Appraisal log

Crime and Corruption Commission retention and disposal schedule

Crime and Corruption Commission

Date: May 2017

Organisational context

After the 1987–89 Fitzgerald Inquiry into police corruption, the Criminal Justice Commission (CJC) was established in 1989 to help restore confidence in Queensland's public institutions. The two-year inquiry also led to the creation of the Queensland witness protection service within the CJC.

The CJC investigated police and public sector misconduct, as well as working with the police to investigate organised and major crime. In 1997, the CJC's crime function was given to the newly formed Queensland Crime Commission (QCC), which was also tasked with investigating paedophilia.

In 2001, the Queensland Government decided to form a single body to fight crime and public sector misconduct — the Crime and Misconduct Commission (CMC), a statutory body created under the *Crime and Misconduct Act 2001*.

Following extensive reviews and legislative changes, the *Crime and Misconduct Act 2001* changed to the *Crime and Corruption Act 2001* and the CMC became the Crime and Corruption Commission (CCC). A new jurisdiction and framework for the CCC was developed with a focus on serious and systemic corruption. In addition, changes are necessary to meet requirements under the *Telecommunications (Interceptions and Access) Act 1979.* These changes and requirements have driven the need to amend the existing CCC schedule.

Summary of changes

Changes not affecting retention and disposal

Across the whole schedule, general changes have been made:

- references to Crime and Misconduct Commission have been changed to Crime and Corruption Commission
- the *Crime and Misconduct Act 2001* is now the *Crime and Corruption Act 2001*
- Act references relating to the *Crime and Corruption Act 2001* and the *Police Powers and Responsibilities Act 2000* have been updated
- terminology such as 'misconduct' and 'integrity' have been changed to 'corruption'.

Retention period & trigger of 'after business action completed' has been updated for this version to agree with the schedule.

Other minor changes not affecting retention and disposal are documented in a table at the end of the log.

Changes affecting retention and disposal

The following information outlines changes to record classes in version 1 that will impact the retention periods of records managed by the CCC. Other classes which remain unchanged have not been noted here. Version 2 of the schedule shows all classes.

Analysis, including liaison with agency staff, has been undertaken to ensure that the changes meet agency and whole-of-government recordkeeping requirements.

Function	Scope note
INFORMATION MANAGEMENT	*The function of providing services based on information and information products. Includes library and records management services.* *This section includes records relating to information management having different retention periods or other special requirements from those information management records covered by the General Retention and Disposal Schedule.*

Activity
CONTROL

Disposal authorisation	Record class and retention period	Justifying the retention period
1801	***Information retrieval requests*** Records relating to requests by the Crime and Corruption Commission (CCC) for information from external agencies or from a telecommunications provider. Includes requests made on a Form4, copies of the information retrieved by these requests and, when the request relates to telecommunications information, a copy of the authorisation issued under s.178–180 of the *Telecommunications (Interception and Access) Act 1979*. This material must be retained until the review under s.187N of the *Telecommunications*	**Changes to this record class:** • entity name • act and section of act under which certificates are issued • retention period & trigger changed from '5 years after last action' • scope of class has changed to include only requests made by the CCC • copies of information provided by agencies removed and covered under reference 1802. **Background/business process:** This record class relates to requests by the CCC for information from external agencies or from a telecommunications provider. The class includes copies of information received from these requests. The TIA Act enables access to telecommunications data by a limited group of law enforcement and national security agencies. The legislation authorises the disclosure of telecommunications data in certain circumstances. Service providers must provide help to agencies requesting access to retained data. Where access to data is required, an authorised officer of the CCC requests the data from the service provider. Providers receiving requests must comply with the recordkeeping requirements in part 13, division 5 of the TIA Act. Amendments to Chapters 4 and 5 of the TIA Act in October 2015 signify that the retention of telecommunications data provided by carriers is subject to strict requirements, which are audited by the

Disposal authorisation	Record class and retention period	Justifying the retention period
	(Interception and Access) Act 1979 (TIA Act) is complete. The review must conclude on or before the third anniversary of the implementation phase. For authorisations, the minimum retention period is three years beginning on the day the authorisation is made. For all other information and documents the retention period is three years after the item came into existence. **Retention period & trigger** 3 years from date of authorisation **AND** once review under s.187N is complete.	Commonwealth Ombudsman annually. Telecommunications data (i.e. 'information and documents') provided by carriers include: • the number called or texted, the time and date of a communication, general location information, or the duration of the communication • information about the parties to the communication (e.g. the name, address, postal and billing information in relation to a customer, the customer's mobile number, email address or landline phone number, and the mobile number, email address, or land line number of the recipient – if known by the service provider). 'Information and documents' are relevantly obtained under the TIA Act for the purpose of: • enforcing the criminal law • administering a law imposing a pecuniary penalty • administering a law relating to the protection of the public revenue. https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionGuidelinesForServiceProviders.pdf The CCC must give to the relevant carrier an authorisation to access the information and documents required. **Regulatory requirements:** *Telecommunications (Interception and Access) Act 1979:* • s.178–180 – authorisations are issued • s.185(1) and 186A(3) – retention periods are defined • s.187N(3), (4) and (5) – require the head of an agency to keep authorisations, that are issued, until the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the data retention scheme is completed. **Business requirements:** The change to the retention period from five years to three years is due to the changes to the retention requirements in the amended *Telecommunications (Interception and Access) Act 1979.* The additional disposal requirement that includes 'when review under s.187N is complete' is also in response to changes to that legislation. Specifically, subsection 185(1) of the TIA Act requires agencies (such as the CCC) to retain authorisations for a period of three years beginning on the day the authorisation is made. Subsection

Disposal authorisation	Record class and retention period	Justifying the retention period
		186A(3) provides that items relating to authorisations for, and use and disclosure of information and documents, must be kept: (a) starting when the item came into existence; and (b) ending the earliest of either (i) when three years have elapsed since the item came into existence; or (ii) when the Ombudsman gives a report to the Commonwealth Attorney-General about the records that include the item in question. The Ombudsman must report to the Minister, in writing, about the results of inspections of records of an agency as soon as practicable after the end of the financial year. The Ombudsman can request as part of their review, data that is retrieved under an authorisation. In addition to the above, s.187N states that heads of law enforcement agencies must retain these records until after a review of the data retention scheme by the PJCIS. This includes a copy of all authorisations made under Chapter 4 of the TIA Act, a copy of all journalist information warrants (and 68 authorisations made under those warrants) made under Chapter 4 of the TIA Act, as well as information reported each year to the Minister relating to the agency's access to historic telecommunications data.[1] On 17 May 2016, the CCC met with QSA. The CCC Director of Legal Services, Rob Hutchings requested that the information regarding s.187N of the TIA Act be included in the description. The proposed changes were reviewed by Legal Services and were agreed to by the senior managers. **Comparison with other schedules' retention period:** Changes to Commonwealth data retention obligations contained in the TIA Act now apply to all law enforcement agencies. QSA contacted the archival institutions regarding their schedules below. They advised these schedules are yet to be updated with the new retention obligations. *State Records Authority of New South Wales Functional Retention and Disposal Authority: DA201 Independent Commission Against Corruption* Reference 3.2.1 Records relating to requests, reasons and permissions for ICAC to access other databanks – Retain minimum of 5 years after last action, then destroy. *Tasmanian Archive and Heritage Office Disposal Schedule for Functional Records of the Department of Police and Emergency Management Disposal Authorisation No. 2351* Records of telecommunications interceptions obtained in accordance with the *Telecommunications (Interception and Access) Act 1979*

[1] http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf, page 67 and 68

Disposal authorisation	Record class and retention period	Justifying the retention period
		and relating to the function of crime detection and investigation – TEMPORARY Destroy 7 years after date action completed, including legal action. **Previous schedules (where applicable):** *Crime and Misconduct Commission Retention and Disposal Schedule QDAN606 v.1* Reference 1801 Information Retrieval – Retain for 5 years after last action.
1802	***Evidentiary certificates*** Records relating to the issue of a certificate under s.185C of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). This includes the certificate and any supporting documentation. **Retention period & trigger** 3 years after business action completed **AND** once review under s.187N is completed.	**Changes to this record class:** • description title changed from Certificate of disclosure • act and section of act under which certificates are issued • retention period & trigger changed from '2 years after last action'. **Background/business process:** This record class covers evidence certificates issued following receipt of records received following requests by the CCC for information from external agencies or from a telecommunications provider. Evidentiary certificates form part of the criminal brief of evidence to be used in court proceedings. They set down anything done by a CCC officer in connection with obtaining, using and disclosing, making a record of, and/or the giving in evidence of information and documents. **Regulatory requirements:** Evidentiary certificates are given by the CCC pursuant to s.185C of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). This material must be retained until the review under s.187N of the TIA Act is complete, and which must conclude on or before the third anniversary of the implementation phase. Section 186A(3) of the TIA Act provides that any item relating to evidentiary certificates must be kept: (a) starting when the item came into existence; and (b) ending when the earliest of either (i) when three years have elapsed since the item came into existence; or (ii) when the Ombudsman gives a report to the Commonwealth Attorney-General about the records that include the item in question, whichever is earlier. **Business requirements:** The change to the retention period from the previous version is due to provisions in the TIA Act, which prescribe minimum retention periods for evidentiary certificates. This material must be retained until the review under s.187N of the TIA Act is complete, and which must conclude on or before the third anniversary of the implementation phase. Section 186A(3) of the same Act provides that any item relating to evidentiary certificates must be kept: (a) starting when the item

Disposal authorisation	Record class and retention period	Justifying the retention period
		came into existence; and (b) ending when the earliest of either (i) when three years have elapsed since the item came into existence; or (ii) when the Ombudsman gives a report to the Commonwealth Attorney-General about the records that include the item in question, whichever is earlier. At a meeting held on 17 May 2016 between representatives from the CCC and QSA, it was agreed that to retain these records for a period of three years after last action was appropriate and would meet the requirements of the TIA Act. **Comparison with other schedules' retention period:** Changes to Commonwealth data retention obligations contained in the TIA Act now apply to all law enforcement agencies. *National Archives of Australia – Records Authority – Australian Federal Police 2006/00446344* Reference 14418 Records documenting arrangements for and the interception of telecommunications by technical intercept. Includes correspondence with telecommunications carriers, copies of evidentiary certificates – Keep as required for the purposes of applicable telecommunications interceptions and access laws and until other use has ceased; then destroy. **Other comments/factors for consideration:** Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes. **Previous schedules (where applicable):** *Crime and Misconduct Commission Retention and Disposal Schedule QDAN606 v.1* Reference 1802 Certificate of Disclosure – Retain for 2 years after last action.

Function	Scope note
MAJOR CRIME	*The function of dealing with major crime referred to the Crime and Corruption Commission by the Crime Reference Committee. Major crime encompasses organised crime, paedophilia and other serious crimes, e.g. murder, arson, extortion.*

Activities
Intelligence Investigations Surveillance

Disposal authorisation	Record class and retention period	Justifying the retention period
1860	***Telecommunications interception material – received*** Material received from other agencies as a result of the use of telecommunications intercept powers as part of a major crime investigation. Once no longer required, where possible, contact originating agency to request whether disposal may occur, then dispose. **Retention period & trigger** Until no longer required for a permitted purpose under the *Telecommunications (Interception and Access) Act 1979.*	**Detailed justification not required, as only minor changes made to this class:** • description title changed from Telephone interception material – received • act reference in retention period & trigger amended • retention period & trigger changed from 'Until no longer required for a permitted purpose under the *Telecommunications (Interception) Act 1979*'. **Regulatory requirements:** *Telecommunications (Interception and Access) Act 1979* – s.79(1)(b); s.79(2); para.7(2)(aaa) **Business requirements:** CCC changed the retention period & trigger to include 'Once no longer required, where possible, contact originating agency to request whether disposal may occur, then dispose'. The change was made because: For a long time, when CCC no longer need the intercept material, they extend the courtesy of contacting the originating agency before destroying intercept material. The CCC write to the agency asking whether they can destroy or if they would prefer the return of the material. This practice stems from the time when they only dealt with material obtained externally (that is prior to the CCC being granted interception powers). The recommended additional statement is included to be consistent with the CCC's practices.

Disposal authorisation	Record class and retention period	Justifying the retention period
	Once no longer required, where possible, contact originating agency to request whether disposal may occur, then dispose.	
1861	***Telecommunications interception material – directly obtained by the CCC*** Material lawfully intercepted by the CCC pursuant to warrant under the *Telecommunications (Interception and Access) Act 1979*. Includes restricted records and stored communications received from carriers. **Retention period & trigger** Until no longer required for a permitted purpose under the *Telecommunications (Interception and Access) Act 1979*.	**Changes to this record class:** • this is a new class in version 2 • 1861 in version 1 is now 1862 in version 2. **Regulatory requirements:** Commonwealth *Telecommunications (Interception and Access) Act 1979*: • s.9(1A) – interception of telecommunication service includes communications as stored communications • s.39 – an agency may apply for a warrant in respect of a telecommunication service or person • s.79(1)(b) – when the chief officer of the agency is satisfied that a restricted record is not likely to be required for a permitted purpose in relation to the agency, the chief officer shall cause the restricted record to be destroyed forthwith • s.79(2) – a restricted record must not be destroyed unless the agency has received from the Secretary of the Department written notice that the entry in the general register relating to the warrant under which the record was obtained has been inspected by the Minister However, s79 does not apply where a communication was intercepted under para.7(2)(aaa). Paragraph 7(2)(aaa) covers interception of a communication as part of network protection duties and it is reasonable to intercept the communication in order to perform those duties • s.110 – allows criminal law enforcement agencies to apply for a warrant to access communications stored by a carrier • s.139 – allows law enforcement agencies to issue a preservation certificate to hold communications for investigations • s.150(1)(b) – requires information or records not required for investigative purposes to be destroyed 'forthwith'

Disposal authorisation	Record class and retention period	Justifying the retention period
		• s.150(2) – requires law enforcement agencies to notify their Minister of which records have been destroyed. They must make a report 3 months after each 30 June. Queensland *Telecommunications Interception Act 2009* s.19 sets out requirements for destruction of restricted records. **Business requirements:** The inclusion of this record class is a result of amendments to the Commonwealth *Telecommunications Interception Act 1979* that granted the CCC interception powers. Under s.79 of the TIA Act, a restricted record held by a law enforcement agency must be destroyed once the record is not likely to be required for a permitted purpose in relation to that law enforcement agency. A restricted record has a very specific definition under the TIA Act – it means 'a record other than a copy that was obtained by means of an interception... of a communication passing over a telecommunications system'. This does not include copies of recordings, documents, and the like. The CCC's specific requirements in relation to retention and destruction of material is contained in s.19 of the *Telecommunications Interception Act 2009* (Qld) (TI Act Qld). This provision largely mirrors that of s.79 in the TIA Act. Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes. **Comparison with other schedules' retention period:** *National Archives of Australia – Records Authority – Australian Federal Police 2006/00446344* Reference 14419 Recordings of technical intercepts and both master product and copies made and disseminated. Includes records describing access to recordings (session lists) its dissemination and product resulting from listening devices – Destroy when no longer required for permitted purpose and after the completion of statutory inspection requirements (where relevant) has been notified to the agency. Note: At the date of issue, a mandatory destruction requirement applies to certain records in this class under the *Telecommunications (Interception and Access) Act 1979*. *National Archives of Australia – Records Authority – Australian Crime Commission 2012/00086171* Reference 61207 Master set of electronic intelligence product recorded as part of technical surveillance activities supporting an intelligence operation – Destroy in accordance with directions from the agency's Chief Executive Officer.

Disposal authorisation	Record class and retention period	Justifying the retention period
1862	***Telecommunications interception material – internal management*** Records relating to the receipt, copying and disposal of telecommunications interception material as part of a major crime investigation. Excludes restricted records and stored communications received from carriers. **Retention period & trigger** Permanent by the agency.	**Changes to this record class:** • description title changed from Telephone interception material – internal management • previously reference 1861 in version 1 • retention period & trigger changed from '7 years after last action'. **Background/business process:** Amendments to the *Telecommunications (Interception and Access) Act 1979* mean the CCC has the power to intercept telecommunications. The CCC must keep documents connected with the issue of warrants to intercept telecommunications and records associated with the interceptions. **Regulatory requirements:** *Telecommunications Interception Act 2009* (Qld) – s.14, 15(1) sets out documents that must be retained **Business requirements:** This record class includes the warrant application, particulars of the warrant and times of interception, particulars relating to the use, communication, and giving of evidence of telecommunications interception material. This record class excludes the original restricted record covered by 1860 that must be destroyed once the permitted purpose for which it was originally obtained no longer exists.[2] At the meeting with QSA on 17 May 2016, the CCC advised that the Parliamentary Commission had interpreted the legislation's silent on retention to mean a permanent retention was required. QSA advised that these records would hold no permanent archival value to the state of Queensland, and so they should be held permanently by the agency. **Comparison with other schedules' retention period:** *National Archives of Australia – Records Authority – Australian Federal Police 2006/00446344* Reference 14419 Recordings of technical intercepts and both master product and copies made and disseminated. Includes records describing access to recordings (session lists) its dissemination and product resulting from listening devices – Destroy when no longer required for permitted purpose and after the completion of statutory inspection requirements (where relevant) has been notified to the agency. Note: At the date of issue, a mandatory destruction requirement

[2] The CCC advised their inspecting entity (the Parliamentary Crime and Corruption Commissioner) made this interpretation of section 19 of the TIA.

Disposal authorisation	Record class and retention period	Justifying the retention period
		applies to certain records in this class under the *Telecommunications (Interception and Access) Act 1979*. *National Archives of Australia – Records Authority – Australian Crime Commission 2012/00086171* Reference 61207 Master set of electronic intelligence product recorded as part of technical surveillance activities supporting an intelligence operation – Destroy in accordance with directions from the agency's Chief Executive Officer.
1865	***Major crime investigations – child exploitation material*** Records that in a way are likely to cause offence to a reasonable adult, which describe or depict a person, or a representation of a person who is, or apparently is, a child under 16 years: • in a sexual context including for example engaging in sexual activity • an offensive or demeaning context • being subjected to abuse, cruelty or torture. Child exploitation material may include some or all of the following: images, audio and visual media, transcribed conversations or chat room conversations. **Retention period & trigger** Until no longer required for operational, investigative, or legal purposes, then destroy.	**Changes to this record class:** • this is a new class in version 2. **Background/business process:** Material as per the records description, which are obtained during the course of an investigation. **Regulatory requirements:** Class included to allow for destruction when no longer required or authorised under s.228H of the *Criminal Code Act 1899* (Qld). **Business requirements:** Due to the nature of the material – and the potential stress factors involved in sighting the material – as well as provisions under the *Criminal Code Act 1899* (Qld), this material should not be kept longer than it is required to achieve an outcome from a court proceeding (which could include an appeal) and it is established that the original material is no longer required for other operational, investigative or legal purposes. With regards to child exploitation material and briefs of evidence, evidence packages are created and burnt to disk, which are encrypted (password protected). The disk stays with the original brief of evidence and a CCC copy of the brief is retained by investigators. Following the completion of the court case, the original brief is usually returned to the arresting officer at some later stage and then is secured in a locked cupboard until a decision is made on how best to store or destroy the evidence. In addition to removing any possible conflict with Code offence provisions, this class will also permit secure retention of some child exploitation material on-site at the CCC to augment the existing reference library of images, which are used for categorisation and investigative purposes. Possessing and distributing child exploitation material is a crime unless it is for a permitted purpose such as a controlled activity/investigation and prosecution/categorisation. The material should never be retained longer as this would potentially be a crime. There is nothing stating how long that it

Disposal authorisation	Record class and retention period	Justifying the retention period
		needs to be kept. It is illegal to keep it unless you are a law enforcement officer acting in the course of your duties or an officer engaged in a controlled activity and only for the purpose of the controlled activity. It is implied in the act that it should be destroyed as soon as practicable after the permitted purpose has finished. **Comparison with other schedules' retention period:** No comparisons. **Other comments/factors for consideration:** Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes.
1870	***Forensic image – binary image – forensic copy*** Similar to a 'copy' or 'duplicate'. It is a forensically sound binary image depicting each '1' and '0' stored on the respective hard drive, USB storage device, or other storage media. It also includes a forensic copy of specific folders and files. It provides a means of examining an item or exhibit using the 'copy' instead of the original source. These copies can later be digitally verified to prove no changes were made from time of acquisition. Note: Copies of specific images are held on the relevant investigations files. **Retention period & trigger**	**Changes to this record class:** • this is a new class in version 2. **Background/business process:** Similar to a 'copy' or 'duplicate', a forensically sound binary image depicts each '1' and '0' stored on the respective hard drive, USB storage device, or other storage media, which has been seized for an investigation. It also includes a forensic copy of specific folders and files on the devices. It provides a means of examining an item or exhibit using the 'copy' instead of the original source. These copies can later be digitally verified to prove no changes were made from time of acquisition. **Business requirements:** Extracts from original material may be used to form briefs of evidence used in court proceedings. Once there is an outcome from these proceedings (which could include an appeal) and it is established that the original material is no longer required for other operational, investigative or legal purposes then the material can be disposed of. It could be argued that there is no need to retain the complete binary image (which contains information not relevant to the investigation and possible other private information) unless there is a need to retain the binary image for as long as the brief of evidence to show the relationship between the snippet and the original images for continuity of evidence purposes. A complete binary image would be retained to ensure the CCC cannot be challenged about the authenticity of their extraction process and to be able to go back to the original throughout a legal case or investigation. It is important to note that the nature of the material may cause stress when viewed, which is another reason for disposal after its use has ceased. **Other comments/factors for consideration:**

Disposal authorisation	Record class and retention period	Justifying the retention period
	Until no longer required for operational, investigative, or legal purposes, then destroy.	Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes.
1874 and 1875	***Surveillance – investigations and intelligence captured under a warrant*** Records relating to surveillance for intelligence and/or investigations captured under a warrant. This includes surveillance logs and running sheets, transcripts, videos and photographs (master negative or digital image). **Retention period & trigger** Until investigations and legal action, including appeal period is complete, then destroy. ***Surveillance – investigations and intelligence not captured under a warrant*** Records relating to surveillance for intelligence and/or investigations not captured under a warrant. This includes surveillance logs and running sheets, transcripts, videos and photographs (master negative or digital image).	**Changes to this record class:** • these two record classes replace record classes 1874, 1875 and 1876 in version 1. • these new classes permit destruction surveillance material used in investigations. • the change meets the requirements of the Commonwealth *Surveillance Devices Act 2004.* **Background/business process:** These record classes cover material relating to surveillance for intelligence and/or investigation purposes taken under a warrant and not taken under a warrant. Types of material include audio, video, logs, transcripts and running sheets of activities. The *Public Records Act 2002* does not apply to records relating to surveillance devices per s.120 of the *Crime and Corruption Act 2001*. Separate legislative requirements in Acts, such as the *Crime and Corruption Act 2001*, *Police Powers Responsibilities Act 2000* and the Commonwealth *Surveillance Devices Act 2004,* govern destruction obligations where surveillance material is gathered under a warrant. **Business requirements:** The retention period and trigger for record class 1874 for surveillance product captured under a warrant meets the requirements of s. 46 of the Commonwealth *Surveillance Devices Act 2004* and s.131 of the Queensland *Crime and Corruption Act 2001,* which mandates destruction of warrant surveillance product. Extracts from original material may be used to form briefs of evidence used in court proceedings. Once there is an outcome from these proceedings, which could include an appeal, and it is established that the original material is no longer required for other operational, investigative or legal purposes, it is no longer required and can be disposed of. Record class 1875 relates to surveillance material not taken under a warrant. This is usually material taken from a public place in connection with an investigation. Raw material is taken from the recorder and placed on our network. This raw material is taken to mean the surveillance material record. A small snippet may be used as part of the investigation. The raw material may be 10 days of 24-hour surveillance of an empty street. Given that there is a requirement to destroy all

Disposal authorisation	Record class and retention period	Justifying the retention period
	Note: Copies of specific images are held on the relevant investigation files. **Retention period & trigger** Until no longer required for operational, investigative, or legal purposes, then destroy.	material taken under a warrant as soon as it is no longer required, it makes no sense to treat the material taken outside a warrant differently. There is no business value in keeping this material post investigation and legal proceedings. Material relevant to the investigation will be featured on the brief of evidence, which takes the retention period of the investigation classes. **Comparison with other schedules' retention period:** *National Archives of Australia – Records Authority – Australian Crime Commission 2012/00086171* Reference 61207 Master set of electronic intelligence product recorded as part of technical surveillance activities supporting an intelligence operation – Destroy in accordance with directions from the agency's Chief Executive Officer. **Other comments/factors for consideration:** Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes. Additional clarification regarding the retention of surveillance material used during investigations and subsequent court proceedings[3] was sought to confirm retention period and trigger for these two record classes.[4]

[3] See Email from Jen O'Farrell, Executive Director, Strategy and Corporate Services, CCC QSA RM8 reference 16/31600.
[4] The implications of the discussions with CCC mean QSA will need to follow up on surveillance record classes in other schedules.

Function	Scope note
CORRUPTION	*The function of dealing with serious cases of corrupt conduct in the public sector or in the Queensland Police Service (QPS). Corrupt conduct means conduct of a person, regardless of whether the person holds or held an appointment, that:* *(a) adversely affects, or could adversely affect, directly or indirectly, the performance of functions or the exercise of powers of:* *(i) a unit of public administration* *(ii) a person holding an appointment* *(b) results, or could result, directly or indirectly, in the performance of functions or the exercise of powers mentioned in paragraph (a) in a way that:* *(i) is not honest or is not impartial* *(ii) involves a breach of the trust placed in a person holding an appointment, either knowingly or recklessly* *(iii) involves a misuse of information or material acquired in or in connection with the performance of functions or the exercise of powers of a person holding an appointment* *(c) is engaged in for the purpose of providing a benefit to the person or another person or causing a detriment to another person* *(d) would, if proved, be:* *(i) a criminal offence* *(ii) a disciplinary breach providing reasonable grounds for terminating the person's services, if the person is or were the holder of an appointment.*

Changes to this function:

Function 12 title changed from: Misconduct & Integrity.

Scope note changed from: The function of dealing with serious cases of official misconduct in the public sector or police misconduct in the Queensland Police Service (QPS). 'Official or Police Misconduct' is any serious misconduct relating to the performance of an officer's duties that is dishonest or lacks impartiality, or involves a breach of trust, or is a misuse of officially obtained information. The conduct must be serious enough to be a criminal offence or to justify dismissal.

Activities
Intelligence Surveillance

Disposal authorisation	Record class and retention period	Justifying the retention period
1931	***Telecommunications interception material – received*** Material received from other agencies as a result of the use of telecommunications intercept powers as part of a corrupt conduct investigation. **Retention period & trigger** Until no longer required for a permitted purpose under the *Telecommunications (Interception and Access) Act 1979*. Once no longer required, where possible, contact originating agency to request whether disposal may occur, then dispose.	**Detailed justification not required, as only minor changes made to this class:** • description title changed from Telephone interception material – received • act reference in retention period & trigger amended • retention period & trigger changed from 'Until no longer required for a permitted purpose under the *Telecommunications (Interception) Act 1979*'. **Regulatory requirements:** *Telecommunications (Interception and Access) Act 1979* – s.79(1)(b), 79(2); para.7(2)(aaa) **Business requirements:** CCC changed the retention period and trigger to include 'Once no longer required, where possible, contact originating agency to request whether disposal may occur, then dispose'. The change was made because: For a long time, when CCC no longer need the intercept material, they extend the courtesy of contacting the originating agency before destroying intercept material. The CCC write to the agency asking whether they can destroy or if they would prefer the return of the material. This practice stems from the time when they only dealt with material obtained externally (that is prior to the CCC being granted interception powers). The recommended additional statement is included to be consistent with the CCC's practices.
1932	***Telecommunications interception material – directly obtained by the CCC*** Material lawfully intercepted by the CCC pursuant to warrant under the *Telecommunications (Interception and Access) Act 1979*. Includes stored communications received from carriers. **Retention period & trigger** Until no longer required for a permitted purpose under the *Telecommunications*	**Changes to this record class:** • this is a new class in version 2. **Regulatory requirements:** Commonwealth *Telecommunications (Interception and Access) Act 1979*: • s.9(1A) – interception of telecommunication service includes communications as stored communications • s.39 – an agency may apply for a warrant in respect of a telecommunication service or person • s.79(1)(b) – when the chief officer of the agency is satisfied that a restricted record is not likely to be required for a permitted purpose in relation to the agency, the chief officer shall cause the restricted record to be destroyed forthwith

Disposal authorisation	Record class and retention period	Justifying the retention period
	(Interception and Access) Act 1979.	• s.79(2) – a restricted record must not be destroyed unless the agency has received from the Secretary of the Department written notice that the entry in the general register relating to the warrant under which the record was obtained has been inspected by the Minister However, s.79 does not apply where a communication was intercepted under para.7(2)(aaa). Paragraph 7(2)(aaa) covers interception of a communication as part of network protection duties and it is reasonable to intercept the communication in order to perform those duties. • s.110 allows criminal law enforcement agencies to apply for a warrant to access communications stored by a carrier • s.139 allows law enforcement agencies to issue a preservation certificate to hold communications for investigations • s.150(1)(b) requires information or records not required for investigative purposes to be destroyed 'forthwith' • s.150(2) requires law enforcement agencies to notify their Minister which records have been destroyed. They must make a report 3 months after each 30 June. Queensland *Telecommunications Interception Act 2009* s.19 sets out requirements for destruction of restricted records. **Business requirements:** The inclusion of this record class is a result of amendments to the Commonwealth *Telecommunications Interception Act 1979* that granted the CCC interception powers. Under s.79 of the TIA Act, a restricted record held by a law enforcement agency must be destroyed once the record is not likely to be required for a permitted purpose in relation to that law enforcement agency. A restricted record has a very specific definition under the TIA Act – it means 'a record other than a copy that was obtained by means of an interception... of a communication passing over a telecommunications system'. This does not include copies of recordings, documents, and the like. The CCC's specific requirements in relation to retention and destruction of material is contained in s.19 of the *Telecommunications Interception Act 2009* (Qld) (TI Act Qld). This provision largely mirrors that of s.79 in the TIA Act. Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes. **Comparison with other schedules' retention period:**

Disposal authorisation	Record class and retention period	Justifying the retention period
		National Archives of Australia – Records Authority – Australian Federal Police 2006/00446344 Reference 14419 Recordings of technical intercepts and both master product and copies made and disseminated. Includes records describing access to recordings (session lists) its dissemination and product resulting from listening devices – Destroy when no longer required for permitted purpose and after the completion of statutory inspection requirements (where relevant) has been notified to the agency. Note: At the date of issue, a mandatory destruction requirement applies to certain records in this class under the *Telecommunications (Interception and Access) Act 1979*. *National Archives of Australia – Records Authority – Australian Crime Commission 2012/00086171* Reference 61207 Master set of electronic intelligence product recorded as part of technical surveillance activities supporting an intelligence operation – Destroy in accordance with directions from the agency's Chief Executive Officer.
1933	***Telecommunications interception material – internal management*** Records relating to the receipt, copying and disposal of telecommunications interception material as part of a corrupt conduct investigation. **Retention period & trigger** Permanent by the agency.	**Changes to this record class:** • description title changed from Telephone interception material – internal management • previously reference 1932 in version 1 • retention period & trigger was changed from '7 years after last action'. **Background/business process:** Amendments to *Telecommunications (Interception and Access) Act 1979* mean the CCC has the power to intercept telecommunications. The CCC must keep documents connected with the issue of warrants to intercept telecommunications and records associated with the interceptions. **Regulatory requirements:** *Telecommunications Interception Act 2009* (Qld) – s.14, 15(1) sets out documents that must be retained **Business requirements:** This record class includes the warrant application, particulars of the warrant and times of interception, particulars relating to the use, communication, and giving of evidence of telecommunications interception material. This record class excludes the original restricted record covered by 1932 that must be destroyed once the permitted purpose for which it was original obtained no longer exists.[5]

[5] The CCC advised their inspecting entity (the Parliamentary Crime and Corruption Commissioner) made this interpretation of section 19 of the TIA.

Disposal authorisation	Record class and retention period	Justifying the retention period
		At the meeting with QSA on 17 May 2016, the CCC advised that the Parliamentary Commission had interpreted the legislation's silent on retention to mean a permanent retention was required. QSA advised that these records would hold no permanent archival value to the state of Queensland so they should be held permanently by the agency. **Comparison with other schedules' retention period:** *National Archives of Australia – Records Authority – Australian Federal Police 2006/00446344* Reference 14419 Recordings of technical intercepts and both master product and copies made and disseminated. Includes records describing access to recordings (session lists) its dissemination and product resulting from listening devices – Destroy when no longer required for permitted purpose and after the completion of statutory inspection requirements (where relevant) has been notified to the agency. Note: At the date of issue, a mandatory destruction requirement applies to certain records in this class under the *Telecommunications (Interception and Access) Act 1979*. *National Archives of Australia – Records Authority – Australian Crime Commission 2012/00086171* Reference 61207 Master set of electronic intelligence product recorded as part of technical surveillance activities supporting an intelligence operation – Destroy in accordance with directions from the agency's Chief Executive Officer.
1951 and 1952	***Surveillance – investigations and intelligence captured under a warrant*** Records relating to surveillance for intelligence and/or investigations captured under a warrant. This includes surveillance logs and running sheets, transcripts, videos and photographs (master negative or digital image). **Retention period & trigger** Until investigations and legal action, including appeal period is complete, then destroy.	**Changes to this record class:** • these two record classes replace record classes 1951, 1952 and 1953 in version 1. • these new classes permit destruction surveillance material used in investigations. • the change meets the requirements of the Commonwealth *Surveillance Devices Act 2004.* **Background/business process:** These record classes cover material relating to surveillance for intelligence and/or investigation purposes taken under a warrant and not taken under a warrant. Types of material include audio, video, logs, transcripts and running sheets of activities. The *Public Records Act 2002* does not apply to records relating to surveillance devices per s.120 of the *Crime and Corruption Act 2001*. Separate legislative requirements in Acts, such as the *Crime and Corruption Act 2001*, *Police Powers Responsibilities Act 2000* and the Commonwealth *Surveillance Devices Act 2004,* govern destruction obligations where surveillance material is gathered under a warrant. **Business requirements:**

Disposal authorisation	Record class and retention period	Justifying the retention period
	Surveillance – investigations and intelligence not captured under a warrant Records relating to surveillance for intelligence and/or investigations not captured under a warrant. This includes surveillance logs and running sheets, transcripts, videos and photographs (master negative or digital image). Note: Copies of specific images are held on the relevant Investigation files. **Retention period & trigger** Until no longer required for operational, investigative, or legal purposes, then destroy.	The retention period and trigger for record class 1951 for surveillance product captured under a warrant meets the requirements of s. 46 of the Commonwealth *Surveillance Devices Act 2004* and s.131 of the Queensland *Crime and Corruption Act 2001,* which mandates destruction of warrant surveillance product. Extracts from original material may be used to form briefs of evidence used in court proceedings. Once there is an outcome from these proceedings, which could include an appeal, and it is established that the original material is no longer required for other operational, investigative or legal purposes, it is no longer required and can be disposed of. Record class 1952 relates to surveillance material not taken under a warrant. This is usually material taken from a public place in connection with an investigation. Raw material is taken from the recorder and placed on our network. This raw material is taken to mean the surveillance material record. A small snippet may be used as part of the investigation. The raw material may be 10 days of 24-hour surveillance of an empty street. Given that there is a requirement to destroy all material taken under a warrant as soon as it is no longer required, it makes no sense to treat the material taken outside a warrant differently. There is no business value in keeping this material post investigation and legal proceedings. Material relevant to the investigation will be featured on the brief of evidence, which takes the retention period of the investigation classes. **Comparison with other schedules' retention period:** *National Archives of Australia – Records Authority – Australian Crime Commission 2012/00086171* Reference 61207 Master set of electronic intelligence product recorded as part of technical surveillance activities supporting an intelligence operation – Destroy in accordance with directions from the agency's Chief Executive Officer. **Other comments/factors for consideration:** Changes to the schedule were sent to all senior managers within the agency for review after Legal Services review and input. There was agreement to the proposed changes. Additional clarification regarding the retention of surveillance material used during investigations and subsequent court proceedings[6] was sought to confirm retention period and trigger for these two record classes.[7]

[6] See Email from Jen O'Farrell, Executive Director, Strategy and Corporate Services, CCC QSA RM8 reference 16/31600.
[7] The implications of the discussions with CCC mean QSA will need to follow up on surveillance record classes in other schedules.

Disposal authorisation	Record class and retention period	Justifying the retention period
1954	***Technical applications*** Records relating to applications for the use of technical devices, covert operatives and associated surveillance and support teams for corrupt conduct investigations. **Retention period & trigger** 10 years after business action completed.	**Changes to this record class:** • previously class 12.13.5 in version 1 • retention period & trigger changed from '15 years after last action'. **Business requirements:** The retention periods relating to surveillance material are not based on whether they relate to corruption or crime. The retention period for those types of records should be retained until no longer required for operational, investigative or legal purposes, then destroy. In version 1, the Technical Applications classes took the retention of minor investigations which is 10 years for crime and 15 years for corruption as it was deemed appropriate that all related records be kept for the same amount of time. Given that surveillance will no longer be dependent on the investigation type, it would make sense to be consistent with the major crimes technical surveillance applications (reference 1876) that has a disposal of 10 years after last action.

Other minor changes not affecting retention, which include updates to legislation not administered by the agency (e.g. taxation legislation), moving of classes due to insertion or removal of others and title changes.

Class and description in version 1	Change in version 2
1761 Taxation Applications	Change to Act reference in records description
1805 Document Production Registers	Title changed to Security Classified Information Registers (no change to records description)
1826 Taxation Applications	Change to Act reference in records description
1831 Covert Company Establishment	Change to Act name in records description
1857 Raw Call Charge Record (CCR) data	Change to Act reference in records description
1878 Taxation Applications	Change to Act reference in records description
1886 Covert Company Establishment	Change to Act names in records description
1946 MAC Daily List	Committee name in records description changed
1964 Covert Company Establishment	Change to Act name in records description