FOI Request Security Compliance Service

ICTPA Deed from which WP3 was derived, extracts relating to Security

13.6 **Special Terms and Conditions**
(a) A special term and condition is a condition that is additional to, or Modifies, the terms and conditions under this Deed or a Service Tower (**Special Term and Condition**).

(b) The Commonwealth may, in its absolute discretion, include any number of Special Terms and Conditions in a Request for Quotation (and the associated Work Order) provided that those terms and conditions:
(i) are consistent with the Deed Objectives;

(ii) do not Modify the liability, indemnity, privacy, security or confidentiality obligations under this Deed or the relevant Service Tower Terms; and

(iii) do not Modify clause 13 of this Deed.
(c) A Special Term and Condition will only apply where the relevant Special Term and Condition is specified in a signed Work Order and satisfies the requirements of clause 13.6(b).

19 Government Furnished Facilities
19.1 **General**
(a) The Commonwealth may permit the Supplier and the Supplier's Personnel access to and use of GFF for the purpose of carrying out its obligations under a Contract.

(b) The Supplier acknowledges and agrees that any rights that the Commonwealth may grant to the Supplier and the Supplier's Personnel to occupy and use GFF:
(i) are non-exclusive rights;

(ii) are personal rights in contract;

(iii) do not give the Supplier or the Supplier's Personnel any interest or estate in the GFF (whether equitable or otherwise); and

(iv) do not create the relationship of landlord and tenant between the Supplier and the Commonwealth.
(c) Where the Commonwealth provides access to any GFF, the Supplier must ensure that it and the Supplier's Personnel comply with all Commonwealth requirements, directions and Commonwealth Policies with respect to GFF, including:
(i) policies with respect to work health and safety, sexual and racial discrimination and security; and

(ii) induction requirements with respect to GFF.
(d) The Supplier must (and must ensure that the Supplier's Personnel) at all times when accessing or using GFF:
(i) use GFF in an efficient manner for the sole purpose of providing the Services in accordance with the relevant Contract;

(ii) keep GFF clean and tidy;
(iii) not do anything that is, or may be, considered by the Commonwealth to be dangerous or offensive; and

(iv) comply with the requirements of the Commonwealth concerning the storage and removal of waste and debris.
(e) The Commonwealth may deny or suspend the Supplier's or any Supplier Personnel's access to any GFF where the Supplier or the Supplier's Personnel do not comply with the provisions of this clause or any other security and work health and safety obligations under the Deed and the relevant Contract.

19.4 **Security incidents**
Without limiting the Supplier's other security obligations under this Deed, the Supplier must:
(a) notify the Commonwealth immediately of any breach or suspected breach of security or unauthorised entry to, or use of, the GFF or other Commonwealth property during the period that the Supplier is providing the Services; and
(b) within 24 hours of any incident referred to in clause 19.4(a) occurring, provide the Commonwealth with a written report of the incident and co-operate with any investigation by the Commonwealth or Australian Federal or State police.

20 Government Furnished Material
(a) Except as otherwise specified in a Work Order, the Supplier will provide all necessary materials, equipment and resources for the performance of the Services in accordance with the relevant Contract.

(b) The Commonwealth will only provide the Supplier with access to materials, equipment, resources and other GFM where specified in a Work Order or otherwise agreed by the Commonwealth.

(c) The Commonwealth will provide all GFM in accordance with this clause and at the place and times specified in the Work Order or as otherwise agreed by the Commonwealth.

(d) Unless the Commonwealth advises otherwise, GFM remains the property of the Commonwealth. The Commonwealth is entitled to identify GFM as the Commonwealth's property and the Supplier must preserve any means of identification.

(e) On receipt of GFM, the Supplier must:
(i) inspect the GFM for physical damage, any Defects or deficiencies which impact on, or are likely to impact on, the intended use of the GFM; and

(ii) report its satisfaction or dissatisfaction with the GFM in writing to the Commonwealth Contract Manager within 5 Business Days.
(f) The Supplier must:
(i) take all reasonable care of, and be liable for loss of or damage to, GFM in its care, custody or control; and

(ii) utilise the GFM in performing the Services with a high degree of professional skill and care and in accordance with this Deed and the relevant Contract.
(g) The Supplier must return GFM (other than consumable items of GFM) to the Commonwealth as specified in the relevant Contract or as directed by the Commonwealth Contract Manager.

(h) The Supplier acknowledges and agrees that the Commonwealth does not give any warranty or representation about the suitability or fitness of any GFM for any particular use or application.

(i) The Supplier must not without the prior written approval of the Commonwealth Contract Manager:
(i) use GFM other than for the purposes of providing the Services in accordance with the relevant Contract;

(ii) Modify GFM;

(iii) transfer possession or control of GFM to any other party;

(iv) communicate or divulge GFM to any other party; or

(v) create or allow to be created any security interest, lien, charge, mortgage or encumbrance over any GFM.
(j) The Supplier must not use GFM other than for a purpose for which the GFM was designed, manufactured or constructed.

(k) The Commonwealth may notify the Supplier of any Intellectual Property Rights applicable to the GFM, and the Supplier must not act contrary to the existence of such rights.

(l) The Commonwealth warrants and represents that is has all approvals, rights, title, licences, interests, permits and property necessary with regards to GFM.2

25 Compliance with Laws and Commonwealth Policies
(a) Without limiting any other obligation under this Deed, the Supplier must ensure that, in the performance of this Deed or any Contract, it complies with and ensures that the Supplier's Personnel comply with, the Laws from time to time in force in the State, Territory or other jurisdictions (including overseas) in which any part of this Deed or any Contract is to be carried out.

(b) The Supplier must comply with, and must ensure that the Supplier's Personnel comply with:
(i) the following Commonwealth Policies of general application, as relevant or applicable to this Deed, any Contract and the Services:
(A) Conflicts of interest; Gifts, hospitality and sponsorship; Notification of post separation employment; Management and reporting of unacceptable behaviour; and Incident reporting and management policies as detailed in the DPPM, DI(G) PERS 25-6, DI(G) PERS 25-7, DI(G) PERS 25-4, DI(G) PERS 35-3, DI(G) ADMIN 45-2 and DI(G) ADMIN 67-2 and *Defence and the Private Sector – An Ethical Relationship*;
(B) Work Health and Safety, Hazardous Substances, Defence Environmental, Ozone Depleting Substances and Synthetic Greenhouse Gases, Public Interest Disclosure and Workplace Gender Equality policies as detailed in the DPPM;

(C) Defence and industry policy as detailed in the *Defence and Industry Policy Statement* and Australian Industry Capability policy as detailed in the DPPM;

(D) the Defence Security Principles Framework3;

(E) Defence stocktaking policy as detailed in DI(G) LOG 4-3-014;

(F) Fraud control policy as detailed in DI(G) FIN 12-1;

(G) Information and Communications Technology Manual (ICTMAN); and

(H) *Defence Work Health and Safety Manual, Volume 2, Part 5, Chapter 1*; and
(ii) any other Commonwealth Policies and specific requirements set out in a Work Order.

40.2 **Access by the Commonwealth**
For the purpose of the Commonwealth exercising its rights under clauses 39 and this clause 40:
(a) the Commonwealth may, at reasonable times and on giving reasonable notice to the Supplier:
(i) access the premises of the Supplier to the extent necessary to conduct audits;

(ii) require the provision by the Supplier or the Supplier's Personnel of records and information in a data format and storage medium accessible by the Commonwealth; and

(iii) inspect and copy documentation, books and records (including ICTPA Documents) in the custody or under the control of the Supplier or the Supplier's Personnel;
(b) the Supplier must provide access to its computer hardware and software to the extent necessary for the Commonwealth to exercise its rights, and provide the Commonwealth with any reasonable assistance requested by the Commonwealth to use that hardware and software; and

(c) the Commonwealth must:
(i) use reasonable endeavours to ensure that audits performed by the Commonwealth do not unreasonably disrupt in any material respect the Supplier's performance of its obligations under this Deed or any Contract or the Supplier's provision of services to other customers; and
(ii) comply with the Supplier's reasonable security policies.

45 Confidentiality

45.6 **No reduction in privacy and security obligations**
Nothing in this clause 45 derogates from any obligation which either party may have under the Privacy Act in relation to the protection of Personal Information.

46.3 **Safeguarding Commonwealth Data**
(a) The Supplier must establish and maintain safeguards against the destruction, unauthorised disclosure or access, loss or alteration of Commonwealth Data in the possession or control of the Supplier that:
(i) are no less rigorous than those notified by the Commonwealth to the Supplier or, if the Commonwealth does not specify any safeguards, no less rigorous than the safeguards that can be reasonably expected in the provision of services similar to the Services; and

(ii) complies with all Laws, and any procedures or requirements specified by the Commonwealth, from time to time.
(b) The Supplier agrees that the Commonwealth may, at any time, with reasonable notice, conduct a security audit of the Supplier's compliance with this clause 46.

46.5 **Commonwealth Data Protection Plan**

(a) If specified in a Work Order, the Supplier must develop for approval by the Commonwealth by the due date specified in the Work Order, a Commonwealth Data Protection Plan (**CDPP**) that sets out how the Supplier and the Commonwealth will deal with and discharge their obligations in respect of Commonwealth Data (including Personal Information) during the provision of the Services. The CDPP must:
(i) be consistent with the requirements of this Deed and any Contract (including this clause 46 and clause 47);

(ii) be consistent with the requirements of the Privacy Act;

(iii) specifically deal with cybercrime risks, including unauthorised access;

(iv) be consistent with the Defence Security Principles Framework; and

(v) set out the steps and processes that the Supplier and the Commonwealth will follow to protect Commonwealth Data from unauthorised access, use, misuse, destruction or loss.
(b) The Supplier must comply with the approved CDPP, unless the Commonwealth otherwise agrees in writing.

47 Commonwealth security
47.1 **Security requirements**
(a) If the Supplier or Supplier's Personnel require access to any Commonwealth Premises under the control or responsibility of the Commonwealth, the Supplier must
(i) comply with any security requirements (including those contained in the Defence Security Principles Framework (**DSPF**))4 notified to the Supplier by the Commonwealth Deed Manager or relevant Commonwealth Contract Manager; and

(ii) ensure that the Supplier's Personnel are aware of and comply with the Commonwealth's security requirements.
(b) The security classification of the Services will be up to and including the level specified in the Work Order. The Supplier must:
(i) if required in the Work Order, obtain and maintain membership of the Defence Industry Security Program (**DISP**) in accordance with Part 2:42 of the DSPF;

(ii) if not required to be a member of the DISP, comply with the classification and protection of official information requirements of Part 2:30 of the DSPF;

(iii) ensure that all of the required Supplier Personnel (if any) possess a personnel security clearance of the level specified in the Work Order, and comply with the requirements and procedures of Part 2:20 of the DSPF. The Supplier is responsible for all costs associated with obtaining and maintaining security clearances for its Personnel; and
(iv) possess the facility accreditation (if any) and ICT system accreditation (if any) specified in the Work Order and comply with the requirements and procedures of Part 2:4 of the DSPF.
(c) With respect to security classified information, the Supplier must:
(i) ensure that no security classified information furnished or generated under this Deed or any Contract is released to a third party, including a representative of another country, without prior written approval of the originator through the Commonwealth Deed Manager or relevant Commonwealth Contract Manager (as relevant);

(ii) promptly report to the Commonwealth Deed Manager or Commonwealth Contract Manager (as relevant) any security incident, as defined by the DSPF, including instances in which it is known or suspected that security classified information furnished or generated under this Deed or any Contract has been lost or disclosed to unauthorised parties, including a representative of another country; and

(iii) ensure that all security classified information transmitted between the parties or a party and a subcontractor, in Australia, whether generated in Australia or overseas, is subject to the terms of Part 2:33 of the DSPF.
(d) Where COMSEC material is transmitted in Australia by the Supplier or the Supplier's Personnel, the Supplier must ensure that:
(i) without limiting clause 47.1(c)(iii), all COMSEC material transmitted between the parties or a party and a subcontractor in Australia is subject to the special security provisions of Part 2:53 of the DSPF; and

(ii) all security classified information transmitted between the parties or a party and a subcontractor located overseas whether generated in Australia or by another country must be subject to the laws of the overseas country regarding the custody and protection of security classified information and to any bilateral security instrument between Australia and the overseas country.
(e) Where COMSEC material is transmitted overseas by the Supplier or the Supplier's Personnel, the Supplier must ensure that:
(i) all COMSEC material transmitted between the parties or a party and subcontractor located overseas must be subject to approval in the first instance by the Director Australian Signals Directorate (**ASD**), in respect of Australian COMSEC material, and by the respective COMSEC authorities in other countries in respect of COMSEC material originating from those countries; and
(ii) once approved for release, the material must be subject to the laws of the overseas country regarding the custody and protection of COMSEC material as determined by the Director ASD and to any bilateral security instrument between Australia and the overseas country.
(f) The Supplier must ensure the requirements of clause 47 are included in all subcontracts where the subcontractor requires access to any Commonwealth Premises, or to security classified information, in order to perform the obligations of the subcontract.

47.2 **Access to the Commonwealth's Premises, systems and files**
(a) Without limiting any other obligation under this Deed or any Contract, the Supplier must ensure that:
(i) direct or indirect access to the Commonwealth's Premises, software, hardware, systems and files is:
(A) not facilitated by the Supplier, other than in accordance with this Deed or the relevant Contract;

(B) absolutely restricted to those Personnel of the Supplier who have been approved by the Commonwealth and who have a need for such access;

(C) not for the Supplier, the Supplier's Personnel or any third party's personal gain, use or benefit; and

(D) limited to the minimum access necessary to enable the Supplier to comply with its obligations under this Deed and the relevant Contract; and
(ii) any access by the Supplier or the Supplier's Personnel to the Commonwealth's Premises, software, hardware, systems and files:
(A) is clearly recorded with full details of the access, including the name of the Supplier's Personnel and the date of his or her access; and

(B) complies with the requirements set out in the relevant Contract or as reasonably required by the Commonwealth.
(b) Unless otherwise specified in a Work Order, the Supplier is:
(i) only permitted to remotely access the Commonwealth's development and test environments; and

(ii) not permitted to remotely access any of the Commonwealth's production environments.
(c) Where the Supplier is permitted to remotely access the Commonwealth's production environment, the Supplier must ensure that it complies with all privacy, security and confidentiality obligations under this Deed and the relevant Contract.
(d) The Supplier must (having due regard for the security concerns inherent in remote access and the Commonwealth's security policies) take appropriate action and maintain appropriate protocols to satisfy its obligations under this Deed and any Contract for the protection and security of all data provided in connection with this Deed or any Contract, including the Commonwealth's Confidential Information, Commonwealth Data, and Personal Information.

47.3 **Notification of security and cyber incidents**
(a) If the Supplier becomes aware of any actual or suspected:
(i) action taken through the use of computer networks that result in an actual or potentially adverse effect on the Supplier's information system and/or Commonwealth Data residing on that system (**Cyber Incident**); or

(ii) other security incident or security breach (including any unauthorised access, use, misuse, damage or destruction of Commonwealth Data, Commonwealth Confidential Information or Personal Information) (**Other Incident**),

the Supplier must:
(iii) notify the Commonwealth immediately (and no longer than 12 hours after becoming aware of the Cyber Incident or Other Incident);

(iv) comply with any directions issued by the Commonwealth in connection with the Cyber Incident or Other Incident, including in relation to:

(A) notifying the Australian Cyber Security Centre, or any other relevant body, as required by the Commonwealth;
(B) obtaining evidence about how, when and by whom the Supplier's information system and/or the Commonwealth Data has or may have been compromised, providing it to the Commonwealth on request, and preserving and protecting that evidence for a period of up to 12 months;
(C) implementing any mitigation strategies to reduce the impact of the Cyber Incident or Other Incident or the likelihood or impact of any future similar incident; and
(D) preserving and protecting Commonwealth Data (including as necessary reverting to any backup or alternative site or taking other action to recover Commonwealth Data).

(b) The Supplier must ensure that:
(i) all subcontracts and other supply chain arrangements, which may allow or cause access to Commonwealth Data, contain no provisions that are inconsistent with clauses 46 and 47; and

(ii) all Supplier Personnel (including to avoid doubt, all subcontractors) who have access to Commonwealth Data comply with clauses 46 and 47.
(c) The Supplier acknowledges that if any Supplier Personnel loses their security clearance or causes a security breach, the Commonwealth may:
(i) after consultation with the Supplier, require the replacement of such Supplier Personnel; or

(ii) immediately terminate the relevant Contract.

47.4 **Supplier's responsibility to prevent Harmful Code**

The Supplier must take reasonable steps to detect and prevent any Harmful Code from being introduced by the Supplier into (or sent from) any Deliverables, or the Commonwealth's systems, including by:

(a) use of the most appropriate and up-to-date virus detection software for preventing and detecting Harmful Code;

(b) implementing practices and procedures that are consistent with industry best practice;

(c) pro-actively monitoring known threats of Harmful Code; and

(d) informing the Commonwealth of any Harmful Code and the steps necessary to avoid the introduction of Harmful Code.

47.5 **Procedure if Harmful Code is found**

(a) If the Supplier becomes aware that any Harmful Code has been introduced into any Deliverables or the Commonwealth's systems, the Supplier must:

(i) notify the Commonwealth immediately;

(ii) provide all information reasonably requested by the Commonwealth in relation to the Harmful Code, its manner of introduction and the effect the Harmful Code has had or is likely to have;

(iii) take all necessary remedial action to:

(A) eliminate the Harmful Code and prevent its re-occurrence; and

(B) rectify any consequences of the Harmful Code (to the extent that they are capable of rectification);

(iv) if the Harmful Code causes a loss of data or loss of operational efficiency, assist the Commonwealth to mitigate the losses and restore the efficiency and/or data;

(v) retain evidence and logs regarding the incident to help in determining the cause, damage and likely source; and

(vi) ensure that sufficient Supplier resources and technology are available to meet its obligations under this clause.

(b) Subject to clause 47.5(d), the Supplier must perform its obligations under this clause at no additional cost to the Commonwealth.

(c) To the extent that the Harmful Code was introduced by the Supplier or the Supplier's Personnel, the Supplier must pay the costs and expenses incurred by the Commonwealth in connection with the activities set out in clauses 47.5(a)(i) to 47.5(a)(vi).

(d) If Harmful Code was introduced by the Commonwealth or a third party and the Supplier incurs costs and expenses in connection with the activities set out in clauses 47.5(a)(i) to 47.5(a)(vi), the parties will, in good faith, agree the reasonable amount of costs and expenses that the Commonwealth will reimburse to the Supplier for the performance of these activities. To avoid doubt, the Supplier's immediate priority must be to conduct, or assist the Commonwealth to conduct, the remedial activities contemplated in clauses 47.5(a)(i) to 47.5(a)(vi).

51.2 **Limitation of liability**
(a) Subject to clause 51.2(b), the liability of each party arising in connection with any Contract is limited to:
(i) the amount specified in the Work Order; or

(ii) if the Supplier is a member of a scheme approved under the Professional Standards Legislation that limits the Supplier's liability, the amount limited by that relevant scheme.
(b) Any limitation of liability under clause 51.2(a) does not apply in relation to liability for any:
(i) personal injury (including sickness and death);

(ii) loss of, or damage to, tangible property;

(iii) infringement of Intellectual Property Rights or Moral Rights;

(iv) breach of the Supplier's or the Supplier's Personnel's obligations relating to security, privacy and the protection of Confidential Information, Personal Information or Commonwealth Data;

(v) fraudulent, unlawful or wilfully wrong act or omission of the Supplier or the Supplier's Personnel; and

(vi) where the Supplier is a member of a scheme approved under the Professional Standards Legislation, any liability that is not limited by the relevant Professional Standards Legislation.
(c) Unless specified otherwise in the Work Order, the limitation of liability specified in clause 51.2(a) applies in respect of each single occurrence or a series of related occurrences arising from a single cause.

59 Indemnities
59.1 **Requirement to indemnify**
The Supplier indemnifies the Commonwealth and its Personnel against any Losses sustained or incurred by the Commonwealth and its Personnel as a result of a Claim made or threatened by a third party arising out of or in connection with:
(a) any act or omission of the Supplier or the Supplier's Personnel that causes:
(i) personal injury (including sickness and death) to any person;

(ii) loss of, or damage to, tangible property;
(b) any fraudulent, negligent, unlawful or wilfully wrong act or omission of the Supplier or the Supplier's Personnel;

(c) a breach of the Supplier's or the Supplier's Personnel's obligations relating to security, privacy and the protection of Confidential Information, Personal Information or Commonwealth Data; and

(d) an allegation that any Services or Deliverables (including the use of any Services or Deliverables) infringes the Intellectual Property Rights or Moral Rights of the third party,
Deed of Standing Offer 83 PREFERRED TENDERER VERSION

that arises in connection with this Deed or any Contract.

61.3 **Breach of a material provision**

Without limitation, for the purposes of clauses 61.1(a) and 61.2(a), each of the following constitutes a breach of a material provision:
(a) a breach of warranty under clause 15 (Warranties);

(b) a failure to comply with clause 30 (Work health and safety);

(c) a failure to comply with clause 32 (Supplier's Personnel);

(d) a failure to comply with clause 41 (Intellectual Property);

(e) a failure to comply with clause 42 (Moral rights);

(f) a failure to comply with clause 44 (Protection of Personal Information);

(g) a failure to comply with clause 45 (Confidentiality);

(h) a failure to comply with clause 46 (Commonwealth Data);

(i) a failure to comply with clause 47 (Commonwealth security);

(j) a failure to notify the Customer of a conflict of interest under clause 54 (Conflict of interest);

(k) a failure to comply with clause 58 (Insurance); and

(l) a failure to comply with clause 66.8 (Assignment and novation).

66.9 Survival
Any provision of this Deed or any Contract (including, to avoid doubt, any Special Terms and Conditions or Service Tower Terms) which expressly or by implication is intended to survive the termination or expiry of this Deed or any Contract will survive such termination or expiry, including:
(a) clause 30 (Work health and safety);

(b) clause 32.6(h) (Subcontractors);

(c) clause 35 (Post Commonwealth separation employment);

(d) clause 39 (Books and record keeping);

(e) clause 40 (Audit and access);

(f) clause 41 (Intellectual Property);

(g) clause 42 (Moral rights);

(h) clause 43 (Escrow);

(i) clause 44 (Protection of Personal Information);

(j) clause 45 (Confidentiality);

(k) clause 46 (Commonwealth Data);

(l) clause 47 (Commonwealth security);

(m) clause 48 (Public statements and announcements);

(n) clause 51 (Liability);

(o) clause 57 (Guarantees and security);

(p) clause 58 (Insurance), as it relates to professional indemnity insurance or errors and omissions insurance;

(q) clause 59 (Indemnities);

(r) clause 60 (Dispute resolution);

(s) clause 63 (Consequences of expiry or termination);

(t) clause 64 (Right of the Commonwealth to recover money);

(u) clause 65 (Transition-out-Obligations); and

(v) this clause 66.9 (Survival).

Deed Glossary

Test	a test carried out to determine whether a Deliverable or a Modification to a Deliverable meets the relevant Acceptance Criteria, and may include (as applicable) User Acceptance Testing, unit testing, implementation testing, End-To-End Testing, security testing, regression testing and other acceptance testing.

WP3 Statement of Work extracts relating to Security.

2.1 General

2.1.1 The Supplier shall provide all activities and tasks related to the lifecycle support and management of the applications, including:

a) Sustainment services for the provision of on-going, in-service support and maintenance of applications, such as:

(i) Maintenance, support and management;

(ii) Design and configuration;

(iii) Development, upgrade and Minor Enhancements;

(iv) Documentation, communication, consultancy, stakeholder engagement ITSM; and

(v) Security accreditation and maintenance, configuration, Australian Government Information Security Manual (ISM) and audit compliance;

2.8 Other Services

2.8.1 The Supplier may be required to provide Other Services at the request of Defence. These Other Services may include:

a) Business support, for example developing business work procedures and work instructions;

b) Strategic program support, for example assisting in identifying and managing the impacts of other Defence projects or initiatives;

c) Specialist assurance or advice, for example providing familiarisation with available functionality and its utilisation; and

d) Extension of services to out of scope applications, for example conducting interface activities to other Defence applications not already specified.

e) Provision of support to the Commonwealth in security, financial and quality assurance audits concerning all delivered services, data, documents and processes, including the implementation of audit findings; and

f) Conducting interface activities to other Commonwealth applications not already specified.

3.2 Application Sustainment

3.2.7 Security management, including but not limited to:

a) Service design;

b) Security control implementation;

c) Security validation for in-scope services;

d) Investigation of security occurrences for in-scope services; and

e) Security review and reporting.

3.2.18 Conduct or coordinate Application Administration, including but not limited to:

a) General systems administration and configuration settings;

b) Server operation and administration support and coordination;

c) Database administration;

d) Middleware administration and configuration settings;

e) Interface (connection) maintenance;

f) Performance analysis and tuning measures;

g) Application security;

h) Archive administration; and

i) Interface control and administration.

3.3 Application Development

3.2.19 Conduct Application-Specific Services, including but not limited to:

a) Batch-input session monitoring and administration;

b) Data load management;

c) Monitor upload jobs including restarts;

d) Early watch alerts monitoring;

e) Batch processing monitoring;

f) Custom Code Management;

g) Manage Source Code Security;

h) Security logs and extracts as required;

i) Maintain Security accreditation; and

j) Documentation maintenance, as required.

3.3.8 Integration test, including but not limited to:

a) Integration test execution;

b) Integration test, technical;

c) Integration test, functional;

d) Integration test, security (for changes deemed to have a potential security impact);

e) Integration test, regression; and

f) Integration test exception management.

3.3.5 Technical requirements, including but not limited to:

a) Detailed tech requirement specification; and

b) Security impact review.

4. 1. Outcomes Framework (Part A – Process Outcomes – E1 Outcomes Framework)

4.2 Design Services

s47E(d)

[redacted]

4.4 Operational Services

s47E(d)

[redacted]

s47E(d)

[redacted]

5.3 Service Attributes

s47E(d)

[redacted]

5.4 5.4 System Information and Specific Requirements

d) Releases and Enhancements:

(i) Anticipated Releases: The number or frequency of releases (or like activities).

(ii) Anticipated Minor Enhancements: The number or frequency of minor enhancement activities. A number of minor enhancements may be grouped together to form a Release;

(iii) Anticipated Major Enhancements: Any expected or known Major Release or Development activities in the next 12-36 months. Unexpected requirements, including changes in legislation, to address critical security vulnerabilities or to comply with Defence's strategic direction, may require Major Release or Development work to occur. These will be addressed using a Contract Variation Proposal or separate ICTPA order.

i) Non-Standard Security Clearance Requirements: Identifies any non-standard security clearance requirements, if different from the standard requirements identified in the Work Order.

6.3 Plan Deliverables

Business Continuity Plan	
Purpose	The purpose of the Business Continuity Plan is provide procedures to prevent and recover from if required, potential threats. The goal is to enable ongoing operations before and during execution of disaster recovery.
s47E(d)	
Due Date	29 January 2021
s47E(d)	

Commonwealth Data Protection Plan	
Purpose	The purpose of the Data Protection Plan is to describe how the Commonwealth's data will be protected during the course of the Services, including application data.
s47E(d) [redacted]	
Due Date	Accepted Plan upon TSR acceptance for the applicable In-Scope Capability.
s47E(d) [redacted]	

Audit Assistance	
Purpose	Defence is subject to internal and external audits and will require the Supplier's assistance with such audits.
s47E(d) [redacted]	[redacted]
Due Date	As required
s47E(d) [redacted]	[redacted]
System and Security Documentation Maintenance	
Purpose	Defence must maintain accurate and current system and accreditation documentation.
s47E(d) [redacted]	[redacted]
Due Date	As required, at least quarterly.
s47E(d) [redacted]	[redacted]
Privileged User Account Management and Audits	
Purpose	Defence must maintain appropriate recordkeeping for Privileged User Accounts to ensure privileged access is provided to essential users only.
s47E(d) [redacted]	[redacted]
Due Date	An audit report of privileged accounts users must be provided to the Contract Manager on a quarterly basis, in an accepted format.
s47E(d) [redacted]	[redacted]

8. 8. Policies and Procedures (Part D – Commonwealth Policies and Procedures – E1 Policies)

Name	Description	Reference

ICTAB Architecture Principles	Enterprise Architecture principles on the use of IT resources	Architecture Principles.pdf
ICTAB Reference Architectures	Authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.	Defence Reference Architecture.pdf
ICT Security Requirements	ICT security requirements for Defence, Industry, Corporate or similar, ICT systems that communicate, store or process; Official, Sensitive or Classified information.	DIAN 26 Additional ICT Security Requirements
ICT Technical Assurance Framework	ICT Technical Assurance Framework (TAF)	Defence ICT Technical Assurance Framework
IT Service Management Process	IT service management (ITSM) is about the activities performed by an organisation to plan, design, deliver, operate and control information technology (IT) services offered to customers	http://drnet/CIOG/ask/SM/DII/Pages/default.aspx
Defence ICT Software Testing Manual	Manual for ICT testing	http://drnet/CIOG/ForStaff/Services/DAA/Pages/ict-software-testing-manual.aspx
Australian Government Security Vetting	Getting a clearance.	www.defence.gov.au/AGSVA/Getting-a-clearance.asp
Defence Security Principles Framework (DSPF)	Provides controls and instructions to support Defence personnel, contractors, Suppliers, to manage security risks.	http://www.defence.gov.au/DSVS/_Master/resources/DSPF-Unclass-Version.pdf
Defence ICT Strategy 2016 - 2020	Both the Defence White Paper and the First Principles Review emphasise the need for a modern and efficient ICT infrastructure. This strategy reflects the increased demands on ICT across Defence, the focus on information, the evolving technology landscape, and changes in the way ICT services are delivered.	https://www.defence.gov.au/CIOG/ICTStrategy.asp

9.8 Resources

9.8.1 The Supplier shall provide resources with appropriate skillsets, Security Clearances 7 , product and technology knowledge, and experience to deliver the Services.

9.8.2 The Supplier warrants that Core Personnel, Specified Personnel, and Additional Personnel are used in the performance of service.

9.8.3 Resources to manage or oversee delivery of the Services are be identified as 'Core Personnel' in Section 9.9.

9.8.4 Specified skills and resources that are required for the day to day delivery of Sustainment Services and Minor Enhancements are be identified as 'Specified Personnel' in Section 9.10.

9.8.5 Additional skillsets to those provided in sections 11.3 and 11.4 that may be used to deliver Other Services are identified as 'Additional Personnel' and as a catalogue of priced SFIA Skills and Levels in Section 9.11.

9.8.6 For the avoidance of doubt, all resources required to deliver the Services (including Core, Specified and Additional Personnel) must be covered by the Fixed Price Monthly Sustainment Prices. The purpose of provided the resource roles and SFIA Skills and Levels is to assist with costing transparency and a price basis for any Other Services.

Foot Note:

7 Standard security requirements are defined in the Work Order and non-standard requirements are defined for individual capabilities in Annexure A.

s47E(d)

Guideline	Section	Topic	Identifier	Revision	Updated	All	O	P	S	TS	ML2	ML3	Dec 22 Description	Sep 22 Description	Comments	s47E(d)
Guidelines for Cyber Security Roles	Chief Information Security Officer	Developing a cyber security communications strategy	ISM-0720	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The CISO develops, implements and maintains a cyber security communications strategy for their organisation.	The CISO develops and maintains a cyber security communications strategy for their organisation.	Added implement	[redacted]
Guidelines for Cyber Security Roles	Chief Information Security Officer	Overseeing cyber security awareness raising	ISM-0735	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.	The CISO oversees the development and operation of their organisation's cyber security awareness training program.	Added implement	[redacted]
Guidelines for Cyber Security Incidents	Managing cyber security incidents	Incident management policy	ISM-0576	9	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An incident management policy, and associated incident response plan, is developed, implemented and maintained.	An incident management policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Cyber Security Incidents	Managing cyber security incidents	Cyber security incident register	ISM-0125	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A cyber security incident register is developed, implemented and maintained.	A cyber security incident register is maintained that covers the following • the date the cyber security incident occurred • the date the cyber security incident was discovered • a description of the cyber security incident • any actions taken in response to the cyber security incident • to whom the cyber security incident was reported	simplified, added control 1803	[redacted]
Guidelines for Cyber Security Incidents	Managing cyber security incidents	Trusted insider program	ISM-1625	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A trusted insider program is developed, implemented and maintained.	A trusted insider program is developed and implemented.	Added maintained	[redacted]
Guidelines for Procurement and Outsourcing	Cyber supply chain risk management	Cyber supply chain risk management activities	ISM-1631	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Suppliers of applications, ICT equipment and services associated with systems are identified.	Applications, ICT equipment and services associated with systems are identified and understood.	Added suppliers	[redacted]
Guidelines for Procurement and Outsourcing	Cyber supply chain risk management	Supplier relationship management	ISM-1785	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A supplier relationship management policy is developed, implemented and maintained.	A supplier relationship management policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Procurement and Outsourcing	Cyber supply chain risk management	Supplier relationship management	ISM-1786	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An approved supplier list is developed, implemented and maintained.	An approved supplier list is developed and implemented.	Added maintained	[redacted]
Guidelines for Procurement and Outsourcing	Cyber supply chain risk management	Sourcing applications, ICT equipment and services	ISM-1787	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Applications, ICT equipment and services are sourced from approved suppliers.	Applications, ICT equipment and services are purchased from approved suppliers.	purchased to sourced	[redacted]
Guidelines for Procurement and Outsourcing	Cyber supply chain risk management	Sourcing applications, ICT equipment and services	ISM-1788	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Multiple potential suppliers are identified for sourcing critical applications, ICT equipment and services.	Multiple potential suppliers are identified for the purchase of critical applications, ICT equipment and services.	purchased to sourced	[redacted]
Guidelines for Procurement and Outsourcing	Cyber supply chain risk management	Sourcing applications, ICT equipment and services	ISM-1789	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Sufficient spares of critical ICT equipment are sourced and kept in reserve.	Sufficient spares of critical ICT equipment is purchased and kept in reserve.	purchased to sourced	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Managed services	ISM-1736	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A managed service register is developed, implemented, maintained and verified on a regular basis.	A managed service register is maintained and verified on a regular basis.	Added developed and implemented	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Outsourced cloud services	ISM-1637	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An outsourced cloud service register is developed, implemented, maintained and verified on a regular basis.	An outsourced cloud service register is maintained and verified on a regular basis.	Added developed and implemented	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1395	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Service providers, including any subcontractors, provide an appropriate level of protection for any data entrusted to them or their services	Service providers provide an appropriate level of protection for any data entrusted to them or their services.	Added subcontractors	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-0072	9	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.	Security requirements associated with the confidentiality, integrity and availability of data entrusted to a service provider are documented in contractual arrangements and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.	removed entrusted	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1571	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The right to verify compliance with security requirements is documented in contractual arrangements with service providers.	The right to verify compliance with security requirements is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1738	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The right to verify compliance with security requirements documented in contractual arrangements with service providers is exercised on a regular and ongoing basis	The right to verify compliance with security requirements documented in contractual arrangements is exercised on a regular and ongoing basis.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-0141	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The requirement for service providers to report cyber security incidents to a designated point of contact as soon as possible after they occur or are discovered is documented in contractual arrangements with service providers.	The requirement for service providers to report cyber security incidents to a designated point of contact as soon as possible after they occur or are discovered is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1794	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A minimum notification period of one month by service providers for significant changes to their own service provider arrangements is documented in contractual arrangements with service providers	Notification by service providers of significant changes to their own service provider arrangements is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1451	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Types of data and its ownership is documented in contractual arrangements with service providers.	Types of data and its ownership is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1572	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The regions or availability zones where data will be processed, stored and communicated is documented in contractual arrangements with service providers	The regions or availability zones where data will be processed, stored and communicated is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1573	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Access to all logs relating to an organisation's data and services is documented in contractual arrangements with service providers.	Access to all logs relating to an organisation's data and services is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1574	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	The storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements with service providers	The storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Procurement and Outsourcing	Managed services and cloud services	Contractual security requirements with service providers	ISM-1575	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements with service providers.	A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements.	added service providers	[redacted]
Guidelines for Security Documentation	Development and maintenance of security documentation	Cyber security strategy	ISM-0039	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A cyber security strategy is developed, implemented and maintained.	A cyber security strategy is developed and implemented.	Added maintained	[redacted]
Guidelines for Physical Security	Facilities and systems	Bringing Radio Frequency and infrared devices into facilities	ISM-1543	4	Dec-22	No	No	No	Yes	Yes	No	No	An authorised RF and IR device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis.	An authorised RF and IR device register is maintained for SECRET and TOP SECRET areas and verified on a regular basis.	S/TS system only	[redacted]

Guidelines for Personnel Security	Access to systems and their resources	Unprivileged access to systems	ISM-1714	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Unprivileged access event logs are stored centrally.	Unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	wording simplified, actions moved to control 1815	s47E(d) [redacted]
Guidelines for Personnel Security	Access to systems and their resources	Privileged access to systems	ISM-1509	2	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Privileged access events are logged.	Use of privileged access is logged.	Changed use to events	[redacted]
Guidelines for Personnel Security	Access to systems and their resources	Privileged access to systems	ISM-1651	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Privileged access event logs are stored centrally.	Privileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	wording simplified, actions moved to control 1815	[redacted]
Guidelines for Personnel Security	Access to systems and their resources	Privileged access to systems	ISM-1650	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Privileged account and group management events are logged.	Changes to privileged accounts and groups are logged.	Wording simplified to capture more actions	[redacted]
Guidelines for Personnel Security	Access to systems and their resources	Privileged access to systems	ISM-1652	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Privileged account and group management event logs are stored centrally.	Privileged account and group change event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	wording simplified, actions moved to control 1815	[redacted]
Guidelines for Personnel Security	Access to systems and their resources	Emergency access to systems	ISM-1715	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Break glass event logs are stored centrally.	Break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	wording simplified, actions moved to control 1816	[redacted]
Guidelines for Communications Infrastructure	Cabling infrastructure	Cable register	ISM-0211	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A cable register is developed, implemented, maintained and verified on a regular basis.	A cable register is maintained and verified on a regular basis.	Added developed and implemented	[redacted]
Guidelines for Communications Infrastructure	Cabling infrastructure	Floor plan diagrams	ISM-1645	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Floor plan diagrams are developed, implemented, maintained and verified on a regular basis.	Floor plan diagrams are maintained and verified on a regular basis.	Added developed and implemented	[redacted]
Guidelines for Communications Infrastructure	Cabling infrastructure	Cable labelling processes and procedures	ISM-0206	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Cable labelling processes, and supporting cable labelling procedures, are developed, implemented and maintained.	Cable labelling processes, and supporting cable labelling procedures, are developed and implemented.	Added maintained	[redacted]
Guidelines for Communications Systems	Telephone systems	Telephone system usage policy	ISM-1078	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A telephone system usage policy is developed, implemented and maintained.	A telephone system usage policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Communications Systems	Video conferencing and Internet Protocol telephony	Denial of service response plan	ISM-1019	9	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A denial of service response plan for video conferencing and IP telephony services is developed, implemented and maintained.	A denial of service response plan is developed and implemented for video conferencing and IP telephony services that includes • how to identify signs of a denial-of-service attack • how to identify the source of a denial-of-service attack • how capabilities can be maintained during a denial-of-service attack • what actions can be taken to respond to a denial-of-service attack	Simplified, added control 1805	[redacted]
Guidelines for Communications Systems	Fax machines and multifunction devices	Fax machine and multifunction device usage policy	ISM-0588	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A fax machine and MFD usage policy is developed, implemented and maintained.	A fax machine and MFD usage policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Enterprise Mobility	Mobile device management	Mobile device management policy	ISM-1533	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A mobile device management policy is developed, implemented and maintained.	A mobile device management policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Enterprise Mobility	Mobile device usage	Mobile device usage policy	ISM-1082	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A mobile device usage policy is developed, implemented and maintained.	A mobile device usage policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Enterprise Mobility	Mobile device usage	Mobile device emergency sanitisation processes and procedures	ISM-0701	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed, implemented and maintained.	Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed and implemented.	Added maintained	[redacted]
Guidelines for Enterprise Mobility	Mobile device usage	After travelling overseas with mobile devices	ISM-1300	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Upon returning from travelling overseas with mobile devices, personnel take the following actions • sanitise and reset mobile devices, including all removable media • decommission any credentials that left their possession during their travel • report if significant doubt exists as to the integrity of any	Upon returning from travelling overseas with mobile devices, personnel take the following actions • sanitise and reset mobile devices, including all removable media • decommission any physical credentials that left their possession during their travel • report if significant doubt exists as to the integrity of any mobile devices or removable media.	removed physical and refers to all credentials	[redacted]
Guidelines for Enterprise Mobility	Mobile device usage	After travelling overseas with mobile devices	ISM-1556	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions • reset credentials used with mobile devices, including those used for remote access to their organisation's systems • monitor accounts for any indicators of compromise, such as failed logon attempts.	If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions • reset user credentials used with mobile devices, including those used for remote access to their organisation's systems • monitor accounts for any indicators of compromise, such as failed logon attempts.	Removed user and refers to all credentials	[redacted]
Guidelines for ICT Equipment	ICT equipment usage	ICT equipment management policy	ISM-1551	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An ICT equipment management policy is developed, implemented and maintained.	An ICT equipment management policy is developed and implemented.	Added maintained	[redacted]
Guidelines for ICT Equipment	ICT equipment usage	ICT equipment register	ISM-0336	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An ICT equipment register is developed, implemented, maintained and verified on a regular basis.	An ICT equipment register is maintained and verified on a regular basis.	Added developed and implemented	[redacted]
Guidelines for ICT Equipment	ICT equipment sanitisation and destruction	ICT equipment sanitisation processes and procedures	ISM-0313	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	ICT equipment sanitisation processes, and supporting ICT equipment sanitisation procedures, are developed, implemented and maintained.	ICT equipment sanitisation processes, and supporting ICT equipment sanitisation procedures, are developed and implemented.	Added maintained	[redacted]
Guidelines for ICT Equipment	ICT equipment sanitisation and destruction	ICT equipment destruction processes and procedures	ISM-1741	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	ICT equipment destruction processes, and supporting ICT equipment destruction procedures, are developed, implemented and maintained.	ICT equipment destruction processes, and supporting ICT equipment destruction procedures, are developed and implemented.	Added maintained	[redacted]
Guidelines for ICT Equipment	ICT equipment disposal	ICT equipment disposal processes and procedures	ISM-1550	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	ICT equipment disposal processes, and supporting ICT equipment disposal procedures, are developed, implemented and maintained.	ICT equipment disposal processes, and supporting ICT equipment disposal procedures, are developed and implemented.	Added maintained	[redacted]

[redacted]

s47E(d)

Guidelines for Media	Media usage	Media management policy	ISM-1549	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A media management policy is developed, implemented and maintained.	A media management policy is developed and implemented.	Added maintained
Guidelines for Media	Media usage	Removable media usage policy	ISM-1359	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A removable media usage policy is developed, implemented and maintained.	A removable media usage policy is developed and implemented.	Added maintained
Guidelines for Media	Media usage	Removable media register	ISM-1713	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A removable media register is developed, implemented, maintained and verified on a regular basis.	A removable media register is maintained and verified on a regular basis.	Added developed and implemented
Guidelines for Media	Media sanitisation	Media sanitisation processes and procedures	ISM-0348	5	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Media sanitisation processes, and supporting media sanitisation procedures, are developed, implemented and maintained.	Media sanitisation processes, and supporting media sanitisation procedures, are developed and implemented.	Added maintained
Guidelines for Media	Media destruction	Media destruction processes and procedures	ISM-0363	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.	Media destruction processes, and supporting media destruction procedures, are developed and implemented.	Added maintained
Guidelines for Media	Media disposal	Media disposal processes and procedures	ISM-0374	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained.	Media disposal processes, and supporting media disposal procedures, are developed and implemented.	Added maintained
Guidelines for System Hardening	Operating system hardening	Operating system releases and versions	ISM-1407	5	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	The latest release, or the previous release, of operating systems are used.	The latest release, or the previous release, of operating systems are used for workstations, servers and network devices.	Simplifed to all OS
Guidelines for System Hardening	Operating system hardening	Operating system releases and versions	ISM-1408	5	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Where supported, 64-bit versions of operating systems are used.	Where supported, 64-bit versions of operating systems are used for workstations, servers, network devices and other ICT equipment.	Simplifed to all OS
Guidelines for System Hardening	Operating system hardening	Hardening operating system configurations	ISM-0383	8	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Default accounts or credentials for operating systems, including for any pre-configured accounts, are changed.	Default credentials for pre-configured accounts are changed.	Specified all OS and expanded to default accounts
Guidelines for System Hardening	Operating system hardening	Application control	ISM-1660	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Allowed and blocked execution events on workstations are logged.	Allowed and blocked executions on workstations are logged.	Specified to execution events
Guidelines for System Hardening	Operating system hardening	Application control	ISM-1661	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Allowed and blocked execution events on internet-facing servers are logged.	Allowed and blocked executions on internet-facing servers are logged.	Specified to execution events
Guidelines for System Hardening	Operating system hardening	Application control	ISM-1662	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Allowed and blocked execution events on non-internet-facing servers are logged.	Allowed and blocked executions on non-internet-facing servers are logged.	Specified to execution events
Guidelines for System Hardening	Operating system hardening	Application control	ISM-1663	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Application control event logs are stored centrally.	Application control event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805
Guidelines for System Hardening	Operating system hardening	PowerShell	ISM-1664	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Blocked PowerShell script execution events are logged.	Blocked PowerShell script executions are logged.	Specified to execution events
Guidelines for System Hardening	Operating system hardening	PowerShell	ISM-1665	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	PowerShell event logs are stored centrally.	PowerShell event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805
Guidelines for System Hardening	Operating system hardening	Operating system event logging	ISM-1747	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Operating system event logs are stored centrally.	Operating system event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805
Guidelines for System Hardening	Application hardening	Microsoft Office macros	ISM-1677	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Allowed and blocked Microsoft Office macro execution events are logged.	Allowed and blocked Microsoft Office macro executions are logged.	Specified to execution events
Guidelines for System Hardening	Application hardening	Microsoft Office macros	ISM-1678	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Microsoft Office macro event logs are stored centrally.	Microsoft Office macro event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805
Guidelines for System Hardening	Authentication hardening	Multi-factor authentication	ISM-1683	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Successful and unsuccessful multi-factor authentication events are logged.	Successful and unsuccessful multi-factor authentications are logged.	Specified to Authentication events
Guidelines for System Hardening	Authentication hardening	Multi-factor authentication	ISM-1684	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Multi-factor authentication event logs are stored centrally.	Multi-factor authentication event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805
Guidelines for System Hardening	Authentication hardening	Setting credentials for user accounts	ISM-1596	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Credentials, in the form of memorised secrets, are not reused by users across different systems.	Passphrases are not reused for single-factor authentication across different systems.	change from passphrase to credentials
Guidelines for System Hardening	Authentication hardening	Protecting credentials	ISM-1685	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.	Changed to Long
Guidelines for System Hardening	Authentication hardening	Protecting credentials	ISM-0418	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.	Physical credentials are stored separately from systems to which they grant access.	Change from physical to include all credentials
Guidelines for System Hardening	Authentication hardening	Session and screen locking	ISM-0428	9	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Systems are configured with a session or screen lock that • activates after a maximum of 15 minutes of user inactivity, or if manually activated by users • conceals all session content on the screen • ensures that the screen does not enter a power saving state before the session or screen lock is activated • requires users to authenticate to unlock the session • denies users the ability to disable the session or screen locking mechanism.	Systems are configured with a session or screen lock that • activates after a maximum of 15 minutes of user inactivity, or if manually activated by users • conceals all session content on the screen • ensures that the screen does not enter a power saving state before the session or screen lock is activated • requires users to reauthenticate to unlock the session • denies users the ability to disable the session or screen locking mechanism.	change from reauthenticate to authenticate
Guidelines for System Management	System administration	System administration processes and procedures	ISM-0042	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	System administration processes, and supporting system administration procedures, are developed, implemented and maintained	System administration processes, and supporting system administration procedures, are developed and implemented.	Added maintained

[redacted]

Guidelines for System Management	System patching	Patch management processes and procedures	ISM-1143	9	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.	Patch management processes, and supporting patch management procedures, are developed and implemented.	Added maintained	s47E(d) [redacted]
Guidelines for System Management	System patching	Software register	ISM-1493	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Software registers for workstations, servers, network devices and other ICT equipment are developed, implemented, maintained and verified on a regular basis.	Software registers are maintained for workstations, servers, network devices and other ICT equipment and verified on a regular basis.	Added developed and implemented	
Guidelines for System Management	Data backup and restoration	Digital preservation policy	ISM-1510	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A digital preservation policy is developed, implemented and maintained.	A digital preservation policy is developed and implemented.	Added maintained	
Guidelines for System Management	Data backup and restoration	Data backup and restoration processes and procedures	ISM-1547	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Data backup processes, and supporting data backup procedures, are developed, implemented and maintained.	Data backup processes, and supporting data backup procedures, are developed and implemented.	Added maintained	
Guidelines for System Management	Data backup and restoration	Data backup and restoration processes and procedures	ISM-1548	2	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.	Data restoration processes, and supporting data restoration procedures, are developed and implemented.	Added maintained	
Guidelines for System Management	Data backup and restoration	Performing and retaining backups	ISM-1511	3	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.	specified need to document frequency and retetniation	
Guidelines for System Management	Data backup and restoration	Backup access	ISM-1705	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.	Unprivileged accounts, and privileged accounts (excluding backup administrators) cannot access other account's backups.	Split, new controls have unpriv accounts	
Guidelines for System Management	Data backup and restoration	Backup access	ISM-1706	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Privileged accounts (excluding backup administrator accounts) cannot access their own backups.	Unprivileged accounts, and privileged accounts (excluding backup administrators) cannot access their own account's backups.	Split, new controls have unpriv accounts	
Guidelines for System Management	Data backup and restoration	Backup modification and deletion	ISM-1707	1	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups.	Split, new controls have unpriv accounts	
Guidelines for System Management	Data backup and restoration	Backup modification and deletion	ISM-1708	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period	Backup administrators (excluding backup break glass accounts), are prevented from modifying or deleting backups.	Included Priv accounts	
Guidelines for System Management	Data backup and restoration	Testing restoration of backups	ISM-1515	3	Dec-22	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises.	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	removed systems and added configuration settings	
Guidelines for System Monitoring	Event logging and monitoring	Event logging policy	ISM-0580	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An event logging policy is developed, implemented and maintained.	An event logging policy is developed and implemented.	Added maintained	
Guidelines for System Monitoring	Event logging and monitoring	Centralised event logging facility	ISM-1405	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	Yes	A centralised event logging facility is implemented and event logs are sent to the facility as soon as possible after they occur.	A centralised event logging facility is implemented and systems are configured to save event logs to the facility as soon as possible after each event occurs.	change from save to send event logs	
Guidelines for Software Development	Application development	Vulnerability disclosure program	ISM-1755	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A vulnerability disclosure policy is developed, implemented and maintained.	A vulnerability disclosure policy is developed and implemented.	Added maintained	
Guidelines for Software Development	Application development	Vulnerability disclosure program	ISM-1756	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed, implemented and maintained.	Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed and implemented.	Added maintained	
Guidelines for Software Development	Web application development	Web application event logging	ISM-1757	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Web application event logs are stored centrally.	Web application event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805	
Guidelines for Database Systems	Databases	Database register	ISM-1243	6	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A database register is developed, implemented, maintained and verified on a regular basis.	A database register is maintained and verified on a regular basis.	Added developed and implemented	
Guidelines for Database Systems	Databases	Database event logging	ISM-1758	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Database event logs are stored centrally.	Database event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805	
Guidelines for Email	Email usage	Email usage policy	ISM-0264	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	An email usage policy is developed, implemented and maintained.	An email usage policy is developed and implemented.	Added maintained	
Guidelines for Email	Email gateways and servers	Email content filtering	ISM-1234	5	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.	Email content filtering is implemented for email bodies and attachments.	Specified harmful content	
Guidelines for Networking	Network design and configuration	Network documentation	ISM-0518	5	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Network documentation is developed, implemented, maintained.	Network documentation is updated as network configuration changes are made and includes a 'current as at [date]' or equivalent statement.	Update wording to consitent with other controls	
Guidelines for Networking	Network design and configuration	Use of Simple Network Management Protocol	ISM-1311	3	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	SNMP version 1 and SNMP version 2 are not used on networks.	SNMP version 1 and 2 are not used on networks.	Simplifed wording	
Guidelines for Networking	Network design and configuration	Protective Domain Name System Services	ISM-1782	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A protective DNS service is used to block access to known malicious domain names.	A protective DNS service is used for networks.	Specified to malicious domain names	
Guidelines for Networking	Network design and configuration	Default accounts and credentials for network devices	ISM-1304	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Default accounts or credentials for network devices including for any pre-configured accounts, are changed.	Default accounts for network devices are disabled, renamed or have their credentials changed.	Added credentials	
Guidelines for Cryptography	Cryptographic fundamentals	Cryptographic key management processes and procedures	ISM-0507	5	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Cryptographic key management processes, and supporting cryptographic key management procedures, are developed, implemented and maintained.	Cryptographic key management processes, and supporting cryptographic key management procedures, are developed and implemented.	Added maintained	
Guidelines for Gateways	Gateways	Gateway event logging and alerting	ISM-1775	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Gateway event logs are stored centrally.	Gateway event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805	

Guidelines for Gateways	Cross Domain Solutions	Cross Domain Solution event logging	ISM-1776	1	Dec-22	No	No	No	Yes	Yes	No	No	CDS event logs are stored centrally.	CDS event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	S/TS system only	s47E(d) [redacted]
Guidelines for Gateways	Web proxies	Web usage policy	ISM-0258	4	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	A web usage policy is developed, implemented and maintained.	A web usage policy is developed and implemented.	Added maintained	[redacted]
Guidelines for Gateways	Web proxies	Web proxy event logging	ISM-1777	1	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Web proxy event logs are stored centrally.	Web proxy event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Simplified, added control 1805	[redacted]
Guidelines for Gateways	Web content filters	Using web content filters	ISM-0963	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Web content filtering is implemented to filter potentially harmful web-based content.	Web content filters are used to filter potentially harmful web-based content.	Specified harmful content	[redacted]
Guidelines for Data Transfers	Data transfers	Data transfer processes and procedures	ISM-0663	7	Dec-22	Yes	Yes	Yes	Yes	Yes	No	No	Data transfer processes, and supporting data transfer procedures, are developed, implemented and maintained.	Data transfer processes, and supporting data transfer procedures, are developed and implemented.	Added maintained	[redacted]
Guidelines for Data Transfers	Data transfers	Data transfer processes and procedures	ISM-1535	5	Dec-22	No	No	No	Yes	Yes	No	No	Processes, and supporting procedures, are developed, implemented and maintained to prevent AUSTEO, AGAO and REL data in both textual and non-textual formats from being exported to unsuitable foreign systems.	Processes, and supporting procedures, are developed and implemented to prevent AUSTEO, AGAO and REL data in both textual and non-textual formats from being exported to unsuitable foreign systems.	S/TS system only	[redacted]
Guidelines for Data Transfers	Data transfers	Manual export of data	ISM-0669	6	Dec-22	No	No	No	Yes	Yes	No	No	When manually exporting data from SECRET and TOP SECRET systems, digital signatures are validated and keyword checks are performed within all textual data.	When manually exporting data from SECRET and TOP SECRET systems, the data undergoes data formatting checks, data type and size checks, signature checks, and keyword checks within all textual data.	S/TS system only	[redacted]

s47E(d) [redacted]

MSP Change Requests that have been raised relating security patching or system updates (relevant to FOI request)

s47E(d)

CHM-1717406-DPE - [redacted]
CHM-1806065-DPE
CHM-1867982-DPE -
CHM-1995194-DPE -
CHM-2081471-DPE -
CHM-2159904-DPE -
CHM-2175081-DPE -
CHM-2218635-DPE -
CHM-2303839-DPE -
CHM-2405882-DPE -

Confirmed via DSMS

s47E(d)

[redacted]

[redacted]

Computer Name	Description of Patch	Link to KB Article	Hotfix ID	Installed On
s47E(d)	Update	http://support.microsoft.com s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	https://support.microsoft.com/ s47E(d)		
	Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
s47E(d)	Update	http://support.microsoft.com s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Update	https://support.microsoft.com/ s47E(d)		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
s47E(d)	Update	http://support.microsoft.com s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	https://support.microsoft.com/ s47E(d)		
	Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
s47E(d)	Update	http://support.microsoft.com s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	http://support.microsoft.com/		
	Security Update	https://support.microsoft.com s47E(d)		
	Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		
	Security Update	https://support.microsoft.com/		

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)

s47E(d)	Security Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com	s47E(d)				
	Update	https://support.microsoft.com/					

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)	s47E(d)	s47E(d)
	Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
s47E(d)	Update	http://support.microsoft.com/	s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com/			
	Security Update	http://support.microsoft.com/			
	Security Update	http://support.microsoft.com/			
	Security Update	http://support.microsoft.com/			
	Security Update	https://support.microsoft.com/	s47E(d)		
	Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
s47E(d)	Update	http://support.microsoft.com	s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com			
	Security Update	http://support.microsoft.com			
	Security Update	http://support.microsoft.com			
	Security Update	http://support.microsoft.com			
	Security Update	https://support.microsoft.com/	s47E(d)		
	Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
s47E(d)	Update	http://support.microsoft.com/	s47E(d)	s47E(d)	s47E(d)
	Security Update	http://support.microsoft.com/			
	Security Update	http://support.microsoft.com/			
	Security Update	http://support.microsoft.com/			
	Security Update	http://support.microsoft.com/			
	Security Update	https://support.microsoft.com/	s47E(d)		
	Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			
	Security Update	https://support.microsoft.com/			

s47E(d)	Security Update	https://support.microsoft.com,	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com,	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	https://support.microsoft.com,	s47E(d)				
	Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
	Security Update	https://support.microsoft.com,					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					

s47E(d)	Security Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Update	http://support.microsoft.com,	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	http://support.microsoft.com,					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

[redacted]

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Security Update	https://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Update	https://support.microsoft.com/	s47E(d)				
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Update	http://support.microsoft.com					
	Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	http://support.microsoft.com					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Update	http://support.microsoft.com/					
	Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Update	http://support.microsoft.com/					
	Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Update	https://support.microsoft.com/	s47E(d)				
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					

s47E(d)	Security Update	https://support.microsoft.com	s47E(d)		s47E(d)		s47E(d)
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
	Security Update	https://support.microsoft.com					
s47E(d)	Update	http://support.microsoft.com/	s47E(d)		s47E(d)		s47E(d)
	Update	http://support.microsoft.com/					
	Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	http://support.microsoft.com/					
	Security Update	https://support.microsoft.com/	s47E(d)				
	Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					
	Security Update	https://support.microsoft.com/					

s47E(d)

[redacted]

Australian Government
Department of Defence

Cyber Security Assessment Team - 47
D1TU – PMKeyS Security Assessment

Defence Security Operation Centre (DSOC)

Technical Report – Final

Version 1.0 | May 2021

~~PROTECTED~~

Document Information

Document Version	1.0
Document Status	Complete
Issue Date	13/05/21
Author	s47E(d)
Owner	Defence Security Operations Centre
Objective ID	BO13202517

Reviews and Approvals

Name	Title	Date	Role
s47E(d)	OIC CSAT-47	13/05/21	Author
	Security Assessor	13/05/21	Author
	Security Assessors	13/05/21	Peer Review
	SO1 Information and Cyber Security, DSOC	24/05/21	Approver

References

ID	Reference
A	ACSC: Complete Australian Government Information Security Manual, dated April 2021
B	Common Vulnerability Scoring System v3.1: Specification Document (Revision 1), First.Org.Inc
C	National Security Agency Cybersecurity Report, NSA/CSS Technical Cyber Threat Framework v2, dated November 2018

Introduction

Background

1. The Defence Security Operations Centre (DSOC) conducted a security assessment of the Personnel Management Key Solution (PMKeyS) Application, as hosted on the Defence One Technical Upgrade (D1TU) Project's User Acceptance Testing (UAT) environment, from 24 Feb – 13 May 2021.

2. PMKeyS is Defence's core information system for personnel management, and the authoritative management record for all Defence personnel, including civilian staff. It utilises Oracle PeopleSoft application solutions for most of its business logic and underlying architecture. The PMKeyS Application is situated in the Defence Protected Environment for use via the Defence Protected Network (DPN), though a small portion of its functionality is accessible via the PMKeyS Home Portal, and accessible via the Internet-accessible Defence Online Service Domain (DOSD).

s47E(d) [redacted]

Scope

s47E(d) [redacted]

s47E(d)

[redacted]

Methodology

Engagement

s47E(d)

[redacted]

Vulnerability Assessment Tool Suite

s47E(d)

[redacted]

Information Security Manual

10. The Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) at Reference A was used to determine risk-managed protection of information and systems from cyber threats posed by the issues and vulnerabilities identified in this report. The ISM is an industry standard guide that helps organisation use their risk management framework to protect information and systems from cyber threats.

s47E(d)

[redacted]

s47E(d)

[redacted]

Findings Summary

14. Technical findings and issues assessed during the security assessment are summarised in Table 1. Detailed information regarding these vulnerabilities can be found in Annex A.

Table 1: Summary of Technical Findings

ID	s47E(d) [redacted]	s47E(d) [redacted]	Page
1.1	[redacted]	[redacted]	10
1.2	[redacted]	[redacted]	12
1.3	[redacted]	[redacted]	13
1.4	[redacted]	[redacted]	14
1.5	[redacted]	[redacted]	15
1.6	[redacted]	[redacted]	16
1.7	[redacted]	[redacted]	17
1.8	[redacted]	[redacted]	19
1.9	[redacted]	[redacted]	21
1.10	[redacted]	[redacted]	23
1.11	[redacted]	[redacted]	25
1.12	[redacted]	[redacted]	27
1.13	[redacted]	[redacted]	28
1.14	[redacted]	[redacted]	30
1.15	[redacted]	[redacted]	32

Conclusion

15. The DSOC deployed CSAT-47 to conduct a security assessment of the recently upgraded PMKeyS application, in order to confirm the remediation of findings identified during the D1R1a assessment, performed in 2017 by a third party, and to identify any new findings.

s47E(d)

17. Details of adverse technical findings are detailed in Annex A, as well as recommendations to support remediation of identified vulnerabilities.

s47E(d)

s47E(d)

SO1 - Information and Cyber Security
Defence Security Operations Centre
DSOC.Ops@defence.gov.au

Annex:
A: Detailed Technical Findings

Detailed Technical Findings

1. The following tables provide detailed information on each of the findings from the DSOC’s security assessment against the PMKeyS system, as implemented in the D1TU UAT environment.

a. **CVSS** – Common Vulnerability Scoring System (Ref B) – this is the determined severity of the issue or vulnerability identified.

b. **Current Observation** – this describes DSOC’s observations of the issue or vulnerability as of the date of assessment.

c. **Technical Cyber Threat Framework** (Ref C) – identifies where an identified issue or vulnerability can be used by an adversary in a targeted attack.

d. **Consequence** – describes how the issue or vulnerability could be leveraged by an adversary.

e. **Recommendation** – course(s) of action that is recommended by DSOC to remediate or mitigate the identified issue or vulnerability.

f. **ISM Controls** – details the relevant ISM controls to the vulnerability or issue identified, IAW Ref A.

This page and the following 24 pages are exempt from release under s47E(d) of the FOI Act.

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

ICT Certification and Accreditation

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	**Group/Service managed systems**
Low	Accreditation Authority (must be SES1/1* or above)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Accreditation Authority (must be SES1/1* or above)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Accreditation Authority (must be SES1/1* or above)	Appointed Group or Service Cyber Security Adviser (CSE). **Note**: In the event that an appointment of a Group or Service Cyber Security Adviser (CSA) has not been made, the Defence ITSA will be the appropriate escalation point.
High	SES2/2*	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence Chief Information Security Officer (CISO) will be the appropriate escalation point.
Extreme	SES3/3*	Appointed Group Head or Service Chief.

Note: *Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Process

Accreditation Requirements

2. All Defence ICT systems must be accredited prior to processing, storing or communicating Official information.

3. ICT systems are to be reaccredited when one or more of the following conditions are met:

a. Commonwealth or Defence policy changes;

b. new or emerging threats to systems are detected;

c. security measures are not operating as effectively as planned;

d. a cyber security incident occurs;

e. changes to the certified system architecture occur;

f. changes to the system risk profile occur;

g. the system extends outside the accreditation boundary;

h. the physical environment in which the system is installed changes; and

i. the system's accreditation expires.

Certification and Accreditation Appointments

4. Refer to Annex A of this Control for the key Governance and Functional appointments in the certification and accreditation process. The Annex also identifies the Certification and Accreditation Authorities for each Group or Service.

Certification and Accreditation (C&A) Process

5. Annex B of this Control demonstrates the C&A process and this should be read in conjunction with the *Roles and Responsibilities* outlined below.

6. If an external Certification Consultant (CC) is required to complete an assessment, they are to be approved by the ITSA or a delegated representative prior to conducting the certification. Failure to do so may render the certification void.

7. When conducting any assessment and/or certification activity for Defence, the Certification Consultant is to follow the Defence Certification and Accreditation Process. Refer to Annex B of this Control.

8. Prior to commencing an assessment, CC must be formally appointed (in writing) by a Certification Authority (CA) or delegated representative.

9. The table below provides the Residual Risk Rating and the responsibility of who can sign off on the risk for each domain/environment for the Certification and Accreditation process being accurately followed.

Table Error! No text of specified style in document. **– Residual Risk and Responsibility**

Residual Risk Rating	**Responsibility**			
	System	**Domain**	**Security Environment**	**Defence Information Environment**
Low	Accreditation Authority (must be SES1/1* or above)	IT Security Adviser	IT Security Adviser	IT Security Adviser
Moderate	Accreditation Authority (must be SES1/1* or above)	IT Security Adviser	Chief Information Security Officer	Chief Information Security Officer
Significant	Accreditation Authority (must be SES1/1* or above)	Chief Information Security Officer	Chief Information Officer	Chief Information Officer
High	SES2/2*	Chief Information Officer	Chief Information Officer via consultation with Defence Security Committee	Chief Information Officer via consultation with Defence Security Committee
Extreme	SES3/3*	Chief Information Officer via consultation with Defence Security Committee	Chief Information Officer via consultation with Enterprise Business Committee	Chief Information Officer via consultation with Enterprise Business Committee

Roles and Responsibilities

Certification Authority

10. A CA is responsible for:

a. identifying and appointing a suitably qualified CC to a Certification assessment (if required);

> ***Note:*** *an outside consultant will not always be required. This will be dependent on the Group/Service and the Protective Marking of material to be processed, stored and communicated on the system.*

b. awarding ICT Certification (endorsing the residual risk identified through a Certification assessment);

c. providing recommendation(s) on Accreditation to the Accreditation Authority, including:

(1) whether to accept the residual risk;

(2) whether to issue a full ICT accreditation (ICTA) or a Provisional ICT Accreditation (PICTA);

(3) any conditions/Information Management Markers that should be placed on the approval;

(4) any remediation activities that must be completed during the approval period (PICTA only);

(5) the duration of the accreditation period; and

a. reporting Certification outcomes to the ITSA.

Accreditation Authority

11. An AA is responsible for:

a. formal recognition, approval and acceptance of the risk(s) to a system;

b. approving a system into operation;

c. reporting Accreditation outcomes to the CISO; and

d. where required, delegating risk acceptance to the CSE/CSA within their Group/Service.

Cyber Security Executive

12. Where the AA chooses to delegate the responsibility of risk acceptance, the CSE must only accept risks up to and including HIGH.

Cyber Security Adviser

13. Where the AA chooses to delegate the responsibility of risk acceptance, the CSA may only accept risks up to and including MODERATE.

Certification Consultant

14. A CC is responsible for:

a. providing advice and guidance to the system owner on the assessment process;

b. providing advice and guidance throughout all phases of the system development, on mitigation strategies and controls to effectively reduce risk within an acceptable risk tolerance;

c. maintaining independence throughout the assessment process;

d. conducting a Security Risk Assessment against current security policy and standards to assess residual risk and address any specific requirements of the CA;

e. providing a Certification Report to the CA which articulates the risks(s) and recommendation(s); and

f. maintaining evidence of activities conducted during a Certification Assessment.

System Owner

15. A System Owner (SO) is responsible for:

a. obtaining and maintaining accreditation of their systems in accordance with the above;

b. assessing the system’s Business Impact Level (BIL);

c. determining Protective markings for information and assets for their systems;

d. developing relevant security artefacts for their system; and

e. maintaining independence from the AA.

Positions and Appointments

Functional Positions

16. Accreditation Authorities:

a. Capability Managers (generally the Group Head or Service Chief) are to act as the Accreditation Authority for their respective Group/Service. They may choose to delegate risk acceptance to their CSE or CSA but must retain the accountability for accreditation. A CSE or CSA must only accept risk to the level outlined under the CSE/CSA roles outlined above. Annex A is a list of functional positions and appointments within Defence relating to C&A.

17. Certification Authorities:

a. ICT Security Branch provides the majority of certification services for Defence SECRET and below systems, with the Assistant Secretary ICT Security (ASICTS) fulfilling the role of CA. Should a Group or Service wish to conduct certification activities for systems within their portfolio, a governance and management structure must be developed and demonstrated prior to a CA being appointed.

b. The Defence ITSA on behalf of the CISO is the only position in Defence authorised to approve the designation of a CA.

c. A list of approved Certification Authorities is at Annex A.

Governance Positions

18. Information Technology Security Adviser (ITSA):

a. The ITSA is responsible for:

(1) managing and reporting on certification activities across Defence; and

(2) endorsing CAs and CCs.

19. Chief Information Security Officer (CISO):

a. the CISO is responsible for managing and reporting on accreditation activities across Defence.

Key Definitions

20. **Certification**: Certification is the process of identifying, assessing and reporting on the risk that an ICT system presents to an information environment.

21. **Accreditation**: Accreditation is the procedure by which an authoritative body (Accreditation Authority) gives formal recognition, approval and acceptance of the risk(s) to an ICT system.

22. **Provisional ICT Accreditation**: Provisional ICT Accreditation (PICTA) is a type of accreditation issued where the Accreditation Authority has requested further controls and/or risk mitigation activities to be undertaken during the provisional accreditation period.

Further Definitions

23. Definitions for common Defence administrative terms can be found on the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – Certification and Accreditation Appointments

Annex B – Defence Certification and Accreditation Process

Document administration

Identification

DSPF Control	ICT Certification and Accreditation
Control Owner	Information Technology Security Adviser
DSPF Number	Control 23.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise Wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	ICT Certification and Accreditation
Related DSPF Control(s)	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch

2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

s47E(d)

From: s47E(d)
Sent: Wednesday, 19 April 2023 2:16 PM
To: s47E(d)
Subject: FW: DSOC - D1TU PMKeyS Security Assessment - Final Report ~~[SEC=PROTECTED]~~

~~PROTECTED~~

Hello s47E(d)
As requested below are the remediation's actions in brief.
Thanks
s47E(d)

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

From: s47E(d)
Sent: Friday, 11 March 2022 11:11 AM
To: s47E(d)
Subject: FW: DSOC - D1TU PMKeyS Security Assessment - Final Report ~~[SEC=PROTECTED]~~

~~PROTECTED~~

s47E(d)

As discussed here is the summary of actions ...

All rows highlighted AMBER needs support from other teams to resolve the issue and rows GREEN are actioned or will be actioned soon.

Please let me know if more information is required.

PEN Test ID	s47E(d)	s47E(d)	Commencement Date	Funding
1.1, 1.2			Commencement date of the project is 1st July 2023.	Approved
1.3			CP team Issue	

1.4	s47E(d) [redacted]	s47E(d) [redacted]	CP team Issue
1.5, 1.6	[redacted]	[redacted]	ICTSB (Cyber Security) to manage the issue or maybe CP team under direction of ICTSB
1.7, 1.8	[redacted]	[redacted]	Defence PKI team
1.9	[redacted]	[redacted]	Issue resolved
1.10	[redacted]	[redacted]	No action
1.11	[redacted]	[redacted]	Issue resolved
1.12	[redacted]	[redacted]	CP team Issue
1.13, 1.14, 1.15	[redacted]	[redacted]	No action

Thanks
s47E(d) [redacted]

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

From s47E(d)
Sent: 10:29 AM
To: s47E(d)
Cc: s47E(d)
s47E(d)
Subject: RE: DSOC - D1TU PMKeyS Security Assessment - Final Report [redacted]

~~PROTECTED~~

Good Morning s47E(d)

My apologies for not responding to you earlier with the remediation plan in response to findings published. D1TU project had been a tough one and we are currently in the closure state and expect final closure by end-March 22.

All the findings in the Penetration Report were reviewed and discussed with Leidos Project support team and other relevant stakeholders and as a consolidated response the Remediation Action Plan for each of the findings has been provided (see attachment).

As the project is winding up the remediation plan will be actioned by CIOG/HICTO/ETOB/DPSS.

Please let me know if additional information or details are required.

Kind Regards,

s47E(d)
ICT People Domain Delivery
Corporate & Logistics Delivery Branch | ICT Delivery Division
Chief Information Officer Group | Department of Defence
s47E(d) Anzac Park West | ACT
M s22
E: s47E(d)
Chat: Lync Instant Messaging

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

From: s47E(d)
Sent: Monday, 24 May 2021 3:17 PM
To: s47E(d)
s47E(d)
Cc: s47E(d)
s47E(d)

s47E(d)

Subject: DSOC - D1TU PMKeyS Security Assessment - Final Report [redacted]]

~~PROTECTED~~

Good Afternoon,

DSOC has produced the final Security Assessment report for the Defence One Technical Upgrade project's PMKeyS Application, see attached.

Kind Regards,

---

s47E(d)

Team Lead – Cyber Readiness Team C – Assessments
Defence Security Operations Centre
ICT Security Branch | ICT Operations Division
Chief Information Officer Group | Department of Defence

s47E(d) | HMAS Harman | Canberra ACT
s47E(d) E: s47E(d)

"High Performance, Teamwork and Respect"

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.