NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

JSP 604 LEAFLET 4800

Regulations for the Installation of Information Communications Technology (Formerly JSP 480)
Part 2: Volume 2 – Chapters 1 – 4 (Feb_2020)

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

List of Contents

The chapters below will be available as separately downloadable documents

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

List of Abbreviations

ACU	Air Conditioning Unit
AMSG	Allied Military Standards Group
AOR	Area Of Responsibility
BEF	Building Entry Facility
BD	Building Distribution
BS	British Standards
CAD	Computer Aided Design
CATV	Cable Access Television
CC	Configuration Control
CESG	Communications Electronic Security Group
CDIO	Chief Digital Information Officer
CM	Configuration Management
CIARFE	Confidentiality, Integrity, Availability, Resilience, Flexibility, Economy
CIDA	Co-ordinating Installation Design Authority
CPC	Circuit Protective Conductor
CPR	Construction Product Regulation
DAIS	Defence Assurance Information Security
DOP	Declaration of Performance
DSO	Departmental Security Officer
ECR	Engineering Change Request
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMR	Electromagnetic Radiation
EMSEC	Electromagnetic or Emissions Security
FD	Floor Distribution
GPG	Good Practice Guide
HMG	Her Majesty's Government
IDA	Installation Design Authority
IDS	Intruder Detection System
ISS	Information Systems Services
JSP	Joint Service Publication
LFH	Low Fire Hazard
LSF	Low Smoke Fume
LSHF	Low Smoke Halogen Free
LSZH	Low Smoke Zero Halogen
MET	Main Earthing Terminal
MOD	Ministry of Defence
MUTO	Multi User Telecommunication Outlet
NCSC	National Cyber Security Centre
OC	Office Commanding
00A	Out of Area
REPO	Remote Emergency Power Off
RFSEC	Radio Frequency Security
RSP	Radio Site Protection
SCIDA	Site Co-ordinating Installation Design Authority
SDA	System Design Authority

SDIPs	SECAN Doctrine and Information Publications
SLI	Service Level Inspection
SPF	Security Policy Framework
SSP	Stainless Steel Pipe
TCA	Tempest Countermeasures Assessment
TCO	Tempest Control Officer
TCP	Tempest Control Plan
TCR	TEMPEST Conformance Review
TSCIDA	Technical Supervisory Co-ordinating Installation Design Authority
TVI	Tempest Visual Inspection
UTP	Unshielded Twisted Pair

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

Guidance and Technical Controls

Rationale for this Leaflet

1. MOD Installation Standards Policy and Governance of the physical and environmental aspects of MOD ICT (as contained in this leaflet) ensure compliance with the Cabinet Office Information Assurance Governance Framework and HMG SPF.

Benefits and Risks of this Leaflet

2. Adherence to this directive ensures control over the installation design, site configuration and environment such that;

a. Confidentiality. By ensuring that where appropriate, installations meet the requirements for RADSEC and are maintained under configuration control.

b. Integrity. By ensuring that installations will not suffer from or be the cause of electrical interference to other co-located installations (EMC).

c. Availability. Optimising operational availability by ensuring that installations are implemented in accordance with relevant standards and good engineering practice, and maintained under effective CM. The aim is to reduce system failure due to poor installation standards and facilitate maintainability, fault rectification and future engineering change.

d. Resilience. By ensuring that where appropriate, installations are provided with diversity of location, power, connectivity and cooling to facilitate continuity of service during unforeseen disruptive malfunction.

e. Flexibility. By ensuring that correct installation documentation and standards are maintained, that installations and recoveries are conducted in a manner that facilitates future change and that a complete Facility information set is available to future Change Designers.

f. Economy. By ensuring that spare capacity is correctly utilised, that additional systems are installed in a manner that makes best use of the site's infrastructure and available space and to co-ordinate change to avoid conflict or promote efficiency such as through combined cross-site duct projects or common works service provision.

Review Date

3. Annually from date of publication.

Technical Controls

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

CHAPTER 01 - Responsibilities and Definitions of CIDA and associated Roles

Introduction

0101. In compliance with legal requirements, the **HMG Security Policy Framework (SPF)** and the **Cabinet Office Information Assurance Governance Framework,** CIO, through D CBM J6 Executive Group, established the MOD CIS Resilience Policy and Recovery Strategy and the DSO publishes JSP 440, the Defence Manual of Security. These MOD policy documents mandate Information and Communications Technology (ICT) security, resilience, Configuration Management (CM), Change Control (CC), installation design control and accreditation processes, thus directly delivering the Cabinet Office governance requirement for compliance with ISO 17799 (BS ISO/IEC 27002), the provision of an Accreditation process and the use of ITIL best practice.

Co-ordinating Installation Design Authority

0102-CIDA is responsible for the MOD Installation Standards Policy direction (as contained in this leaflet) and Governance of the physical and environmental aspects of MOD ICT ensuring compliance with the Cabinet Office Information Assurance Governance Framework and HMG SPF.

0103. MOD Installation Standards Policy ensures control over the installation design, site configuration and environment such that the following is ensured, whilst assuring that within a defined site, all security and safety requirements relating to each ICT installation are met and maintained;

a. **Confidentiality.** By ensuring that where appropriate, installations meet the requirements for RADSEC and are maintained under configuration control.

b. **Integrity.** By ensuring that installations will not suffer from or be the cause of electrical interference to other co-located installations (EMC).

c. **Availability.** Optimising operational availability by ensuring that installations are implemented in accordance with relevant standards and good engineering practice, and maintained under effective CM. The aim is to reduce system failure due to poor installation standards and facilitate maintainability, fault rectification and future engineering change.

d. **Resilience.** By ensuring that where appropriate, installations are provided with diversity of location, power, connectivity and cooling to facilitate continuity of service during unforeseen disruptive malfunction.

e. **Flexibility.** By ensuring that correct installation documentation and standards are maintained, that installations and recoveries are conducted in a manner that facilitates future change and that a complete Facility information set is available to future Change Designers.

f. **Economy.** By ensuring that spare capacity is correctly utilised, that additional systems are installed in a manner that makes best use of the site's infrastructure and available space and to co-ordinate change to avoid conflict or promote efficiency such as through combined cross-site duct projects or common works service provision.

0104. Defence CIDA policy direction ensures that the physical and environmental aspects of Defence ICT installations are compliant with the Cabinet Office Information Assurance Governance Framework and HMG SPF. To ensure compliance with these policies:

a. Certification of new and extant ICT installations is required before ICT systems can be accredited and re-accredited.

b. SCIDAs shall be established and maintained for all ICT facilities. Defence CIDA's SCIDA Framework Document establishes the delivery requirement for SCIDAs to provide the necessary CM of the physical and environmental aspects of Defence ICT Installations.

0105. In accordance with HMG SPF, CIDA uses a risk management approach. Risk is assessed to identify the potential impact to MOD business through the loss or reduction of Confidentiality, Integrity, Availability or Resilience from the viewpoint of the physical and environmental aspects of ICT installations.

0106. Identified risk is managed through normal CIDA process (see Chapter 04) or one of the following routes

a. The problem is rectified to remove the risk.

b. Risk to MOD data is directed to the appropriate system Accreditor for resolution or escalation, as appropriate; or for formal acceptance by the appropriate Information Risk Owner.

c. Risk to personnel or facilities are directed through the facility management to the Head of Establishment (HOE) for resolution or acceptance.

Site Co-ordinating installation Design Authority

0107. To deliver MOD Installation Standards Policy, CIDA support the establishment of site based teams to deliver much of the day to day work. These teams are known as Site CIDA (SCIDA). All MOD facilities shall have a SCIDA, established in accordance with the Defence SCIDA Framework Document and recognised by Defence CIDA. All CIS change at site level must be in accordance with the requirements of JSP 604: Leaflet 4800 and agreed with the SCIDA. For Top Secret MOD ICT, SCIDA shall engage with Defence CIDA who have additional governance responsibilities of TS systems.

0108. The Site CIDA (SCIDA) function is to ensure that the full benefits of Physical and Environmental CM for MOD ICT are delivered across sites in accordance with the SCIDA Framework Document or Contract.

0109. TLBs are responsible for the provision of SCIDA at their sites with this responsibility normally delegated to the Head of Establishment or site owner. From the viewpoint of coordination of change and the regulation of installation standards, a SCIDA should preferably be independent from the organisations who deliver change.

0110. Where a site or facility owner provides a SCIDA to conduct SCIDA provision below that required by MOD and detailed in the SCIDA Framework Document then an assessment of the risk to the Confidentiality, Integrity and Availability of the ICT systems and data must be undertaken and formally recorded.

0111. The effectiveness of a SCIDA may be evaluated, by Defence CIDA personnel, through formal audit of both the SCIDA and the SCIDA process

Technical Supervisory Co-ordinating Installation Design Authority

0112. In certain circumstances, CIDA will authorise the appointment of a Technical Supervisory Co-ordinating Installation Design Authority (TSCIDA) to supervise the SCIDA(s) in the day to day running of the SCIDA role. The TSCIDA will always be an MOD employee with a technical communications background, and may be part of another, relevant, MOD organisation. The TSCIDA will always report to the CIDA on aspects relating to their TSCIDA role.

0113. To avoid lengthening chains of responsibility, the appointment of a TSCIDA should be limited to essential situations. A TSCIDA should not be appointed over a SCIDA where an individual is primarily filling the 'Contract Manager' as opposed to a supervisor role.

0114. A TSCIDA may be appointed under the following circumstances:

a. Where a non-MOD SCIDA has been appointed or contracted and the Defence CIDA is unable to provide the technical support required at a specific location; or

b. To co-ordinate or provide a technical focal point for specialist areas, normally, across several sites.

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

CHAPTER 02 — Configuration Management and the CIDA

Role Introduction

0201. JSP945, Part 1, Para 1.2 *"MOD Policy for Configuration Management'* defines Configuration Management (CM) as the through life management of changes to the products as-designed, as-built and as-maintained standard. It enables changes and different build standards to be traced back to the system requirements. These changes may be introduced to mitigate or nullify the effects of product deterioration due to ageing, corrosion or repair on repair. The changes may also take the form of in-service modification to: improve safety, reduce risk, mitigate obsolescence, improve performance, improve supportability, comply with legislative changes, provide enhanced capability, allow for technology insertion or the correction of product defects and to the final disposal of products.

0202. The main objective of CM is to document and provide full visibility of the product's present configuration and on the status of achievement of its physical and functional requirements. A further objective is that everyone working on the project at any time in its life-cycle uses correct and accurate documentation.

0203. It is essential that the technical and organisational activities which are performed within the CM process are fully integrated for the process to be effective. These activities are listed below:

a. Configuration identification.

b. Change Control.

c. Configuration status accounting.

d. Configuration audit.

CIDA Application of Configuration Management

0204. Defence CIDA is mandated with the responsibility for optimising the maintenance of operational capability, flight safety and electrical security by co-ordinating changes into MOD ICT facilities and by regulating installation standards. CIDA authority applies to all sites, buildings, rooms and mobile/transportable equipment facilities but not to aircraft, ships or submarines.

0205. Day to day activities on a site is normally delegated to the Site CIDA (SCIDA) except for deployed operations which are usually managed centrally. The application of CM to an MOD ICT system is dependent upon the CIDA Service Level assigned to that system (see guidelines at Annex A). In accordance with the mandates of JSP 440, the minimum requirement is the granting of Installation Approval by CIDA.

0206. CIDA has no remit to include system or application software in its CM activities. The CIDA CM 'product', therefore, is the physical, in terms of layout, and electrical, in terms of connectivity, facets of all MOD ICT facilities. CIDA discharges its CM responsibilities for MOD ICT facilities by ensuring that the following procedures are adhered to.

Configuration Identification

0207. A library of 'As Fitted' drawings, including Site Plans, Location Maps and system documentation is generated from site survey and/or assembled from extant information to form the CM baseline for all MOD ICI. Drawing content and standards are fully documented at Chapter 12.

Change Control

0208. All changes to a CIDA controlled facility must go through a Change Control (CC) procedure to obtain CIDA endorsement before the change is implemented. Full details are documented at Chapter 4.

Configuration Status Accounting

0209. To facilitate visibility, traceability and the efficient management of evolving configuration, SCIDA maintain records of pertinent data relative to all 'change' of MOD ICT systems that fall within their AOR, and may use a variety of resources, in either paper or digital format, dependent on the volume of data that is recorded.

Configuration Audit

0210. To ensure continuing conformance to CIDA requirements, sites must be regularly inspected by the SCIDA. This will be carried out to a `SCIDA Inspection Plan', with associated Inspection Reports produced. Separately, Defence CIDA conducts an assurance regime for all SCIDA/sites, the timing of which being determined by the Defence CIDA in consultation with the SCIDA. In combination, the CIDA and SCIDA process constitutes the Configuration Audit.

0211. The frequency of Configuration Audits of MOD ICT systems depends on the `CIDA Service Level' for the system (in accordance with at Annex A).

0212. The configuration audit examines the 'As Fitted' product to its configuration documentation to ensure compliance. The audit confirms that the product conforms to the physical and functional requirements through assessment of:

a. The comprehensiveness of the CIDA baseline package.

b. Installation standards and maintainability across the whole site meet CIDA requirements.

c. Common Equipment layout and engineering requirements are being maintained.

d. Information Security requirements of JSP 440 continue to be maintained.

e. The progress of observations and actions raised in previous audit reports.

f. The local procedures intended to prevent unauthorised change.

g. Unauthorised changes that have occurred and where relevant, the organisation responsible.

0213. On completion of a configuration audit, a report of the results, including recommended actions to correct non-compliance, will be issued to all 'interested parties'.

Annex A - CIDA Service Levels

1. Configuration Management (CM) requires resources and thus must be directed where the gain is most tangible. The CIDA Service Levels for MOD facilities are designed to ensure that areas with the highest business importance are afforded the most significant protection. This gives the greatest benefit to operational capability, safety and security. Their application also helps to identify those sites that require CM but where it is not currently being delivered, thereby increasing the understanding of existing and future resource requirements.

2. In recognition of the above, 3 levels of provision have been devised to reflect the degree of effort required to comply with the requirements. Service Levels are assigned through consultation between CIDA, TSCIDA where appropriate, the facility stakeholders and the SCIDA. The facility stakeholders may include, but not necessarily be limited to, the Engineering and Operational Sponsors and Local Engineering Staff. Once assigned, a Service Level may be reassigned by agreement of all relevant agencies. A site may contain separate areas assigned differing service levels.

3. The SCIDA Inspection regime is directly related to the assigned CIDA Service Levels.

4. The Defence CIDA Service Levels are defined as follows:

a. **CIDA SERVICE LEVEL 1**

- MOD facilities directly supporting Operational Capability, **OR**
- Facilities where short term or extended denial of service would cause significant disruption to operational or direct operational support capability, **OR**
- Facilities having a **high population** of data processing equipment accredited at **SECRET** or higher, **OR**
- Flight Safety related facilities.

b. **CIDA SERVICE LEVEL 2**

- Facilities not directly supporting Operational Capability **AND** having a **low population** of equipment accredited at **SECRET** or higher, **OR**
- Facilities not directly supporting Operational Capability **AND** having a **high population** of equipment accredited at **OFFICIAL.**

c. **CIDA SERVICE LEVEL 3**

- Facilities not directly supporting Operational Capability **AND** having a **low population** of equipment accredited at **OFFICIAL.**

5. MOD facilities that only contain telephones, accredited at OFFICIAL, or internet installations are not necessarily subject to CM. However, all wireless installations are to be the subject of SCIDA control.

6. All cross site ducting and cables are to be subject to CM and will be treated as Service Level 2 as a minimum.

7. Notwithstanding the CM requirements of CIDA, the full Radio Site Protection (RSP) procedures are to be followed where applicable.

8. Table 2-1 is an overview of the minimum CM requirements at sites with different service levels. Table 2-2 is an alternative way of viewing the minimum CM requirements.

Table 2-1 Service Levels, Depth of CM and Frequency of Inspection (Note 1)

Service Level	**Extent of Change Control**	**Minimum Frequency of Facility Inspections by SCIDA**	**Requirement for CM Drawings**
1	Establish/maintain CM Baseline Full ECR process mandatory	1 y earl y	Full CM drawing set established and maintained
2	Full ECR process is mandatory. Note 1	**2** yearly	Full TEMPEST drawing set established and maintained IDA As Fitted drawings held, alternatively, CM drawings
3	**All** changes **must** be assessed ECR Pt 1 Mandatory Pts 2-5 at SCIDA discretion. Note 2	Sample inspections may take place from time to time	IDA 'As Fitted' drawings may be held, CM drawings optional

Notes:

For traditional telephone extensions (Plain Old Telephone Service [POTS]):

1. SCIDA must be notified of the proposed works (ECR 1). ECRs 2 - 5 at SCIDA discretion dependant on proposed change effect on existing ICT.

2. ECR Pts 1-5 at SCIDA discretion. The ATO is to ensure full liaison with the SCIDA to identify System Service Levels.

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

Table 2-2 Minimum SCIDA CM Requirement

Item	Activity	Service Level 1	Service Level 2	Service Level 3
1	**SCIDA Advice**			
2	**Change Control** Process			Note 1
3	**Maintain Drawings & Information**		Note 2	Note 3
4	**Conduct SCIDA Inspections**	Note 4	Note 5	Note 6
5	**Establish the Facility's CM Baseline**			

Notes:

1. Notification of all Change (ECR Pt **1** or equivalent) is mandatory. The need for ECR Pts 2 — 5 will be determined by SCIDA. Decisions not to proceed to ECR Part 5 will require a form of written design endorsement to the Design Agency and written installation conformance to the Security Accreditor.
2. Create & maintain TEMPEST drawings for all ICT systems processing information at SECRET or higher. IDA 'As Fitted' Drawings, or alternatively CM Drawings, are to be held.
3. IDA 'As Fitted' Drawings may be held.
4. Mandatory yearly Inspection of all ICT systems by SCIDA.
5. Mandatory 2 yearly inspection of all ICT systems by SCIDA.
6. Inspections by SCIDA on request from site.

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

CHAPTER 03 — Defence SCIDA Enterprise

Intentionally blank

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

CHAPTER 04 - The CIDA Engineering Change Process

Introduction

0401. A change may be initiated from within a site or by a Project Team (PT), a customer, contractor or supplier and, in accordance with the guidelines contained within JSP 945 *"MOD Policy for Configuration Management",* all change proposals shall be documented in order to protect the integrity of the effected system. It is incumbent on all change designers to initiate change control procedures through the SCIDA as early as possible in the change design cycle to enable protection of the effected installation against conflicting requirements.

0402. To comply with CIS Security Requirements, successful security accreditation of any Information and Communications Technology (ICT) affected by any 'Change' within a MOD site is dependent upon Installation Approval being granted by CIDA. This requirement is satisfied through the issue of a CIDA Certificate of Installation Conformance to the relevant System Security Officer. On MOD sites this is the responsibility of the SCIDA appointed by the Head of Establishment (HOE) who will be responsible for Configuration Management (CM) of the ICT systems within their site and keeping Defence CIDA informed of their site CM status.

0403. Any organisation that initiates change to any ICT, its environment or Radio Site Protection Zone is to ensure that CIDA installation standards and Change Control requirements are mandated and used for the associated work. This applies to all tasks from major projects to local engineering changes and will be correctly specified by mandating JSP 604:4800 requirements in the related contract or work instruction.

0404. It is important that CIDA are made aware and consulted about proposed changes before an Invitation to Tender (ITT) process or a formal contract has been agreed to ensure appropriate requirements are part of any proposed change. Subsequent CIDA approval may be problematic if there has not been an involvement at the start of a change life cycle.

CIDA Change Control Procedures

0405. CIDA has identified a 5 stage Change Control model for use at all MOD sites. Local Change Control systems may be used where preferred to the CIDA model but they must contain all the elements of paragraph 0407 and the non-compliance procedure at paragraph 0419. All facilities must be able to use the CIDA model Engineering Change Request (ECR) because those PTs that role out systems across defence will use it. Use of the complete ECR process is dependent upon the SCIDA Service Level assigned to each individual facility (see guidelines at annex A to chapter 02 for details)

0406. In addition to the following Change Control procedures, all changes affecting Radio Site Restriction zones, the sites occupied by Microwave Links, Navigation Aids, Radars and Radios or similar C-E equipment must be separately notified to MOD-RSP in accordance with paragraph 0424.

CIDA Engineering Change Request

0407. The CIDA ECR process consists of five parts, each of which has a specific purpose in the Change Control of ICT facilities. The five parts for the ECR process are as follows

a. Part 1 - Initial Project Information.

b. Part 2 - Change Proposal and Request for Design Endorsement.

c. Part 3 - Design Endorsement of a Change Proposal.

d. Part 4 - Installation Completion Statement.

e. Part 5 - Certificate of Installation Conformance.

0408. To supplement the ECR process and ensure tight CM, the following procedures may also be applied:

a. Retrospective ECR.

b. CIDA Unsatisfactory Feature Report.

c. Quick Reaction Fax Approval.

0409. The CIDA CM process model is explored in more detail below, with example ECR forms reproduced at the end of this chapter.

ECR Part 1 - Initial Project Information

0410. Part 1 of the ECR process is designed to involve CIDA at the earliest possible stage of a project. It is to include sufficient detail to enable CIDA to safeguard the change against the effects of any conflicting work. It also serves as a request for CIDA Change Control drawings and other relevant information that may assist the change designer.

ECR Part 2 - Change Proposal & Request for Design Endorsement

0411. Part 2 is used to provide detailed design proposals to CIDA in order to obtain CIDA approval and is to include all relevant detail and a comprehensive list of all statutory requirements, standards, codes of practice, equipment specific installation requirements, reports and guidance that the proposed change will comply with in sufficient detail to allow CIDA to assess whether the change is likely to meet the necessary requirements. (Drawings detailing the proposal, in accordance with the requirements of Chapter 12 are normally required to support this activity). For minor changes, Parts 1 & 2 may be combined.

ECR Part 3 - Design Endorsement of a Change Proposal

0412. If the design of the change proposal is in accordance with all CIDA requirements, the change is endorsed and Part 3 will be issued to the IDA. The Part 3 will always have a time limitation imposed, normally 6 months, to maintain effective CM. If the proposed change does not meet all requirements, SCIDA will liaise with the designer to achieve conformance.

0413. The ECR Part 3 is issued to the design agency as confirmation that the proposed change and its implementation will not breach any standards or requirements that are applicable to the subject facility. It has no contractual standing and is not to be construed as an Authority to Proceed (ATP). ATP may only be conferred by the facility owner in conjunction with the relevant budget holder**.**

ECR Part 4 - Installation Completion Statement

0414. Part 4 of the ECR process requires a statement from the IDA that the change has been completed in accordance with the endorsed design and CIDA installation standards. Neither the change itself, nor any associated contracts are to be considered as being complete until "As Fitted" CM drawings, in AutoCAD compatible and/or hard copy format, have been approved by and lodged with the SCIDA. The Change Implementer or Change Designer shall liaise with SCIDA to enable SCIDA assessment of the physically completed change before the change Implementer leaves the site.

ECR Part 5 - Certificate of Installation Conformance

0415. If, after inspection, all aspects of the installed change are considered by CIDA to be satisfactory and in conformance with all requirements, the change will be certified as being conformant by the issue of Part 5 of the ECR process.

Non-Compliance & Risk Management

0416. If, during the change control cycle, a non-compliance with any relevant regulation is identified, it must be confirmed whether, under existing Health & Safety at Work Regulations as defined in Statutory Instruments (SI), there is an absolute duty to comply with those Regulations. Where an Absolute Duty to Comply exists, the non-compliance must be rectified prior to handover of the system. The SCIDA is to provide full written detail of the non-compliance to the Change Initiator. In such cases where rectification is delayed, the Duty Holder, normally the HOE, shall be made aware of the non-compliance.

0417. In other cases, where there is no absolute duty to comply, and all avenues of resolution have been exhausted, then that non-compliance may be risk managed. The SCIDA is to provide full written detail of the non-compliance, including any detrimental effect the non-compliance may have on other ICT, to the Change Initiator. The Change Initiator, with assistance from and agreement of SCIDA, shall identify the appropriate Risk Owner. Where there is contention, Defence CIDA shall arbitrate. The Risk Owner shall consider the full impact of the non-compliance before accepting or declining the associated risk.

0418. An accepted risk shall be formalised by a Risk Management Statement which is to be referenced by and become part of the CIDA Design Endorsement or Installation Conformance Certificate. A declined risk shall be formalised by the Risk Owner providing direction, relative to the resolution of the risk, to the Change Initiator.

Retrospective Engineering Change Request

0419. A Retrospective ECR (RECR) is to be raised when a change is suspected to have occurred without the required CIDA approval process having taken place. Submission of an RECR will ensure that, where required, the ring-fence around a facility can be adjusted to prevent a repeat of similar unauthorised change in the future. The RECR procedure will also attempt to identify those responsible for any remedial work necessary to correct installations that either fall below acceptable standards or where a CIDA authorised installation or the CIDA overall plan for a facility is compromised.

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)

CIDA Unsatisfactory Feature Report

0420. Installations may exist that do not fully meet all CIDA requirements as mandated by this publication. These installations will be evaluated on a case by case basis through the CIDA Unsatisfactory Feature Report (CUFR) process and concessions agreed or remedial action initiated as deemed appropriate. If a concession is agreed that permits an installation to remain in a sub-standard condition, any future Change proposals for that installation are to include corrective actions sufficient to bring the installation into full compliance with CIDA Installation Standards.

Quick Reaction Fax Approval

0421. Use of a Quick Reaction Fax Approval (QRFA) is in itself a commitment that the Change Designer will initiate full ECR procedure within 10 working days and, when the full ECR has been processed, the Change Initiator will manage the implementation of any modification that is necessary to bring the installation into conformance with CIDA requirements. This caveat is necessary because imposed time constraints may preclude detailed assessment of the proposal. The following are acceptable situations appropriate to the use of a QRFA:

a. Where a proposed change could not have been foreseen and is required in response to an Urgent Operational Requirement (UOR) or Urgent Engineering Requirement (UER).

b. In exceptional circumstance where it is deemed to be overwhelmingly beneficial to MOD.

0422. In extreme circumstances, a change may take place without even a QRFA. The commitments mandated by the use of the QRFA will also apply.

Documentation Availability

0423. A full set of documentation detailing all applicable statutory requirements, standards, codes of practice, maintenance procedures, system design, installation design and equipment specific installation requirements, is to be available locally following all changes to all ICT facilities. Additionally, SCIDA are to hold "As Fitted" drawings and connectivity data relating to the facilities affected by the change.

Additional Requirements Relating to C-E Facilities

0424. The following aspects of CM are frequently overlooked by organisations submitting change proposals that affect C-E or C4I hardware, its environment or Radio Site Restriction Zone. All proposals that effect these aspects are to be brought to the attention of MOD-RSP at the earliest possible stage of a change:

a. Radio Site Clearance and Safeguarding.

b. MOD Register of Radio Sites.

c. Site Plans or Navigation Aid, Radar and Radio, Location Maps

Radio Site Clearance, Site Safeguarding & MOD Register of Radio Site.

0426. All requirements to apply change to Radio Frequency (RF) emitters/receivers on MOD sites must include an early application, in accordance with JSP 604:3032 Radio Site Clearance to MOD-RSP for approval, Radio Site Clearance and amendment of the Register of Radio Sites (RRS). Information on any RF propagation path safeguarding requirements must be included in these applications to enable protection, for each site, against degradation by future development or installation.

NOTE: This document (Reference Ch1-4/20/v3 - Feb/20) replaces and supersedes Chapters 1 - 4, JSP 604 Pt 2, leaflet 4800, Chapter 11 (V5.5 Feb 18)