INFORMATION AND SECURITY 3

3 INFORMATION AND SECURITY

The events of 7 February 2009 are part of Victoria's history. The work of the Commission forms part of that history and will be of political, policy, social, community and legal significance long after the Commission has concluded. The archival and historical legacy extends beyond the Commission's reports and hearings to the record of those individuals and communities affected by the fires. In particular, the documentation of the community consultations, the public submissions, and the lay witness statements provide a unique insight.

The Commission took seriously its statutory and moral obligations from an archival and historical perspective. It also attached high importance to its duty to those who engaged with it to respect their contributions, privacy and the requirements of due process.

In practical terms, the Commission needed efficient and secure information systems to manage the large volumes of materials it produced and received, as well as a safe and secure physical environment in which to work. Consequently, the Commission made a major investment in a stand-alone information technology network and secure systems and facilities and from the outset planned for the archiving of its records.

3.1 INFORMATION

The Commission handled an extremely large number of records, many of them sensitive or confidential. It was crucial that efficient systems be developed early and maintained properly so that the Commission could organise the material sensibly to maximise effective use of it, use the material during the hearings and the report preparation process, and archive the material at the end of the Commission.

The Commission decided to be an electronic Commission to the greatest extent possible, the grounds for this being a desire for practical efficiency and broad accessibility.

3.1.1 RECORDS MANAGEMENT

Early in its existence the Commission developed a business classification scheme to provide an organisational framework for all Commission information. This helped with daily management of access to materials, as well as with security. It also helped to identify records to be transferred to the state archives held by the Public Record Office Victoria at the conclusion of the Commission.

The scheme was based on the Commission's core functions, rather than on work groups or organisational structure, and it supported collaboration and information sharing throughout the organisation. Initially implemented on the shared file server, the scheme was later transferred to the document management system that was introduced in August 2009 as part of a general desktop software upgrade. The document management system was used for storing and managing all internally generated documents. Within it, documents were generally available to all sections of the Commission. Access was restricted if there was a business need or material had a higher security classification.

Staff were able to gain access to documents from within desktop applications and from a web-based portal that also served as the Commission's intranet, providing organisational and other useful information.

While the Commission was in operation it was not subject to the Victorian *Freedom of Information Act 1982*, but records will be subject to the Act once the Commission ceases operations and the records are transferred to the custody of a successor agency. In recognition of this, the Commission established records management systems that would not only facilitate its operations but also support a successor agency in readily meeting its *Freedom of Information Act 1982* obligations.

3.1.2 INFORMATION MANAGEMENT SYSTEMS AND SERVICES

From the outset it was clear that information management systems and services would be an integral part of the Commission's work. They needed to be user friendly, sturdy and able to facilitate the rapid processing of documents generated in the Commission or provided to the Commission by other parties and the public. They also needed to cater for desktop access to information within the Commission and the hearing rooms, for parties' access to exhibited material, and for archiving at the end of the Commission. All this needed to be done with due regard for document security.

3.1.3 CASE MANAGEMENT SERVICES

As noted in Chapter 2, document management for the directions hearings and the Commission's first three weeks was provided by Corrs using the Ringtail™ system. For the transition from Corrs to the Commission's systems, an implementation plan was mapped out to integrate the required IT hardware and information management systems and services provided by e.law.

e.law had five weeks from the time of its appointment to be ready to provide full court operator, document management and transcription services. Achieving this was not easy: among other things, the required hardware could not be delivered by the original supplier, and an alternative supplier had to be found at short notice.

In addition, the initial system for saving internally generated documents was established on a shared file server rather than the designated document management system. This made it harder to track and locate documents. It also made it difficult to change individuals' practices so that they could work within the Commission's records and document management policy. In time these difficulties were resolved.

The main features of the information management systems and services e.law provided are described in the following sections.

CaseVantage

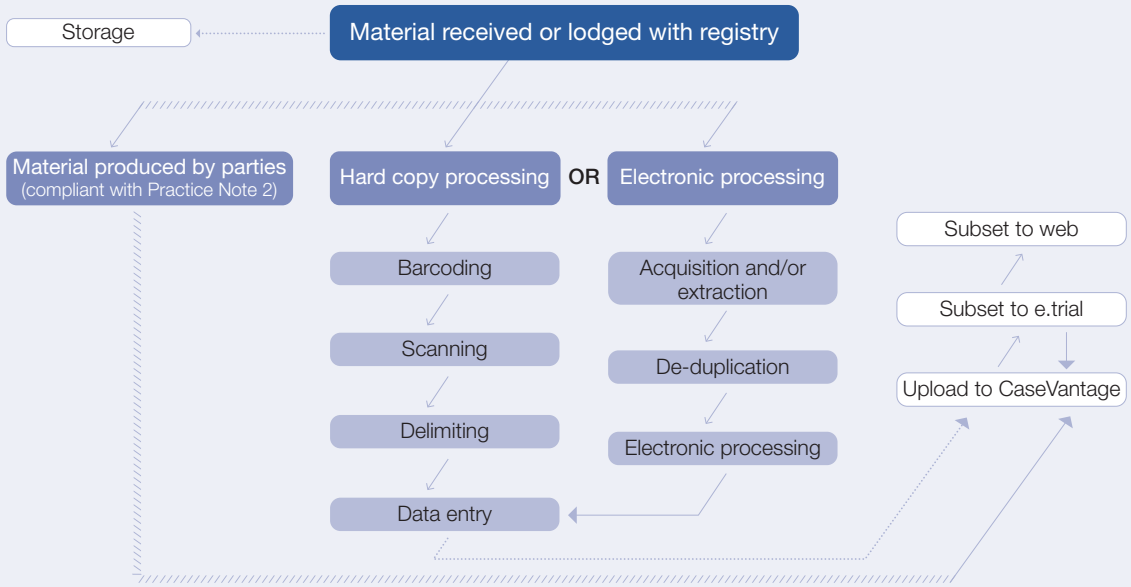
CaseVantage is a specialised case management system that allows large volumes of documents to be managed efficiently. All hard-copy documents received by the Commission were bar-coded, scanned, objectively coded, and loaded into CaseVantage's searchable database. The Commission also received from most parties material that had already been digitised, and this too was loaded into CaseVantage.

e.law customised CaseVantage with specific fields, allowing information to be categorised to reflect the Commission's needs. The system was used to search, identify and analyse material created and received and to build up the documents required to support the investigative work and the hearings.

On 2 June 2009 the Commission issued Practice Note 2, 'Producing material to the 2009 Victorian Bushfires Royal Commission under summons or by way of a submission', which detailed the standards and practices parties were expected to adopt in order to facilitate speedy exchange of electronic records between the Commission and the parties.

Figure 3.1 shows the flow of material through the Commission's document management system.

Figure 3.1 Document management flow



Source: e.law Asia Pacific.

e.trial

e.trial is e.law's exhibit and evidence management system used for presenting documents in a hearing room. Documents held in CaseVantage that were scheduled to be tendered during the course of hearings were progressively uploaded to e.trial. This allowed the Commission and the parties in the hearing room to have immediate access to exhibited material.

Exhibited information could also be made securely available to parties, remotely and immediately. Because of the restrictions on some parties' leave to appear, e.law developed a methodology whereby individual documents could be served selectively, thus restricting them to those parties with leave to appear for the relevant term of reference. The Commission also used e.trial to serve on the relevant parties notice of documents that would be used in hearings. This allowed for the timely delivery of large volumes of material, which was essential to support the hearings.

The Commission provided at least one licence to use e.trial to each party and more for larger parties. A variation to the original e.law contract was signed to allow e.law to provide additional licences to those parties that required more licences at the parties' own cost, which was a set price per licence.

3.1.4 IT STRUCTURE AND DESIGN

The Commission met its IT needs by calling on a variety of hardware and software vendors. The Commission's IT provider, DiData, designed and built the network and provided ongoing maintenance and desktop support services. (Appendix I shows the Commission's IT architecture in diagrammatic form.) Server virtualisation technology was used extensively. This minimised the number of physical devices required and provided disaster recovery options—which were ultimately used.

The standard operating environment found on each desktop computer and laptop was locked down in accordance with the Commission's security requirements to reduce the risk of exploitation and ensure the protection of sensitive material. The standard operating environment also meant that if problems occurred with a workstation, the workstation could be quickly rebuilt without affecting the overall network. Each laptop had full device encryption deployed.

To reduce the chance of losing sensitive data, workstations were protected by antivirus software. One of the prime areas for potential loss of sensitive material and security compromise was the email system: several different controls were implemented to minimise the risk of exposure, and all email received from the internet was scanned for viruses and malware.

All internet traffic was also scanned for malware and viruses using a forward proxy solution, which put an interface between the workstations and the internet for extra security. This device also enforced internet content controls that limited the use of categories of internet content known to pose high risks of corruption, such as webmail, to further limit the Commission's vulnerability to loss of sensitive data.

A system-wide back-up occurred nightly and copies of the back-up tapes were stored in a secure facility off site to minimise the risk of data loss and provide recovery if required.

As a result of these measures, the Commission had secure and reliable infrastructure with sufficient redundant capacity to cope with the volume of data and to protect the network if damage occurred. The resilient architecture, technical ability, and on-call 24-hour support allowed for the operation of services without concern about the underlying IT infrastructure.

Box 3.1 Flooding

The importance of business continuity planning was demonstrated twice with the IT systems.

The Commission experienced not one but two floods. The first, in June 2009, was caused by a leaking hot water dispenser on level 14 of 222 Exhibition Street. Fortunately, the flood caused only minor damage, and the systems were rebooted with minimal down time.

The second flood was more serious. On Saturday 21 November 2009 a water pipe burst on level 14, causing major flooding to the building. The majority of the Commission's core ICT infrastructure and fit-out on the northern side of the building was damaged as a result. The flooding particularly affected the communications room, which was a secure climate-controlled area housing a large volume of sensitive equipment with very restricted access. The flooding also affected the hearing rooms and communications rooms on Level 11.

A major effort and impressive technical ability on the part of DiData rectified the situation. The majority of services were available the next morning, before the week's hearings began, thus causing few problems other than wet carpet in the hearing rooms and allowing the scheduled hearings to proceed without interruption. Ninety-five per cent of all affected services were restored within 24 hours. The damaged hardware was replaced over several months, the associated outages being planned to minimise interruptions to the Commission's work.

Had it not been for sound continuity planning, quick action, and access to extensive technical expertise, combined with use of server virtualisation technology and the resilient nature of the Commission's ICT systems, the flood could have caused severe and potentially crippling disruption.

3.1.5 ARCHIVING

It was evident from the outset that the Commission's records would be an important part of the public and historical record of the State. This is true not only for its publicly accessible records, such as reports, exhibits and transcripts, but also for the records of the Commission's internal processes and inquiry.

In recognition of this and the archiving obligations imposed by statute, the Commission began planning for the archiving of its records in early March 2009, with the secondment of a staff member from the Public Record Office Victoria. As a 'start-up' organisation, the Commission had a unique opportunity to build archival provisions into the design and implementation of its systems, policies and practices. Above all, it was vital to ensure that no important records were 'lost', particularly in view of the Commission's commitment to openness and transparency.

Every record created or received by Commission personnel in the course of Commission business is a public record and must be managed in accordance with the requirements of the State's *Public Records Act 1973*. Under the Act, the Keeper of Public Records issues standards for the management of public records, including retention and disposal requirements. In broad terms, records identified as permanent will be transferred to the Public Record Office Victoria, and temporary records (notably administrative records related to finance, contracts and personnel) will either be transferred to the Department of Premier and Cabinet (as successor agency) or be destroyed. As provided under the Act, certain permanent records will be closed to public access for designated periods. For example, records of the inquiry into the fire-related deaths will be closed for up 99 years to protect the privacy of those who perished and their surviving family. Once the closures are confirmed, PROV will maintain and manage the closures for the appropriate periods.

The information management systems and services contract with e.law specified that the transfer of Commission records to PROV must be in accordance with the Standard for the Management of Electronic Records (PROS99/007), also known as the Victorian Electronic Records Strategy (VERS), published by PROV.

VERS compliance was built into the document management system by the inclusion of additional PROV-certified software (RecordPoint) that converts the metadata of a document into a form consistent with VERS for long-term preservation. The Commission furthered this by issuing Practice Note 2, which provided that the Commission and parties would produce material in relevant long-term preservation format file types.

From mid-2009 the Commission worked with PROV on retention and transfer requirements. In the first half of 2010 tests were conducted to ensure that Commission systems could produce records compliant with PROV standards. As the Commission winds down all permanent records will be transferred to PROV. It is expected this transfer will be largely digital, in compliance with the Public Records Act. The Commission will be the first organisation to effect a large-scale transfer to PROV in compliance with VERS.

3.2 SECURITY

Security—of people and documents—was a priority. During the Commission data were collected from the general public, state governments, the Commonwealth Government, private organisations, and people directly affected by the fires. The data ranged from information in the public domain to classified and protected material, including material subject to public interest immunity and legal professional privilege claims, as well as a considerable amount of sensitive personal information. A strong yet flexible security environment was essential.

The Commission's independent security analyst made an initial risk assessment and helped with the development of the Commission's security policy. This policy applied to all personnel working at the Commission, including contractors, and covered the following:

- building access
- hearing room security
- systems and facilities for managing and storing Commission documents and information
- information and communication technologies.

3.2.1 BUILDING ACCESS

The Commission's offices on level 12 were fully secured. Access was possible only by using a swipe card, to reach both the floor and then the offices. The hearing rooms on level 11 were on a partially secure floor: public access was permitted in the entry area and the hearing rooms (when they were open), but members of the public were not permitted to enter secure areas without being escorted by security-cleared staff. Swipe card access was used for entry into secure areas. Some areas, such as the data centre room, had highly restricted access limited to essential personnel only.

3.2.2 HEARING ROOM SECURITY

In Victoria, royal commissions are prescribed as courts under the Court Security Regulations 2004. This meant the Commission had all the powers available to a court under the State's *Court Security Act 1980* with respect to search and seizure powers. This was important for ensuring that the Commission exercised a duty of care to all who participated in the hearings.

Under this authority the CEO of the Commission entered into an agreement for the provision of security services and appointed authorised officers who were empowered to search people and confiscate prohibited items as a condition of entry to the Commission. G4S Custodial Services Pty Ltd was engaged to provide security services for the hearing rooms, including X-ray scanning, front-of-house security, daily opening and closing of hearing rooms and the public access areas during hearings, acting as floor wardens in case of emergency, and regular testing of the emergency response alarms.

The CEO signed an instrument of delegation for each G4S security officer that allowed them to confiscate and receipt prohibited items identified during the scanning process. G4S staff worked closely with the building security provider, ISS Facility Services, which was the first responder to all incidents and was at all times in radio contact with G4S officers.

There were no major security problems or breaches during the hearings.

3.2.3 INFORMATION AND RECORDS

The Commission complied with the Information Privacy Principles as set out in the Victorian *Information Privacy Act 2000*. A privacy statement was available on the Commission's website, and at all times the Commission was explicit in its reasons for collecting personal information. Private and personal information was gathered solely for the purpose of conducting Commission business.

The Commission decided to adopt the Commonwealth Government *Protective Security Manual* as the basis for classification and protection of sensitive records. This approach ensured that Commission information was managed in accordance with its sensitivity. The Commission assessed the risks associated with inappropriate access to its information by unauthorised persons, and in mid-2009 implemented a 'Protected level' security environment for its information management. The security classifications and definitions used in the Commission were established to protect information, compromise of which could cause damage to the Commission, the parties, the ongoing investigations of Victoria Police, commercial entities or members of the public.

Most documents were classified as commission-in-confidence because they were internal documents related to the Commission's operations and inquiry, and any compromise of them could potentially damage the Commission's interests. Some materials did attract the highest protection. As an example, information gathered as part of the inquiries into the fire-related deaths inquiry was given the highest security classification, Protected. The aggregated personal information collected in the course of these inquiries was of such a personal nature that its compromise could potentially cause damage and distress to members of the public, particularly the families and friends of the deceased.

All personnel were briefed on their responsibilities in relation to the different categories of secure materials. Access rights were controlled and regularly reviewed to ensure that they remained appropriate.

As noted, parties' access to relevant Commission information was managed and controlled through e.trial, with access limited to the terms of each party's leave to appear.

Even in a secure environment, it is interactions with the outside world that pose the greatest risk. This was demonstrated in May 2010, when the content of documents made available to parties via e.trial, under standard hearing protocols and not otherwise publicly available at the time, was leaked to the media.

3.2.4 INFORMATION AND COMMUNICATION TECHNOLOGIES

In addition to the *Protective Security Manual*, the Commission adopted the Defence Signals Directorate's *Information and Communications Technology Security Manual* as the basis for its security policy and practice. These two publications represent best practice for physical, personal and technology security in Australia. The Commission designed its systems and processes in accordance with this regime.

The Commission selected information technology equipment from a Defence Signals Directorate security-endorsed product list and, where this was not possible, sought advice on the international common criteria accreditation of the product. Designs were peer validated and tested.

Specific Commission personnel were given remote secure access to the Commission's internal systems through a secure two-step authentication virtual private network solution using routing and remote secure access technology. RSA was accessible only on specific laptops, and access was restricted and monitored in the firewall connection.

A storage area network was located in the level 12 secure data room. It stored all electronic classified material and had inbuilt back-up capacity in case a section of it failed. This ensured correct access and physical security of the data holdings. Servers, particularly those that were connected to the internet, were protected by devices that ensured access to the Commission's systems, and data was provided only to authorised users. The website was hosted by an external provider to minimise exposure of the Commission's network to intrusion. This 'intrusion protection' ensured there were no breaches of the firewalls, and the various back-up mechanisms ensured that the Commission was always able to maintain a functioning system.

All these measures combined to ensure that the Commission had a secure network complying with best-practice standards. This allowed it to meet its obligation of ensuring the security of the data developed and collected as part of its work. It also gave those providing information to the Commission confidence that their information was secure.

Image 3.1 In the County Court hearing room

Source: Courtesy of the *Herald & Weekly Times*.