within a reasonable timeframe viii) Review, at least every **6 months** the event types selected for logging purposes to ensure these still meet business requirements ix) Capture the operational status of the logging system and alert on any failures which impact the system's operational capacity.
3108	Audit reduction and report generation		X	X	X	The Supplier shall provide and implement an appropriate audit record reduction and report generation capability that: i) supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and ii) does not alter the original content or time ordering of audit records.
3109	Integration of records with incident management		X	X	X	The Supplier shall integrate audit record review, triage, analysis, and reporting processes with organisational governance and incident management structure.
3110	Monitor alerts/advisories and take action			X	X	The Supplier shall monitor system security alerts and advisories and take action in response.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
3200	Proactive security event discovery		X	X	X	The Supplier shall detect, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of business Functions and protection of Data even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).
3201	System abnormalities for attack detection		X	X	X	The Supplier shall define examples of abnormal system behaviour to aid in detecting malicious activity that is otherwise hard to identify. The Supplier shall take appropriate action upon identifying this behaviour.
3202	Proactive attack discovery			X	X	The Supplier shall implement reasonable and proportionate measures to detect malicious activity affecting, or with the potential to affect, the operation of Functions and protection of Data.
3203	Use indicators of compromise from alerts		X	X	X	The Supplier shall monitor system security alerts and advisories and take action in response using agreed and managed indicators of compromise.
3204	Presence of unauthorised system components		X	X	X	The Supplier shall implement proportionate measures to: i) Detect the presence of unauthorised hardware, software, and firmware components within the system using tooling ii) Take the following actions when unauthorised components are detected: disable network access by such components; isolate the components; notify systems administrators and/or security operations teams.
	Objective D: Minimising the impact of cyber security incidents The Supplier shall ensure capabilities exist to minimise the adverse impact of a cyber security incident on the operation of Functions and protection of Data, including the restoration of Functions and Data.					
4100	Response and recovery planning		X	X	X	The Supplier shall implement well-defined and tested incident management processes that aim to ensure continuity of business Functions and protection of Data in the event of system or service failure. Mitigation activities are designed and where possible automated to contain or limit the impact of a compromise.
4101	Response plan			X	X	The Supplier shall have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of business Functions and protection of Data and covers a range of incident scenarios.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
4102	Response and recovery capability			X	X	The Supplier shall have the capability to enact their incident response plan, including effective limitation of impact on the operation of Functions and protection of Data. During an incident, the Supplier shall enact processes and capabilities to provide access to information sources on which to base their response decisions to coordinate incident handling activities with contingency planning activities.
4103	Testing and exercising			X	X	The Supplier shall carry out exercises to test response plans at least every **12 months**, using past incidents that affected their (and other's) organisation, and scenarios that draw on threat intelligence and risk assessments.
4104	Incident handling capability		X	X	X	The Supplier shall establish an operational incident handling capability for organisational information systems that is consistently applied across the organisation and includes: i) Adequate preparation, detection, forensic analysis, containment, recovery, and user response activities ii) Tracking, documenting, and reporting incidents to appropriate organisational officials and/or authorities iii) Sufficient rigour, intensity and scope.
4105	Exfiltration tests			X	X	The Supplier shall conduct data exfiltration tests at the network boundaries at least every **12 months**. These tests must be conducted against both authorised and covert channels.
4106	Attempted unauthorised connections from staff		X	X	X	The Supplier shall audit the identity of internal users associated with denied communications.
4200	Lessons learned		X	X	X	The Supplier shall, when an incident occurs, incorporate root cause analysis and lessons learned information from incident response activities into incident response procedures, training and testing. The Supplier shall implement the resulting improvements immediately or, at minimum, within **30 days** of the completion of the root cause analysis.
4201	Business Continuity Risk Assessments			X	X	The Supplier shall perform Business Continuity Risk Assessments to determine relevant risks, threats, and likelihood & impact of a service outage or Data Breach. The Supplier shall record the output of these Risk Assessments within a risk register along with the required controls and/or procedures to mitigate or remove the risk and/or threat.

Control ID	Control Short Name	Control Levels				Control Requirements
		L0	L1	L2	L3	
4202	Operation resilience for equipment				X	The Supplier shall assess the requirement for redundant networking and telecommunication systems to protect Functions and Data. Where required, the Supplier shall implement and protect these systems.

4 Acknowledgements

Defence Cyber Protection Partnership (DCPP) Controls Working Group Members - https://www.gov.uk/guidance/defence-cyber-protection-partnership

Defense Contract Management Agency - https://www.dcma.mil/

National Cyber Security Centre (NCSC) - https://www.ncsc.gov.uk/

National Institute of Standards and Technology (NIST). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Series 800-171, Rev 2, February 2020, Includes updates as of January 28, 2021. https://doi.org/10.6028/NIST.SP.800-171r2

National Institute of Standards and Technology (NIST). Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171, NIST 800-172, Rev 1, February 2021. https://doi.org/10.6028/NIST.SP.800-172

MITRE ATT&CK® - https://attack.mitre.org/

United States Department of Defense - https://www.defense.gov

Section 3

Normative References

1 The publications shown below are referred to in the text of this standard. Publications are grouped and listed in alpha-numeric order.

Note: Def Stan's can be downloaded free of charge from the DStan web site by visiting **<**http://dstan.uwh.diif.r.mil.uk/**>** for those with RLI access or **<**https://www.dstan.mod.uk**>** for all other users. All referenced standards were correct at the time of publication of this standard (see 2, 3 & 4 below for further guidance), if you are having difficulty obtaining any referenced standard please contact the UK Defence Standardization Help Centre in the first instance.

Def Stans

Number	Title

STANAGs

Number	Title

Allied Publications

Number	Title

Other References

Standard Type	Standard Name

2 Reference in this Standard to any normative references means in any Invitation to Tender or contract the edition and all amendments current at the date of such tender or contract unless a specific edition is indicated. Care should be taken when referring out to specific portions of other standards to ensure that they remain easily identifiable where subsequent amendments and supersession's might be made. For some standards the most recent editions shall always apply due to safety and regulatory requirements.

3 In consideration of clause 2 above, users shall be fully aware of the issue, amendment status and application of all normative references, particularly when forming part of an Invitation to Tender or contract. Correct identification of standards is as defined in the ITT or contract.

4 DStan can advise regarding where to obtain normative referenced documents. Requests for such information can be made to the UK Defence Standardization Help Centre. Details of how to contact the Help Centre are shown on the outside rear cover of Defence Standards.

Definitions

For the purpose of this standard, ISO/IEC Guide 2 'Standardization and Related Activities – General Vocabulary' and the definitions shown below apply.

Definition	Description

Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
BPSS	Baseline Personnel Security Standard
BYOD	Bring Your Own Device
CAB	Change Advisory Board
CCTV	Closed Circuit Television
CRP	Cyber Risk Profile
CSM	Cyber Security Model
CVSS	Common Vulnerability Scoring System
DCPP	Defence Cyber Protection Partnership
Def Stan	Defence Standard
DEFCON	Defence Condition
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DStan	UK Defence Standardization
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
ID	Identification
IdAM	Identity and Access Management
ITT	Invitation to Tender
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MOD	Ministry of Defence
NSV	National Security Vetting
NTP	Network Time Protocol
PII	Personally Identifiable Information

RFID	Radio Frequency Identification
SPF	Sender Policy Framework
UK	United Kingdom
USB	Universal Serial Bus
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access

Changes since previous issue

The changes incorporated in this issue are shown below. For more information please contact DStan through the UK Defence Standardization Help Centre. Details of how to contact the Help Centre are shown on the outside rear cover of Defence Standards.

Clause	Page	Change	Change Reason
1	2-2	Clause 1 (‘Scope’) has been updated.	To clarify that the scope of this standard is the Supplier’s overarching corporate or enterprise environment and to provide additional context.
2	2-3	Clause 2 ('Reporting of Incidents') from Issue 3 has been removed.	The clause duplicated the obligation in DEFCON 658.
2	2-3	Annex A (‘Cyber Risk Profiles’) from Issue 3 has been removed. In its place, Clause 2 now introduces the new ‘Cyber Risk Profiles’ and Clause 3 contains the new ‘Cyber Risk Profile Requirements Table’.	The new Cyber Risk Profiles are the core content of the updated standard.
2	2-3	Annex B from Issue 3 (‘MOD Identifiable Information’) has been removed.	MOD Identifiable Information is no longer referenced within the standard.

Defence Standards are published by and obtainable from:

Defence Equipment and Support

UK Defence Standardization

Kentigern House

65 Brown Street

GLASGOW

G2 8EX

UK Defence Standardization Help Centre

Please direct any enquiries via the Standardization Management Information System (StanMIS) Help Centre.

To access the StanMIS Help Centre please select either http://stanmis.gateway.isg-r.r.mil.uk/ (for MOD and industry users with MOD Core Network (MCN) access) or https://www.dstan.mod.uk/StanMIS/ (for all other users), and, after logging in, please follow the link to the Help Centre. If required, users can also register for an account from the login screen.

File Reference

The DStan file reference relating to work on this standard is 01737/2023.

Contract Requirements

When Defence Standards are incorporated into contracts, users are responsible for their correct application and for complying with contractual and statutory requirements. Compliance with a Defence Standard does not in itself confer immunity from legal obligations.

Revision of Defence Standards

Defence Standards are revised as necessary by an up-issue or amendment. It is important that users of Defence Standards ensure that they are in possession of the latest issue or amendment. Information on all Defence Standards can be found on the DStan Websites https://www.dstan.mod.uk and http://dstan.gateway.isg-r.r.mil.uk/index.html, updated weekly. Any person who, when making use of a Defence Standard, encounters an inaccuracy or ambiguity is encouraged to notify UK Defence Standardization (DStan) without delay in order that the matter may be investigated, and appropriate action taken.