This document is classified as **Green**. Disclosure is limited, recipients can distribute this information to SEC Parties and SMIP stakeholders but must not be made publicly available.

SSC Guidance for Device Security Assurance and Triage

Part 4: DCC 4G Communications Hub Triage Security Controls Framework (4G CH TSCF)

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.0
Date	20 November 2025
Document Status	SSC Approved
Date of Next Review	TBD
Classification	Green

Change Record

Date	Author	Version	Change Reference
20/11/2025	SECAS	1.0	Aligned with SSC Guidance on Device Security Assurance and Triage Part 2 section 8 (Use Case 005) and the DCC, Use Case 005, 4G CH Triage Specification and approved by SSC.

Contents

Note: references to 'DCC' throughout this document should be read to apply to the DCC including its Data Service Providers, its LTE Device Manager, its DCC LTE Communications Hub (CH) Provider and its 4G CH Triage Facility Provider.

1. Regulatory Context

The security controls and assurance arrangements for the end-to-end Smart Metering System are defined in the Smart Energy Code (SEC) and aim to provide confidence to all SEC Parties that the systems and Devices supporting smart metering are appropriately secure.

The SEC Section G7.19 places an obligation on the Security Sub-Committee (SSC): *"The Security Sub-Committee shall:*

(j) develop and maintain documents to be known as "SSC Guidance for Device Security Assurance and Triage" which shall set out the guidance of the Security Sub-Committee in respect of the requirements and processes to be followed in respect of Devices (including their triage and refurbishment) in order to:

(i) achieve appropriate levels of security assurance in accordance with the requirement of this Code; and

(ii) obtain and maintain CPA Certification."

The SSC Guidance for Device Security Assurance and Triage is in four parts:

- Part 1 provides the methodology, a process and a template for any party to raise a change to the Commercial Product Assurance (CPA) Security Characteristics (SCs) or to raise a Use Case for Device Triage.

- Part 2 provides details of the arrangements and the Security Requirements and Guidance to be applied to Use Cases that have been approved by the SSC.

- Part 3 provides details of the assurance arrangements for Use Case 004 Triage Facility Providers in the form of a Triage Security Controls Framework (TSCF):
  - Section 1 of the TSCF describes the purpose and what the TSCF aims to achieve; the different types of Security Assessment and their frequency; and the role of the User CIO;
  - Section 2 of the TSCF provides greater detail at a practical level for the User Assessment lifecycle with information and logistical requirements for how a User should engage with the User CIO; the timeline for User Assessments; and the detailed questions the User CIO might ask, and the evidence it might expect to see from a User to support its assessment.

- Part 4 (this document) is the DCC 4G CH Triage Security Controls Framework (4G CH TSCF) and provides details of the assurance arrangements for 4G CH Triage Activities (Use Case 005) undertaken by the DCC. This assures the security responsibilities of the DCC in respect of 4G CH Triage Activities. For Use Case 005, this involves the DCC, the DSP and Device Manager roles in providing the 'Unlock' and 'Lock' commands and anomaly detection and the 4G CH Triage Facility Provider. These roles must all meet the requirements of the SSC Guidance for Device Security Assurance and Triage Part 2 Section 8.4 to 8.8; compliance with the DCC's 'Use Case 005 Triage Specification Document' and relevant

parts of SEC Section G12. The DCC is also required to comply with SEC Sections G2, G4, G5, G6 and G9 in respect of the Triage of 4G Communication Hubs and details of the compliance required is in the wider DCC SCF. What the DCC CIO will look for to assure the SEC Section G security controls is set out in detail in the wider DCC SCF Part 2, Appendix B.

The SSC Guidance for Device Security Assurance and Triage forms part of the SEC Materials defined in SEC Section M5.1, and the document is regularly reviewed and updated by the SSC.

The Communication Hub Technical Specifications (CHTS) and Great Britain Companion Specifications (GBCS) are Schedules to the SEC that contain a minimum set of functional, technical and security requirements to enable Communication Hub Devices to be installed and to operate efficiently and securely in consumer premises.

The SSC Guidance for Device Security Assurance and Triage Part 4 has been created to support 4G Comms Hub (and later generations) Triage for Use Case 005 approved by the SSC since the CHTS and GBCS do not contain requirements applicable after the Device has been removed from the consumer premises.

The documents comprising SSC Guidance for Device Security Assurance and Triage assume the reader has a high degree of familiarity with the SEC and the CPA SCs and is knowledgeable on security matters. As such, defined terms (where capitalised) have the same meaning as those defined in the SEC and CPA SCs and other capitalised terms are defined in this document.

This document covers the all the 4G CH Triage Activities including the DCC, the DSP, the LTE DM, the LTE Comms Hub Manufacturer contracted by the DCC to support the LTE SMWAN and the 4G CH Triage facility Provider. Other Devices and Use Case 004 Triage Facility Providers are not in scope of this document.

2. Introduction

Security and privacy are at the heart of the end-to-end Smart Metering System. Considerable effort has been invested by the energy industry in designing security protection into the end-to-end ‘trustbased’ security architecture. Security requirements have been developed for smart metering equipment, Users, the DCC and Triage Facility Providers with the purpose of designing proportionate security controls which are subsequently implemented and assured. The smart metering security obligations are set out in the DCC Licence and the Smart Energy Code (SEC) in Section G.

As required by the SSC Guidance on Device Security Assurance and Triage and aligned with the Smart Energy Code (SEC), a CHTFP shall be a Service Provider contracted directly by the DCC or sub-contracted by the LTE CH Manufacturer and shall be independently assessed before being approved to undertake Triage Activities by the DCC Independent Security Assurance Service Provider also known as the DCC Competent Independent Organisation (DCC CIO) and subsequently to a pre-defined DCC security assessment cycle set out in the SEC Section G9 and as required by the SSC.

The purpose of these assessments is to provide confidence to SEC Parties (via the SEC Panel’s responsibility, now delegated to the Security Sub-Committee (SSC), to set the compliance status using the categories defined in SEC G9.28 -G9.31.

Following consideration of the DCC CIO Security Assessment Report, the SSC will provide the DCC with the compliance status and will confirm the nature and timing of the next assessment.

To enable the SSC to set the compliance status, the DCC CIO will examine compliance with the SSC Guidance for Device Security Assurance and Triage Part 2 Section 8.4 to 8.8 and compliance with the DCC’s ‘Use Case 005 Triage Specification Document’ as well as the relevant SEC Section G12 security obligations.

As part of annual DCC Security Assessments under the DCC SCF, the DCC CIO will also examine compliance with the SEC security obligations in SEC Sections G2, G4, G5 and G6 in respect of the Triage of 4G Communication Hubs.

The 4G CH TSCF is intended to provide the basis for an acceptable level of security assurance of the 4G CH Triage process including the DCC, its SPs and the CHTFP and provides a guide to the types of evidence which could be provided to demonstrate compliance with security obligations.

The Security Sub-Committee (SSC) is responsible for producing and maintaining the 4G CH TSCF as part of the SSC Guidance for Device Security Assurance and Triage and each version is approved by the SSC.

The DCC CIO must use the latest version of the 4G CH TSCF, the SSC Guidance on Device Security Assurance and Triage, the DCC, Use Case 005, 4G CH Triage Specification and the SEC.

3. Purpose

What the 4G CH TSCF is intended to achieve

The 4G CH TSCF is intended to provide support and guidance to all parties involved in the DCC Security Assessment Process. The 4G CH TSCF shall:

(i) set out the arrangements and scope of the DCC CIO Security Assessment to meet the requirements of the SSC Guidance on Device Security Assurance and Triage, the DCC, Use Case 005, 4G CH Triage Specification and the Smart Energy Code (SEC) to be applied to the 4G CH Triage process, including the CHTFP; and

(ii) be designed to ensure that such security assurance assessments are proportionate and achieve appropriate levels of security assurance in respect of the DCC, its relevant Service Providers and CHTFP in their unique operational context in advance of approval to start Triage Activities and (at least) annually thereafter.

This 4G CH TSCF provides detailed and practical guidance for the DCC CIO, the DCC, its relevant Service Providers and CHTFPs to assist them through the assessment process and the steps required prior to commencing and continuing Triage Activities. Appendix B describes the type of evidence the DCC CIO will expect to see. The formulation of a DCC Management Response to the DCC CIO observations as well as preparing for the review by the Security Sub-Committee (SSC) and the likely steps needed to be able to remediate non-compliances are the same as described in the wider DCC SCF and are not repeated in this document.

What the 4G CH TSCF describes

This document provides detail at a practical level for the DCC CIO Security Assessment of the 4G CH Triage process including the CHTFP. It explains:

- information for the personnel within the DCC, its relevant Service Providers and CHTFP who need to engage with the DCC CIO along with the timeline for DCC 4G CH Triage Security Assessments;
- the detailed questions the DCC CIO might ask, and the evidence it might expect to see from the DCC and its relevant Service Providers and 4G CH Triage Facility Providers to support its assessment along with SSC clarifications where these seem appropriate**. This is a 'must read' section for the DCC, its relevant Service Providers and 4G CH Triage Facility Providers prior to undertaking a DCC CIO Security Assessment.**
- Frequently Asked Questions

What the 4G CH TSCF is not intended to achieve

The 4G CH TSCF is not designed to be a complete or prescriptive list of tests that the DCC, its relevant SPs and CHTFP must pass to be able to demonstrate compliance with its obligations.

Similarly, it does not aim to be a complete 'compliance checklist' exercise of controls that will be tested by the DCC CIO and the evidence that will be requested. The DCC, its relevant SPs and CHTFP must identify and manage security risks that are appropriate to the 4G CH Triage process.

The 4G CH TSCF is not exhaustive in its description of the questions that the DCC CIO may ask of participants in the 4G CH Triage Activities or in the evidence that the DCC CIO may need to gather to support its work.

Therefore, it should not be regarded as a replacement for the SEC and its supporting documents.

For the avoidance of doubt, the DCC, its relevant SPs and CHTFPs are required to comply with the SSC Guidance on Device Security Assurance and Triage, the relevant SEC obligations and the DCCs 'Use Case 005 Triage Specification Document'.

4. The Role of the DCC CIO

4.1 The primary role of the DCC CIO in respect of 4G CH Triage Activities is to conduct assessments of the DCC and its relevant Service Provider's compliance with:

a) The SSC Guidance on Device Security Assurance and Triage for Use Case 005;
b) The DCCs 'Use Case 005 Triage Specification Document'; and
c) Relevant parts of the SEC Sections G12 noting that compliance with SEC Sections G2, G4, G5, G6 and G9 will be assured by the wider DCC Security Controls Framework (DCC SCF).

4.2 The DCC CIO is also required, where requested, to consider the DCC's Management Response to this assessment and to advise the Security Sub-Committee on matters of noncompliance. The DCC CIO communicates impartial observations to the DCC, its relevant SPs and CHTFP and the Security Sub-Committee. The DCC CIO is not responsible for making the decision regarding the compliance status or regarding sanctions that could be imposed should the DCC be deemed to be non-compliant with its obligations. The sanctions framework is specified in the SEC.

4.3 The role of the DCC CIO is to:

a) carry out DCC CIO Security Assessments at such times and in such manner as are required by the DCC and the SSC;

b) provide DCC CIO Security Assessment Reports in relation to the 4G CH Triage processes that have been the subject of a DCC CIO Security Assessment;

c) receive and consider DCC Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;

d) otherwise, at the request of, and to an extent determined by, the Security SubCommittee, carry out an assessment of the compliance of the DCC, any relevant SP or CHTFP with its obligations in Section 4.1 above and. where:

(i) following a DCC CIO Security Assessment, any material increases in the security risk relating to party has been identified; or

(ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;

(e) at the request of the Security Sub-Committee, provide to it advice in relation to:

(i) the compliance of any party involved in the 4G CH Triage process with its obligations under Section 4.1 above; and

(ii) changes in security risks relating to the Systems, Data, functionality and processes of any party supporting the 4G CH Triage process which fall within Section G5.14 (Information Security: Obligations on Users) which also apply to the DCC, its relevant SPs and CHTFP;

(g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and

(h) undertake such other activities and do so at such times and in such manner, as may be further provided for in this 4G CH TSCF.

5. DCC Security Assessments of 4G CH Triage Activities

5.1 Prior to undertaking any 4G CH Triage Activities, the DCC and its relevant SPs shall be subject to an initial Full DCC Security Assessment by a DCC Competent Independent Organisation (CIO) following the process in SEC Section G9.

Initial and subsequent DCC CIO Security Assessment

5.2 The initial and subsequent DCC CIO Security Assessment is carried out by the DCC CIO to assess the DCC, its relevant SPs and CHTFP compliance against the obligations specified in Section 4.1 above. It is typically performed on-site with the party supporting the 4G CH Triage process as agreed in advance. The DCC CIO will review evidence to establish the extent of compliance. The assessment involves:

- a review of relevant documentation, interviews with key stakeholders and the testing and evidence collection to demonstrate the effective operation of identified controls to demonstrate compliance with the scope of Section 4.1 above The DCC CIO will therefore require access to all key documentation and on-site access, as well as key stakeholders as agreed with the DCC, its relevant SPs and CHTFP, prior to commencing the assessment;
- a review of the outcome of any previous security audits or ISO27001 assessments and any risk assessments conducted and mitigations or changes implemented since they were identified;

Follow-Up Security Assessment

5.3 A Follow-Up Security Assessment is an assessment carried out by the DCC CIO at the request of the SSC. The DCC Security Assessment Response (generally known as the DCC Management Response), where relevant, sets out the steps the DCC commits to take to address any instances of non-compliance or partial compliance observed by the DCC CIO. The SSC may request the DCC CIO to perform a Follow-Up Security Assessment of any party involved in the 4G CH Triage process to:

a) identify the extent to which the party has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

b) assess any other matters related to the DCC Security Assessment Response that are specified by the Security Sub-Committee.

The scope and duration of the Follow-Up Security Assessment is dependent on the requirements set by the SSC who will provide details to the DCC and the DCC CIO.

Post Assessment

5.4 Following the completion of a DCC CIO Security Assessment, the DCC CIO will produce a written report which shall:

a) set out the findings of the DCC CIO on all the matters within the scope of the DCC CIO Security Assessment;

(i) specify any instances of actual or potential non-compliance of the 4G CH Triage Activities with its obligations set out in Section 4.1 above which have been identified by the DCC CIO; and

(ii) set out the evidence which, in the opinion of the DCC CIO, establishes each of the instances of actual or potential non-compliance which it has identified; and

(iii) specify any material increase in the security risk relating to that party to the 4G CH Triage Activities which the DCC CIO has identified since the last occasion on which a DCC CIO Security Assessment was carried out in respect of the 4G CH Triage process; and

(iv) set out the evidence which, in the opinion of the DCC CIO, establishes the increase in security risk which it has identified.

5.5 The DCC CIO will submit a draft copy of the DCC CIO Security Assessment Report to the DCC, its relevant SP and CHTFP for review of factual accuracy checking and also to enable the DCC to start to co-ordinate and draft a Security Assessment Response (known as the DCC Management Response) for submission to the SSC. The DCC shall have 5 working days to review the report and respond to the DCC CIO with changes of factual accuracy for consideration but will continue to draft the Management Response for DCC review.

5.6 The DCC CIO will then have up to 5 working days to accept, explain or reject factual accuracy changes submitted for considerations by the DCC. The DCC CIO Security Assessment Report will be updated as applicable where the change is accepted by the DCC CIO and re-issued to the DCC, its relevant SPs and CHTFP.

5.7 From the point at which the DCC receives the original draft copy of the DCC CIO Security Assessment Report, the DCC will have 15 working days to compile the Management Responses for DCC review to the identified observations and to submit these to SECAS. The DCC Management Responses are intended to satisfy the requirements of the DCC CIO Security Assessment Response.

5.8 SECAS will undertake a validation of the DCC Management Response on behalf of the SSC and will advise the SSC of the extent to which the response meets the DCC CIO observation. Where SECAS considers that the DCC Management Response is inadequate or requires clarification, SECAS will advise the DCC and provide an opportunity for an improved response to be submitted. The DCC CIO will then have 5 working days to consider the DCC Management Response (updated as appropriate following SECAS advice) and the SECAS validation and to provide comments to the SSC.

Assessment of Compliance

5.9 Following the completion of the initial Full DCC Security Assessment of 4G CH Triage Activities, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Management Response.

5.10 After considering the initial Full DCC Security Assessment Report and the DCC Management Response, the compliance status shall be set in accordance with Sections G9.28 to G9.31.

5.11 The Security Sub-Committee shall identify whether any remaining non-compliances exist and shall, where appropriate:

(a) note and record that there are no non-compliances; or

(b) note and record the specific non-compliances that need to be addressed.

5.12 Where the Security Sub-Committee identifies no non-compliances, then it will notify that the DCC and its relevant SPs may undertake 4G CH Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage, supported by the SEC and the DCC, Use Case 005, 4G CH Triage Specification.

5.13 Where the Security Sub-Committee identify specific non-compliances, they will confirm:

(a) whether Triage Activities may be undertaken and specific non-compliances remediated by a specific date; or

(b) whether Triage Activities must not be undertaken until the specific non-compliances have been remediated to the satisfaction of the Security Sub-Committee; or

(c) whether a Follow-up Security Assessment is required to be completed to confirm the specific non-compliances have been satisfactorily remediated.

Scheduling a subsequent DCC Security Assessments of 4G CH Triage Activities

5.14 Within 12 months following completion of the initial DCC Security Assessment of 4G CH Triage Activities, the DCC shall schedule a subsequent DCC Full Security Assessment with the DCC CIO.

Appendix A – Frequently Asked Questions

(Note that greater detail is provided in 4G CH TSCF Appendix B that will address many of the FAQs)

How do I engage with the DCC CIO?

The DCC will engage directly with the DCC CIO. The DCC will facilitate engagement by the DCC CIO with the relevant DCC SPs and CHTFP and participate around any scheduling questions. Typically, the assessment schedule for all 4G CH Triage parties will be agreed by the DCC and DCC CIO before the start of Triage Activities and before the start of each assessment year. The DCC will provide the Security Sub-Committee with a Forward Look of Security Assessments.

When should I begin preparation and evidence gathering for the assessment?

It is strongly recommended that preparation and evidence gathering for the 4G CH Triage process begin three months prior to the assessment date. The DCC CIO will accept implementation evidence, such as security logs, if they are less than 3 months old.
The DCC, its relevant Service Providers and CHTFP are advised that a lack of relevant and timely evidence could result in an Inadequate rating within the report.

When will I get my assessment report?

Unless otherwise agreed, a draft DCC Security Assessment report will be released to the DCC for review 10 days after the final day of the fieldwork at the same time that it is released to the SSC. The DCC will then have 15 days to compile the DCC Management Responses to the identified observations and submit these to SECAS. This will be considered as the DCC Security Assessment Response, as mandated by G9.21. In the interim, the DCC will have 5 days to provide the DCC CIO with comments with regards to factual accuracy checking or any report queries. The DCC CIO will then have 5 days to respond to the DCC to accept, explain or reject and make updates to the report, which will be sent back to the DCC.

How do I ensure an efficient assessment?

There are a number of key factors which contribute to ensuring an efficient assessment. It is recommended that the DCC, its relevant SPs and CHTFP:

- Involve their internal audit, governance, risk and compliance teams in preparing for the assessment.
- Have a clearly articulated scope and definition for the 4G CH Triage systems and processes that are under assessment and that identifies interdependencies.
- This scope should take into consideration key requirements from the SSC Guidance on Device Security Assurance and Triage Part 2 Section 8 (Use Case 005) and the DCCs ‘Use Case 005 Triage Specification Document’ and relevant parts of SEC Section G12 noting that compliance with SEC Sections g2, G4, G5 and G6 will be assured via the DCC Security Controls Framework (SCF).
- The scope should also take into consideration key definitions from the SEC, such as “DCC Total System”, “DCC Internal Systems”, “DCC Systems”, “DCC IT Supporting Systems” and “Separate”.

- Have a 4G CH Triage process diagram that clearly demonstrates a) the roles of different parties in the 4G CH Triage Activities, b) how 'Separation' has been achieved and c) identifies the security controls to treat the risks identified in the risk and specifically that the 'Unlock' and 'Relock' functions are securely carried out.]
- Ensure that risks have been thoroughly assessed, factoring in impacts to the Confidentiality, Integrity and Availability of in-scope assets.
- Have a clearly defined traceability matrix linking the in-scope security obligations the DCC is required to meet to the security controls implemented which the DCC deems supports their compliance.
- Provide the DCC CIO with the required documentation including hard and soft copies in a timely manner prior to the start of the assessment. The DCC should consider existing certifications which could be relied upon by the DCC CIO, e.g. ISO 27001 certificates for an appropriate scope.
- Be prepared to show and/or upload to the DCC GRC tool the DCC CIO evidence (the DCC SCF Part 2 provides relevant examples) to support the obligations under assessment.
- In the case of assessments at the DCC or DCC SP site, provide meeting locations including a permanent 'base' location for the DCC CIO onsite team to be located throughout assessment.
- Have the appropriate staff or suitable alternates available throughout the assessment and inform the DCC CIO in advance if any key staff are unavailable.
- Remain transparent and cooperate with the DCC CIO throughout the assessment.

How will the DCC CIO take account of existing security certifications, such as ISO 27001?

The DCC CIO will take account of existing security certifications and assess whether reliance can be placed upon them during the course of the review. For example, if a SP or CHTFP holds ISO 27001 certification for the scope of their part of the 4G CH Triage process, there is a likelihood that the DCC CIO will be able to place reliance upon this, subject to being able to confirm the exact scope of certification, the level of testing performed, and whether any material changes had occurred since certification was awarded.

Whom might the DCC CIO need to meet with?

Within the DCC, its relevant Service Providers and 4G CHTFP, the DCC CIO may need to meet:

- Chief Information Security Officer (CISO) / lead security consultants and architects
- Security Director and lead security consultants and architects
- ISMS officer / manager
- Security Operations Centre (SOC) Manager
- Service Provider (SP) Security Personnel
- System administrators
- Solution designers
- Human Resources representatives
- Internal audit / Compliance
- Third parties (where applicable

Appendix B –Security Obligations Applicable to the DCC, its relevant SPs and CHTFP

The security obligations relevant to 4G CH Triage Activities are outlined in the tables below:

Table 1: obligations specific to Use Case 005 that are specified in 'SSC Guidance on Device Security Assurance and Triage Part 2 Section 8' and require compliance with the processes set out in the 'DCC, Use Case 005, 4G CH Triage Specification'; and - Table 2: relevant obligations on 4G CH Triage Facility Providers (CHTFPs) aligned to SEC Section G12.

Note that compliance with SEC Sections G2, G4, G5, G6 and G9 will be assured by the wider DCC Security Controls Framework (DCC SCF).

TABLE1:

Security Requirements are specified in the SSC Guidance on Device Security Assurance and Triage Part 2 Section 8.

Many requirements are met via the DCC's 'Use Case 005 Triage Specification Document' that should be read alongside this 4G CH TSCF.

Section 8.4 (DCC, DCC DM and 4G CHTFP)	**Comms Hub Triage Provider's Triage System:** a secure IT system established and operated by the CHTFP, typically as part of a designated reverse logistics handling function, and which connects to other systems to perform functions including at least: • gather the correct inputs necessary for refurbishment (e.g. firmware and certificates to be used), and validate their integrity and authenticity • communicate with the target CH to obtain its identity details • request Unlock messages (including MAC and signature) from the DCC • deliver Unlock messages to a target CH • generate and deliver diagnostic and refurbishment sequence messages to a target CH • confirm the final state of the refurbished CH.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' in Section 3 – 5 and Appendix D section 9 and particularly section 9.6.

What the DCC CIO might expect to see	• Evidence of the process for initial 4G CH diagnostics including suitability for refurbishment; • Evidence of gathering necessary inputs and validation of CH identity details, integrity, authenticity and record keeping; • Evidence of a secure unlocking process by the DCC DM and CHTFP including any failure handling; • Evidence of the refurbishment process including sanitisation and updating firmware to the latest stable version; • Evidence of Validation of Refurbishment by DCC DM that the Test Bench Client has successfully sent "GetInformation" command with dummy signature to updated 4G CH Device normal application to read the new device public keys and org certificates serial number.

Section 8.4 (DCC, DCC DM and 4G CHTFP)	Communication with the DCC system for Triage activities must use a secure Virtual Private Network connection (or suitable private connection) that includes mutual authentication and appropriate confidentiality, integrity and authenticity protection of the communications.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' in Section 3.4.3.2 and Appendix B.
What the DCCCIO might expect to see	• Evidence that communication across the Triage System Interface (between DCC Systems and CHTFP Triage System) uses standard secure, protocols (as defined in Appendix B) and a dedicated secure Multi-Protocol Label Switching (MPLS) communication solution provided by Gamma, so-called "Gamma-link". • Evidence that the End point in the CHTFP's Facility is directly to the Gateway (access point) for the Triage System. • Evidence that the Gateway system establishes independent network links to each authorised Test Bench Client system, and these are intimately coupled to their respective Test Bench (Test Tool) HW adapter jigs that facilitate communication to subject 4G CHs that are to undergo Triage Activities. • Evidence that components of the DCC network such as Device Manager, OMS, and SharePoint are accessed via the Triage System Interface using a set of specifically design interfaces. The interfaces provide access to the DCC services via authenticated API access.
8.5.1 Decommissioning Devices prior to Triage (DCC)	The DCC is responsible for the process to ensure that the notification of removal of the CH from its installation site (or other location) to the CHTFP site is recorded and to ensure that the CH status in the DCC's SMI is correctly updated to show that the Device is not installed and is in a de-commissioned state.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 4.1.3.

What the DCC CIO might expect to see	• Evidence that the DCC provides and maintains a process to ensure to ensure that the notification of Removal of the 4G CH from its installation site and its transfer to the CHTFP site via the defined handling, and logistics service is recorded. • Evidence that the 4G CH status in the DCC's SMI is correctly updated to show that the Device is not installed. • Evidence that the DCC process ensures that the removed Device is moved to a status of being "Decommissioned".
8.5.2 Responding to Unlock requests (DCC, DSP, DCC DM and 4G CHTFP)	The DCC is responsible for validating the request for an Unlock message (using a statement of target CH identity that has been signed by the target CH), including confirming that the target CH is recorded as being in a suitable state for refurbishment by the CHTFP, and supplying a valid Unlock message if (and only if) the validation checks are successful.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 4.2.5.
What the DCC CIO might expect to see	• Evidence that the DCC has a secure process for validating the request for an Unlock message and assessing the status of the identified 4G CH Device before issuing an Unlock command.

	• Evidence that the CHTFP has confirmed the target 4G CH Device identity - see Appendix D, section: **Error! Reference source not found.** , **Error! Reference source not found.**. • Evidence that the DCC DM will only receive Unlock requests from an authorised CHTFP. • Evidence that the DCC DM process will validate the 4G CH Device GUID as provided in the notification using the currently registered Device CHF Digital Signing credentials according to the GUID received. • Evidence that the DCC DM process verifies that the target CH is recorded as being in a suitable state for refurbishment by the CHTFP and this includes that the candidate 4G CH Device is in the Decommissioned state (for devices being returned after previously being Installed). • Evidence that the DCC DM generates and provides a valid Unlock message if (and only if) the validation checks are successful. • Evidence that Unlock commands generated by DCC DM will not use Future Dating and use a protection against replay counter that is a continuation of any previous use of this command for a 4G CH device with the verified GUID.

8.5.3 Supplying inputs for refurbished device (DCC)	The DCC is responsible for supplying the CHTFP with the correct firmware and other content to be put onto the target CH during the refurbishment sequence.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 4.2.8.
What the DCC CIO might expect to see	• Evidence that the 4G CH Manufacturer has provided tested and certified firmware and configuration data Refurbishment Packs to the DCC for subsequent management by DCC DM during Triage Activities. • Evidence that DCC Operations will perform an offline verification to ensure the firmware included in the pack aligns with CPL approvals and then shares with the DCC DM. • Evidence that the DCC DM conducts validations a) of the Hash Validation, utilising the SHA-256 algorithm to verify the integrity of the files; and b) of the Digital Signature, validating the digital signature present in the metadata using the Manufacturer's public certificate to confirm authenticity. • Evidence that the two Refurbishment Packs are represented by configuration items managed by the DCC DM. • Evidence that the format of the Refurbishment Pack metadata is maintained in the DCC Interface Specification document SD4.20.40, *DM Portal User & DCC SharePoint Interface Specifications*, DCC_IF40, (DCC). • Evidence that the DCC securely stores the material received from the Manufacturer.
8.5.4 Updating Device records after Triage (DCC & 4G CHTFP)	The DCC is responsible for updating their records for the target CH to reflect the notification from the CHTFP of the new Keys generated for the triaged Device (and any other updates to technical parameters associated with the target CH, removing any associations with a previous installed location), and for confirming the other Certificates present on the triaged Device.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 4.2.9.

What the DCC CIO might expect to see	• Evidence that the DCC is maintaining and updating records for the target 4G CH to ensure new Keys generated for the triaged Device (and any other updates to technical parameters associated with the target CH) are correctly recorded. • Evidence that the DCC removes any associations with a previous installed location, • Evidence that the DCC ensures the Certificates installed on the 4G CH Device following Refurbishment (Factory Reset in Use Case 005) are correct according to the required configuration. • Evidence that the CHTFP Triage System process reads the newly installed device public keys and org certificates serial numbers.
8.5.5 Receiving and preserving downloaded logs (DCC & 4G CHTFP)	The DCC is responsible for receiving and preserving the logs that the CHFTP has downloaded from a target CH before the refurbishment sequence is executed.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 4.2.10.
What the DCC CIO might expect to see	• Evidence that, after use of an Authorized Unlock and during the subsequent diagnostics stage (before Refurbishment) the CHTFP will download Logs from the Unlocked 4G CH Device. • Evidence that the downloaded logs are as listed in Appendix D, section **Error! Reference source not found.**, **Error! Reference source not found.**. • Evidence that the DCC manages these logs securely including access control and retention periods.
8.5.6 Assuring the Triage and refurbishment process (DCC)	The DCC is responsible for producing a 'Use Case 005 Triage Specification Document', and the DCC CIO is responsible for providing assurance in the Triage and refurbishment process via the DCC CIO annual assessment of DCC Service Providers (in accordance with the DCC Security Controls Framework required by SEC Section G7.19(a) and G9.2(d)(iv)).
What the DCC CIO might consider	See the DCC's 'Use Case 005 Triage Specification Document', particularly section 5.1
What the DCC CIO might expect to see	• Evidence that the DCC's 'Use Case 005 Triage Specification Document' is regularly reviewed and maintained. • Evidence of DCC CIO Assessments in line with the DCC Security Controls Framework and this 4G CH TSCF.

8.6.1 Triage and refurbishment process (DCC & CHTFP)	The CHTFP prepares the target 4G CH for Triage, gathering the correct firmware image and configuration data to be applied (according to specification by the DCC);
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 4.2.8; 9.6.18 and 9.6.19.
What the DCC CIO might expect to see	• Evidence that the 4G CH Manufacturer has provided tested and certified firmware and configuration data Refurbishment Packs to the DCC for subsequent management by DCC DM during Triage Activities. • Evidence that DCC Operations will perform an offline verification to ensure the firmware included in the pack aligns with CPL approvals and then shares with the DCC DM. • Evidence that the DCC DM conducts validations a) of the Hash Validation, utilising the SHA-256 algorithm to verify the integrity of the files; and b) of the Digital Signature, validating the digital signature present in the metadata using the Manufacturer's public certificate to confirm authenticity.
8.6.1 Triage and refurbishment process (DCC & CHTFP)	The CHTFP downloads and preserves the security and event logs from the target CH (and any other logs that may contain records of triage mode Unlock commands) and sends them to the DCC for storage, in accordance with SSC-approved policy;
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 9.2.
What the DCC CIO might expect to see	• Evidence that the CHTFP downloads and preserves the security and event logs from the target 4G CH (and any other logs that may contain records of triage mode Unlock commands) and sends them to the DCC for storage. • Evidence that the DCC stores security and event logs in accordance with the DCC's Data Retention Policy.
8.6.1 Triage and refurbishment process (DCC, DSP, DCC DM and 4G CHTFP)	An Unlock message is requested from the DCC for the target CH, including MAC and signature as for a GCBS critical (SME.C.C) message;

What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 9.6.29.

What the DCC CIO might expect to see	• Evidence that the DCC has a secure process for ensuring the request for an Unlock message is authentic and authorised. • Evidence that the Unlock message will allow commands to be sent to the CH using the CSP pins until the device is rebooted/power is removed. • Evidence that the 4G CH Device checks for a WAN Provider digital signature on Unlock messages. • Evidence that the DCC DM provides a ACB Message Authentication Code (MAC) in accordance with GBCS specifications. • Evidence that the message has 'Protection Against Replay'. • Evidence that the CH checks that the Originator Counter in the Command has a value that is greater than the value held by the Device for this type of Command in the corresponding Immediate Execution Counter.
8.6.1 Triage and refurbishment process (DCC, DCC DM, CHTFP)	The Unlock message is sent to the target CH, leaving it in an unlocked state (if the CH rejects the Unlock message then CHTFP policy will define the approach to retrying and/or when a decision would be reached to securely destroy the target CH);
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 9.6.2.

What the DCC CIO might expect to see	• Evidence that, during its normal power-on start-up mode, the 4G CH will detect its environmental context to determine if a suitable a communication connection is formed between the 4G CH and the Test Bench using the serial communication protocol. • Evidence that the Test Bench Client validates that the CHF GUID event matches the CHF GUID and, if there is a mismatch in CHF GUID, the operation is terminated. • Evidence that the Test Bench Client application sends the validated CHF GUID and its signature to DM for validation. • Evidence that 4G CH unlocking is validated. • Evidence that, if the unlock command is resent to an already unlocked CH, the device will generate a valid response, indicating through a payload that the device is already unlocked.
8.6.1 Triage and refurbishment process (CHTFP)	Diagnostic commands are sent to the target CH to determine whether it is suitable for refurbishment;
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 9.3.
What the DCC CIO might expect to see	• Evidence that the Test Bench interacts with the 4G CH and performs a series of tests to determine if the device has any Faults. These tests should be sequential and failure in one result should not affect the next test. • Evidence that a test report is generated at the end of all tests and sent to DCC OMS to decide the next best action.

	• Evidence of an effective process to determine if the device is suitable for refurbishment and that this is recorded and the device proceeds to the refurbishment process. • Evidence that a Fault Analysis Report (FAR) is generated irrespective of the test results.
8.6.1 Triage and refurbishment process (CHTFP)	If the target CH is not suitable for refurbishment then it is securely destroyed by the CHTFP and records kept;
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 4.2.1.

What the DCC CIO might expect to see	• Evidence that, when a device is diagnosed as unsuitable for refurbishment, then it is securely destroyed by the CHTFP and records maintained. • Evidence that, if the CHTFP refurbishment sequence is not successful i.e. if any test or check fails, then the target 4G CH is securely destroyed by the CHTFP and the CHTFP notifies the DCC to update their status record. • Evidence that a Fault Analysis Report (FAR) is generated irrespective of the test results.
8.6.1 Triage and refurbishment process (DCC, CHTFP)	If the target CH is suitable for refurbishment then the CHTFP applies the refurbishment sequence (using the new firmware image and configuration data), which also ensures the deletion of any sensitive data on the target CH (including consumption data as appropriate in section 8.7 below);
What the DCC CIO might consider	• See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' Appendix D (Section 9).
What the DCC CIO might expect to see	• Evidence that the CHTFP prepares the target 4G CH for Triage, gathering the correct firmware image and configuration data to be applied (according to specification by the DCC) as described in section **Error! Reference source not found.**. • Evidence that the CHTFP downloads and preserves the security and event logs from the target 4G CH (and any other logs that may contain records of triage mode Unlock commands) and sends them to the DCC for storage, in accordance with SSC-approved policy. • Evidence that an Unlock message is requested from the DCC for the target CH, including a WAN Provider signature and an ACB-SMD MAC in the same way as for GCBS critical (SME.C.C) messages, see section **Error! Reference source not found.**. • Evidence that the Unlock message is sent to the target CH, leaving it in an unlocked state (if the 4G CH rejects the Unlock message, then CHTFP policy will define the approach to retrying and/or when a decision would be reached to securely destroy the target 4G CH.

	• Evidence that Diagnostic commands are sent to the target 4G CH to determine whether it is suitable for refurbishment, see section **Error! Reference source not found.**. • Evidence that, if the target 4G CH is not suitable for refurbishment, then it is securely destroyed by the CHTFP and records kept. • Evidence that, if the target 4G CH is suitable for refurbishment then the CHTFP applies the refurbishment sequence (using the new firmware image and configuration data), which also ensures the deletion of any sensitive data on the target 4G CH (including consumption data as appropriate), see section **Error! Reference source not found.** and the Sanitise section **Error! Reference source not found.**.
8.6.1 Triage and refurbishment process (DCC, CHTFP)	If the refurbishment sequence is not successful then the target CH is securely destroyed by the CHTFP and the CHTFP notifies the DCC to update their status record for the target CH to reflect the destruction (and to prevent reuse of the device identifier);
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' Appendix D Section 9.2.
What the DCC CIO might expect to see	• Evidence that, if the refurbishment sequence is not successful then the target 4G CH is securely destroyed by the CHTFP and the CHTFP notifies the DCC to update their status record for the target 4G CH to reflect the destruction (and to prevent reuse of the device identifier).
8.6.1 Triage and refurbishment process (DCC, CHTFP)	If the refurbishment sequence is successful then the CHTFP notifies the DCC to update their status record and configuration records for the target CH, and releases it for re-installation
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' Section 9.2.
What the DCC CIO might expect to see	• Evidence that, if the refurbishment sequence is successful, then the CHTFP notifies the DCC to update their status records and configuration records for the target 4G CH and releases it for re-installation.

8.6.2 Additional rules (DCC, CHTFP)	None of the commands used in Triage may be capable of future-dated invocation. Any diagnostic commands available after unlocking must not perform any critical refurbishment actions.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly Section 9.7.1.

What the DCC CIO might expect to see	• Documentary evidence that none of the commands used in Triage Activities (Diagnostics or Test) will be presented with the intention of future-dated invocation by any means, e.g. attempted use of GBCS fields devised for this purpose. • Documentary evidence that all command generated by the DCC Systems or the CHTFP's systems for submission to the 4G CH Device will not contain future dated commands. • Documentary evidence that the 4G CH Device will verify that no future dating is present in any command received over its Triage Interface and will reject any such command formation. Note that this requirement will have been assured under the Device CPA evaluation.
8.6.2 Additional rules (DCC, CHTFP)	Triage mode on the target CH is required to lock on any of the actions specified in the SC mitigations for locking triage mode on a 4G CH (see DEV.5.M<105> 'Locking Triage mode' in Section 5.1 of *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC & CH SCs and CPA Build Standard Extensions"*). It must not be possible to install a 4G CH while Triage mode is unlocked: CH design must confirm that Triage mode can never be unlocked when a CH is subject of Install and Commission or Operational use.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 9.6.5.

What the DCC CIO might expect to see	• Evidence that, if the connection has changed either through loss of power, or loss of physical connection, then the 4G CH Device will perform its normal shutdown process according to its 4G CH Device design. • Evidence that, as part of shutdown, any established Test Bench communications session will be terminated and the 4G CH Device is locked. • Evidence that, where a shutdown results in the device being locked, a new Unlock command must be requested by the Test Bench Client. • Evidence that 4G CH Device Unlock Commands cannot be replayed, they must be regenerated through a new request from the Test Bench Client to DM and then back to 4G CH Device. • Evidence that, restarting the Triage Process without full power cycle by removing the device from the Test Bench hardware, the 4G CH Device status is changed to lock once unplugged and if the device is connected back after 5 seconds, then 4G CH Device restart the Triage Process. • Evidence that, if the device is unplugged and not plugged back at all then the normal shutdown is performed as per 4G CH Device design. • Documentary evidence that the DCC will not attempt to install an unlocked 4G CH.
8.6.2 Additional rules (DCC, CHTFP)	The CHTFP is required to record the actions performed on the target CH (and to preserve a record of the connection between the old and new CH identities).

What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 4.2.9.

What the DCC CIO might expect to see	• Evidence that the CHTFP records the actions performed on the target CH (and preserves a record of the connection between the old and new CH identities). • Evidence that the CHTFP retains details of any batch in which a Device was processed or can be inferred from the CHTFP's records based on the date/time of the Device's processing. • Evidence that the CHTFP can return records for a) a specific identified device or b) a group constituting a *batch* (as defined by the CHTFP's scheduling and organisation of Triage Activities • Evidence that the records are maintained by the DCC Asset Management system. • Evidence that the DCC is able to provide the SSC with up to date records on request, this is to support longer term considerations, such as assessing a newly discovered vulnerability, or analysis or other security concerns including group effects,
8.8 Requirements relating to DCC interactions (DCC, DSP, DCC DM, CHTFP)	The DCC will ensure secure communications with the CHTFP to (including, but not limited to): • enable the CHTFP to obtain the Unlock messages for a target CH that the DCC confirms is in an appropriate, noninstalled state (including MAC and signature);
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 3.4.3.2.
What the DCC CIO might expect to see	• Evidence that the communication across the Triage System Interface (between DCC Systems and CHTFP Triage System) uses standard secure, protocols (as defined in Appendix B) and a dedicated secure Multi-Protocol Label Switching (MPLS) communication solution provided by Gamma, so-called "Gamma-link". • Evidence that an Unlock message is requested from the DCC for the target CH, including a WAN Provider signature and an ACB-SMD MAC in the same way as for GCBS critical (SME.C.C) messages, see section **Error! Reference source not found.**.
8.8 Requirements relating to DCC interactions (DCC, DCC DM and 4G CHTFP)	The DCC will ensure secure communications with the CHTFP to (including, but not limited to): • enable the DCC to authorise the CHTFP to perform refurbishment when appropriate;

What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 4.2.1.
What the DCC CIO might expect to see	• Evidence that the DCC DM provides and maintains secure communications with the CHTFP to enable the DCC to authorise the CHTFP to perform refurbishment when appropriate.

	• Evidence that interactions between DCC DM and the CHTFP related to authorising the Refurbishment of a 4G CH are supported by service functions made available on the interfaces between the DCC DM and the CHTFP as described in section:**Error! Reference source not found.**, **Error! Reference source not found.**.
8.8 Requirements relating to DCC interactions (DCC, DCC DM and 4G CHTFP)	The DCC will ensure secure communications with the CHTFP to (including, but not limited to): • enable the CHTFP to request signing of new device credentials, and enable the DCC to respond with signed credentials;
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 4.2.2.
What the DCC CIO might expect to see	• Evidence that the DCC DM provides and maintains secure communications with the CHTFP to enable the CHTFP to request signing of new Device credentials and enable the DCC DM to respond with signed credentials. • Evidence that, during the Refurbishment task, the CHTFP Test Bench Client application sends 'Issue Device Credentials' command (with dummy signature) to the 4G CH Device to create the new pending private/public keys. • Evidence that the Device responds with a CSR for each of: 1. CHF Digital Signature 2. CHF Key Agreement 3. GPF Digital Signature 4. GPF Key Agreement • Evidence that, if the status is 'OK', the Testbench Client will proceed with Refurbishment process and, during update, key rotation is performed from the pending device keys to active keys in the 4G CH Device.

8.8 Requirements relating to DCC interactions (DCC, DCC DM and 4G CHTFP)	The DCC will ensure secure communications with the CHTFP to (including, but not limited to): • enable the CHTFP to notify the DCC of the refurbished CH identity and configuration details (and of other results such as secure destruction of a target CH).
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document', particularly section 3.2.1.
What the DCC CIO might expect to see	• Evidence that, after refurbishment, the secure interface enables the Test Bench to send the Fault Analysis Report along with device logs to DCC OMS. • Evidence that, at the end of Triage and Diagnostics, the secure interface notifies DCC OMS of the next action (Dispose/Refurbish/Return to Vendor). • Evidence that, the secure interface enables the Test Bench to notify the DCC OMS about the Refurbishment status which leads to ORR status update by OMS.

	• Evidence that the secure interface enables CHTFP to notify DCC OMS to dispose of the identified Comms Hub.

TABLE 2:

Security Requirements in SEC Section G12 'Security Assurance of Device Triage Facilities' insofar as they relate to 4G CH Triage Activities

Where relevant, some of these requirements are met via the requirements in Table 1 since they are specified in the DCC's 'Use Case 005 Triage Specification Document' that should be read alongside this 4G CH TSCF. In these cases, the security requirements are cross-referenced to avoid duplication.

SEC Obligation G12.4(a)	Each Triage Facility Provider shall: (a) not attempt to undertake "Triage Activities" on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process); *Note: This obligation relates only to "the tamper -protection boundary required by CPA Security Characteristics*
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section Appendix A and section 4.1.2 Note: This requirement relates to a 'Secure Perimeter' tamper event and not an 'Installation'' tamper event. The Installation Tamper event must occur upon device removal from the installation premises (except where the device is not functional or has no power) and is likely to be a common occurrence and an 'allowable breach' in 4G CH Triage Activities and will have already triggered an alert. The CHTFP assessment for this requirement can only examine the device for evidence of attempts to tamper by: 1. Inspection of the device Secure Perimeter as defined for CHTS (SEC, 2017, Schedule 10, section 4.3), or 2. Inspection of seals or tamper evident coating that satisfy requirements of CPA CH SC (Section DEP.3.M925).

What the DCC CIO might expect to see	• Evidence that all 4G CHs arriving at the 4G CHTFP are placed into a Goods Inwards storage area before being scheduled for entry to the Test Bench based Triage and Use Case 005 process. • Evidence that the Device undergoes a visual inspection by an assigned Triage Facility Operator who will refer to a CHTFP Returned Device Inspection Checklist to ensure the Physical Inspection is compliant with DCC requirements and the SEC obligation to not permit tampered 4G CHs to proceed to the Triage Activities. • Evidence that, where the visual inspection identifies damage or signs of tamper, the Operator will take photographic evidence of damage or tamper evidence for inclusion in the Preliminary Fault Analysis Report (PFA). • Evidence that 4G CHs with evidence of tamper will be repackaged and placed in the designated storage area.

SEC Obligation G12.4(b)	Each Triage Facility Provider shall only use a Triage Tool and Triage System Interface that is provided by a manufacturer to access the manufacturer's "Triage System" that has confirmed compliance with the requirements of the Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly Appendix B Note: There is some overlap with Table 1: Section 8.4 (DCC, DCC DM and 4G CHTFP) "*Communication with the DCC system for Triage activities must use a secure Virtual Private Network connection (or suitable private connection) that includes mutual authentication and appropriate confidentiality, integrity and authenticity protection of the communications.*"
What the DCC CIO might expect to see	• Evidence that the Test Bench specification, architecture and processes defined in the DCC's 'Use Case 005 Triage Specification Document' are maintained and updated to meet the requirements of the Triage Tool in SEC Section G12(b). • Evidence that the Triage System Interface requirements are met by the responses to Table 1: Section 8.4 (DCC, DCC DM and 4G CHTFP) relating to a secure VPN with mutual authentication and appropriate confidentiality, integrity and authenticity protection of the communications.
SEC Obligation G12.4(c)	Each Triage Facility Provider shall ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage Interf ace;

What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly Appendix C
What the DCC CIO might expect to see	• Evidence of adherence with the role-based access control policy, procedures, including a review of the ongoing relevance of the access privileges granted to personnel in line with the 'need to know' principle. • Evidence that access credentials for the Test Bench Client (Triage Tool), are tightly controlled and a 90-day forced change of passwords has been implemented. • Evidence that joiners, movers and leavers are handled in compliance with policies and the access rights are removed from the system controlling access where appropriate. • Evidence that access the Test Bench Client PC that contains the Test Bench executable application requires Active Directory login credentials including user name and password. • Evidence that AD access credentials will not allow the Test Bench Client PC to be used for any purpose other than for defined Test Bench activity. • Evidence that a secondary authentication is required by the Test Bench Operator based on use of a username and password. These credentials are in addition to, and separate from the Active Directory credential and are required to be successfully presented by the Operator before the application can be used.

SEC Obligation G12.4(d)	Each Triage Facility Provider shall at all times prevent unauthorised use of the Triage Tool and Triage System Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly Appendix C relating to physical security.
What the DCC CIO might expect to see	• Evidence of the physical security controls to prevent access to the Test Bench Client. • A documented process which details the controls in place to prevent unauthorised use and ensure the physical security of the Triage Tool, Triage System Interface and any Devices within the Triage Facility in which Triage Activities take place. • Evidence that the CHTFP has implemented sufficient controls to prevent unauthorised use and ensure the physical security of the Triage Tool, Triage System Interface and any Devices within the Triage Facility. • Evidence that the Triage Tool within the Triage Facility has only been unlocked for use by an authorised operative.

SEC obligation 12(f)	Each Triage Facility Provider shall maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of: (i) the Requestor of any change to the configuration of a Device; (ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities; (iii) details of Triage Activities successfully undertaken; (iv) details of any failed attempts to complete Triage Activities; and (v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor;
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 3.2.6
What the DCC CIO might expect to see	• Evidence that the DCC Asset Management System (part of the DCC Asset and Supply Chain division) maintains up to date records of: ○ All notifications of process progression, success and failure, as well as all associated records. ○ All asset data sets including: (i) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities. (ii) details of Triage Activities successfully undertaken. (iii) details of any failed attempts to complete Triage Activities; and (iv) confirmation that tamper-protection as defined and agreed to meet the requirements of the CPA Security Characteristics are established to the same standard as during original manufacture before returning a Device.
SEC Obligation G12.4(g)	Each Triage Facility Provider shall when requested by the Security Sub-Committee to do so, provide the Security SubCommittee with an up-to-date copy of the records maintained pursuant to Section G12.4(f)
What the DCC CIO might consider	See the descriptions in the DCC's 'Use Case 005 Triage Specification Document' particularly section 3.2.6 This requirement overlaps with Table 1: 8.6.2 "*Additional rules (DCC, CHTFP): The CHTFP is required to record the actions performed on the target CH (and to preserve a record of the connection between the old and new CH identities).*"

What the DCC CIO might expect to see	• Evidence that the DCC Asset Management system is able to provide the SSC with up to date records on request and that the request can return records for: ○ A specific identified device ○ A group constituting a *batch* (as defined by the CHTFP's scheduling and organisation of Triage Activities) which can be used to identify effects that may have resulted from the Triage System configuration or issues that may be consequential to use of material provided for use in Refurbishment etc.