MANAGEMENT OF FREEDOM OF INFORMATION REQUESTS IN OTHER JURISDICTIONS

for

The Department for Constitutional Affairs

September 2003

Joyce Plotnikoff and Richard Woolfson
Consultants in Management, ICT and the Law
Cheldene
Church Lane
Preston
Hitchin
Herts SG4 7TP
Tel: 01462 457555
Fax: 01462 457229

CONTENTS

ACKNOWLEDGEMENTS

1   INTRODUCTION

1.1   Background to the research

The Freedom of Information Act (FOIA) received Royal Assent in November 2000. On its website, the Lord Chancellor's Department (subsequently the Department for Constitutional Affairs) described the Act as providing:

> 'clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector.
>
> The legislation will apply to a wide range of public authorities, including Parliament, Government Departments and local authorities, health trusts, doctors' surgeries, publicly funded museums and thousands of other organisations.'[1]

In all, the Department estimated that around 88,000 public authorities would be subject to the Act.

The Act is being implemented in stages with full implementation expected by January 2005.[2] The last provisions to be implemented relate to the individual right of access to information held by public authorities.

Under sections 45 and 46 of the FOIA, the Department for Constitutional Affairs provides guidance to public authorities on operating the Act. In connection with that responsibility, the Department commissioned this research. Its purpose was to investigate automated systems used by public bodies in other jurisdictions with similar legislation when responding to requests for information.

1.2   Objectives of the research

The research sought information on manual and electronic systems used in other jurisdictions to manage, monitor and report on applications made under Freedom of Information legislation. It also investigated products already available or under development in the UK.

1.3   Methodology

Information about systems used in other jurisdictions was sought in the following ways:

---

[1] See http://www.lcd.gov.uk/foi/foiact2000.htm
[2] Section 87(3) sets a deadline for full implementation of five years from the date the Act was passed.

- a list of questions aimed at government personnel responsible for their department's response to requests for information was e-mailed to contacts in twelve countries that have already implemented Freedom of Information legislation
- a separate list of questions was e-mailed to 21 software companies which were known to have relevant products or which were thought likely to have such products
- a software demonstration arranged by British Telecom was attended
- an Internet search was conducted relating to systems used in responding to Freedom of Information requests
- interviews were held with four Freedom of Information professionals in the US Department of Justice and two academics with a research interest in Freedom of Information. In addition, a telephone conference was held with two government staff and a software support manager in the US Federal Bureau of Investigation.

We received responses from 17 government departments in eight countries and from seven software companies. E-mailed comments were also received from the Campaign for Freedom of Information.

The lists of questions used in the course of the research are reproduced at Annex A.

2   MANAGING THE RESPONSE TO FREEDOM OF INFORMATION REQUESTS

2.1   Introduction

This chapter analyses the information provided by those responsible for responding to requests made under Freedom of Information (FOI) legislation. It draws also on the comments received from academics and others who submit requests for information.

2.2   Types of automated systems

Respondents distinguished two main types of system used in relation to FOI requests.[3] The first of these offers the ability to track the progress of requests from receipt through to response. The second allows portions of a word-processed document or scanned image of a document to be blanked out (a process known as redaction) and annotated to indicate the exemption under which redacted text has been withheld.

Tracking systems were more common than redaction systems but neither was in universal use, particularly for agencies that received a small volume of requests:

> 'We do not use an automated system to support the processing of FOI requests, as our organisation usually receives no more than four FOI requests a year' *(National Archives of Australia)*

> 'This office is quite small and we only have one part-time officer who processes the approximately 40 valid requests received per year. At the moment, this processing is conducted manually' *(Commonwealth Ombudsman)*

> 'No specialised automated systems are used' *(Australian Securities and Investments Commission)*

> 'We don't have an automated system dedicated to handling FOI requests. Most of our processing is still manual handling' *(Rockdale City Council, New South Wales)*

> 'The State Services Commission does not have an automated system for processing Official Information Act[4] requests' *(New Zealand)*

> 'In principle, requests concerning document access should be registered in an index (diary) at least in cases where the request is in writing and has been sent to an authority. Nowadays the index is in many cases part of a more comprehensive data system. In practice, information on documents can be requested in various ways, for example by telephone, in writing - including e-mail - or by visiting the competent

---

[3] This does not include general electronic records management system used in identifying records responsive to a request.
[4] This is the name of the New Zealand FOI legislation.

authority. When a document is immediately sent after an oral request, the request is not registered' *(Finland).*

For others, automated support was limited to general-purpose information retrieval systems used in identifying records responsive to a request:

> 'The ten Swedish central government departments, the Ministry of Justice being one of them, do not use any automated systems specifically to support the processing of FOI requests … The main automated system to support the processing of FOI requests is that used for the registration of official documents, RK-Dia. There are no other record keeping systems within the ministries'

> 'There are no government bodies or agencies in the Netherlands that use ICT in the process of dealing with FOIA-requests other than the use of databases to retrieve the requested information. But these databases are used for retrieving information in general and not for FOIA requests specifically'

> 'The [only automated system] is the records management system used by Council for storage of all records. i.e. it is not for FOI only' *(City of Sydney, New South Wales).*

Many of those with automated systems designed specifically to deal with FOI requests had developed their applications in-house or were using a system developed by another government department. The sophistication of these systems varied widely. Queensland Health currently uses an old DOS-based system developed by the Department of Justice which has limited functionality and was described as 'unreliable'.[5] New York State has a simple single-user tracking system based on Microsoft Access. New requests are input and the system generates a referral memo. In five days, the program automatically produces an acknowledgment letter to the requester. The system is updated to record the receipt of relevant records. It has no report generation capability.

The New South Wales (NSW) Road Transport Authority uses two automated systems to support FOI processing. The first is simply an Excel spreadsheet that records the progress of the applications and uses standard Excel features to produce management and statistical reports. The second is a newly developed system linked to the first which automatically prepares the acknowledgement letter, adds the application to an FOI management follow-up list, lists the application in the weekly report to the Minister and registers the file in the file registration system. The NSW Premier's Department originally developed the package on Paradox software and subsequently converted it to Microsoft Access.

The Office of Information and Privacy (OIP) in the US Department of Justice (DoJ) coordinates and implements policy development and compliance government-wide in relation

---

[5] A requirements specification for a replacement system has been produced. It seems likely that this will be based on a system developed by the Department of Transport.

to the FOIA. It also deals with FOIA and privacy requests directed at senior levels within the DoJ, all FOIA appeals involving the DoJ and mandatory declassification of classified material. Staff prepare declarations for court and work closely with departmental counsel in defending FOIA litigation. The office uses an Oracle based stand-alone system developed in-house which combines the management of FOIA and privacy requests. Access is password-protected and incoming requests are assigned to one of three tracks. There is a searchable 'subject' field and similar enquiries are allocated, where possible, to the analyst who handled the subject area previously. The type of requester can be only be identified using the 'lawyer' field as when designed it was not envisaged that it would be useful to identify other categories. There is a field to identify whether the request was received on consultation or referral from another agency. OIP does not generally refer on to other agencies (though it may advise the requester to write elsewhere) but does refer to other parts of the DoJ.

The 'component' field identifies which office(s) across the department the request should go to. There is a 'status' field which is updated by the analyst handling the request as processing proceeds. Values include backlog (i.e. waiting to be assigned); processing; review; no record; and approval. The status field is important when responding to phone enquiries about what is happening to a particular request.

There is no flag to allow analysts to highlight sensitive requests and no link to word-processed forms or standard letters. The system has no redaction capability (this is done manually) but there are codes indicating which exemptions, if any, were used and codes for case closure, for example no record; failure to identify record; total grant; partial denial; and failure to comply with requirements (to pay fee or to identify themselves in a personal request).

Internet searches show that other US agencies have also gone down the route of in-house development. A database specialist in the National Oceanic and Atmospheric Administration within the US Department of Commerce has developed a number of applications for his Agency including a FOIA tracking system. The Freedom of Information Tracking System (FITS) was developed by the US Mint and is installed on the Mint's network. However, it is used by only one user and does not interface with any other systems. The Freedom of Information Management Tracking System (FOIMATS) is an administrative system used by the Environmental Protection Agency's FOI Office. The system tracks the status of requests for information under the requirements of the FOIA. The data from this system is used for the Agency's annual FOIA activity report to the DoJ.

Perhaps the most ambitious in-house development has been undertaken in Mexico. The *Instituto Federal de Acceso a la Información Pública* (IFAI) has three automated systems to help process FOI requests. The first, known as the *Sistema de Solicitudes de Información* (SISI), registers requests of information issued on the Internet or on paper to the ministries and entities of Federal Government. The use of this system is obligatory for the 250 units of

the Federal Government.[6] More than 50 of these units participated in the development process. This is a distributed system which provides central control of requests.

The second automated system supports Federal Government agencies in the administration of the requests. This system was donated by the Ministry of Tourism to the IFAI and is compatible with SISI (although not electronically linked to SISI because not all Ministries could meet the communication requirements for integration). The necessary adjustments to achieve compatibility and compliance with Freedom of Information Law were undertaken by the governmental ICT organisation. The system has been adopted by more than 100 of the 250 Federal Government units.

The third system is internal to the IFAI and is used for administration of appeals. It is fully compatible with the SISI. The system automatically assigns appeals to one of the Commissioners and their authorised advisors with the appropriate security clearance.

Finally, some of the agencies responding to our enquiries were using commercial FOI software packages or systems designed to their specifications by outside contractors. For instance, NSW Department of Health used the TRIM package developed by Tower Software for tracking FOI requests.[7] The US Department of Education recently reviewed commercial products and decided to replace its system based on LotusNotes with the package FOIAXpress.

The US Federal Bureau of Investigation (FBI), which has the biggest FOIA operation of any US government department, had commissioned Vredenburg Inc. to develop a system that performed both tracking and redaction functions. This system is based on existing software which was tailored to specific FBI requirements. The most challenging aspect of the development was the 'state of the art' imaging and redaction system. This updated the tracking information automatically to minimise manual data entry. About 99 per cent of the documents to be accessed are only available on paper. Anything to be redacted is scanned in first and the original and redacted versions are available again if the document is the subject of a future request. This is seen as a great help as retrieval of manual files can be problematic.

The system can be linked to other systems if necessary and this should make it possible to access electronic records when these become the subject of requests. In time, the FBI plans to scan in all paper files so that the paper versions can be destroyed.

Vredenburg has also provided FOIA systems to other US agencies including the National Security Agency, the Defence Intelligence Agency, the Central Intelligence Agency, the Securities and Exchange Commission and the Internal Revenue Service. Some of the features developed for the FBI are now in the core product.

---

[6] It can be viewed at http://informacionpublica.gob.mx/
[7] TRIM was used in conjunction with the FOI reporting software developed by NSW Premier's Department referred to above.

The position in Canada is of particular interest because it is much more centralised than in the US. The President of the Treasury Board is responsible for government-wide coordination and administration of Canada's FOI laws which are known collectively as Access to Information and Privacy (ATIP) Acts. The Treasury Board Secretariat has created, owns and maintains a database system known as Co-ordination of Access to Information Requests System (CAIRS). All Federal institutions enter new access requests daily on CAIRS, allowing the Treasury Board Secretariat to monitor such requests. CAIRS is used to coordinate requests across departments and since '9/11' is also used for central oversight in relation to sensitive security requests. The CAIRS software was upgraded in 2001 and is web-based. It was designed to permit public access to some fields but this facility has not been activated.

The Canadian software company Privasoft has developed a suite of software products to assist government institutions in handling ATIP requests. ATIP*flow* is a case management and workflow tool that centrally consolidates all activities between FOI staff, the department, involved parties, and requesters. It is used by 40 of the larger government institutions in Canada. Privasoft claims that ATIP*flow* assigns requests, retrieves required documents, generates automated correspondence and consolidates all notes, telephone calls and actions taken by staff into a single case file for easy and efficient retrieval. A major attraction for Canadian users of *ATIPflow* is that data can be directly uploaded to CAIRS. A companion package called ATIP*image* can be used for image capture and redaction of documents.

Privasoft and British Telecom are currently developing a strategic partnership aimed at producing a similar suite of products for UK government institutions.

2.3   Perceived strengths and weaknesses of automated systems

The experience of NSW Department of Health with TRIM illustrates the issues associated with the use of standard software packages rather than bespoke systems. The Department praised the facilities TRIM provides for locating and tracking documents (provided all staff use the system correctly) and was satisfied with its ability to track responses to requests made to other branches or divisions to supply a copy of documents to the FOI Unit. However, TRIM was not very helpful for accounting purposes as the Department is required to calculate FOI statistics on a financial year basis while TRIM operates on a calendar year basis.

 The Department also stressed that the effectiveness of TRIM, or any FOI system, could be undermined by poor document management. It depended on staff creating a TRIM entry for every document received by or created by the agency and when documents are placed on file or moved to another area. If this is not done consistently, TRIM incorrectly identifies the file's location.

An entry is made in TRIM for every document received in the FOI unit even though not all are FOI applications. This causes confusion between the numbering of the documents and the numbering of FOI applications. Similar problems are likely to arise whenever a general document management system is also used to track FOI requests.

Even systems designed specifically to meet departmental needs had shortcomings. The US DoJ system stored the dates when requests were received but did not calculate or display the time that had elapsed or whether the statutory response time had expired. Nor did it record who in the Department had been approached for records relating to the application and their response. Instead, this information was noted in a manual log.

A common problem with older systems was that report generation facilities were insufficiently flexible. The DoJ system could only generate a limited set of reports covering, for example, pending and closed requests, each analyst's cases, open and closed appeals and the median time to disposition. It could not provide reports showing how long requests had been pending by the track to which they have been assigned or analyse the types of requester. Alasdair Roberts of Syracuse University observed that the Canadian ATIP*flow* package did not include a flexible report generator. In contrast, the FBI singled out the report generator in their system for particular praise. Its flexibility helped individuals manage their own work and also assisted managers. It was possible to report, for example, on the work pending in each queue.

The Canadian Department of Defense (DND) did not comment on the report generation features of ATIP*flow*. However, it did identify as a recurring weakness the ability of all users to access all files. Once logged on, an individual could change dates, actions, comments and other data regardless of that person's position or function. This could be a particular difficulty if a user made a change after a weekly, monthly or annual report has been generated because the next report would not reconcile with the previous one. The problem is due to be remedied in the next version of the software.

The DND also used ATIP*image* for image capture and redaction of documents. While praising many of the its functions, it pointed out a number of problems associated with use of the system:

- the large electronic memory and speed requirements

- the need for detailed user training

- some employees had found it difficult to work with documents 'on screen' rather than on paper (this had been alleviated by using large 21-inch monitors so that the whole document can be viewed at once in actual size and by incorporating anti-glare features)

- the initial workload was much heavier on the 'front end' compared to using hard copies and photocopiers. The documents had to be triaged, indexed, and scanned prior to review

- the document search and compare feature was only as good as the effort applied to the indexing function, which could be time-consuming. Indexing involved filling out fields such as from/to, subject, type of document and date. Because documents are scanned as images (rather than converted to text), the index is the only way to search

- if employees are on a system connected to the internet (even with a firewall), a separate local area network or stand-alone system is required to ensure document security.

In commenting on the shortcomings of their automated systems, many pointed to a fundamental issue that automation could not overcome: underlying weaknesses in the process being automated would persist after computerisation.

Vredenburg's representative at the FBI acknowledged that a mistake had been made in deciding to automate the existing manual processes. For example, the FBI had about 30 'queues' or tracks to which requests could be assigned. These had been reproduced in the system. They now think that the processing of FOIA requests should have been simplified and streamlined prior to automation.

The Canadian DND also stressed the importance of getting the right underlying procedures. They pointed out that consistent standards must be developed and monitored amongst users otherwise system-generated information would be incorrect and misleading.

2.4   Quality controls to preserve data integrity

Respondents described the following approaches to ensuring that the quality of the data on their computer systems was not compromised:

City of Sydney, NSW:	Hard copies of all material relevant to a matter are placed on the appropriate file. There are no other quality control checks
NSW Department of Health:	Access to the TRIM system is password protected. Access to certain fields is restricted to certain personnel. Access to the FOI Reporting System is also password protected. The manager is responsible for ensuring that the data is entered correctly, usually by comparing the date with other records
Rockdale City Council, NSW:	A Council officer must be present when files are being viewed
NSW Road Transport Authority	Access to the computer software is restricted to the staff working in the area that deals with the FOI applications and the necessary IT support staff
Canadian Department of National Defense	The *ATIPimage* system is accessible by all users within the Directorate Access to Information and Privacy (DAIP), any of whom can make changes to any file. This does cause potential difficulties but is not a significant problem in practice. Quality control consists of ensuring that users inputting information are applying proper standards. A system analyst conducts a weekly review of data, looking for anomalies. Spot checks are also conducted.

Mexico	Each Ministry or Entity is given a digital certificate. The requests are automatically assigned to each Ministry or Entity and only they have access to their requests. Each change is registered in the system through log files and by the system itself. It stores the user identity, time and requester identity. Only the middle tier is accessible through the web. The back tier (the database) is not accessible. There are periodic backups of the database. Internally, at the Ministry of Public Function, only authorized personnel have access to the system physically and through the network.

US departments self-report on their FOIA performance. Tom Blanton at the National Security Archive of George Washington University indicated that there are no external quality controls; even the General Accounting Office, the audit arm of Congress, has only looked at departmental annual reports. The National Security Archive website[8] reports on its ongoing audit exercise. It has asked for the 10 oldest requests held by each department and some were unable to identify these.

2.5   Steps in processing requests

Although the extent of automation varied between agencies and jurisdictions, the underlying steps in the process were similar, namely:

- identification and logging of new requests on receipt
- assigning to a member of staff for processing
- where necessary, communicating with the requester to clarify or narrow down the request
- contacting appropriate individuals in the agency asking them to provide any records they might hold that are responsive to the request
- assessing the content of such records to determine whether legal exemptions to their disclosure apply
- redacting (deleting) those parts of disclosable records that attract exemptions and annotating the redacted document to indicate which exemptions apply to each deletion
- forwarding the redacted records to the requester and noting on the log that the response has been completed.

Detailed procedures may have slight variations or additions. Agencies dealing with particularly sensitive or classified material are likely to have the most robust procedures. For instance, when the FBI receives a written request, it checks a central index to discover if there is a file on any person mentioned in the request. A decision is made as to whether the file is pertinent to the request. If it is, the master file is scanned in, held in 'backlog',

---

[8] http://www.gwu.edu/~nsarchiv/

reviewed and redacted as necessary, reviewed by a supervisor and finally the images are 'sealed' (after which they cannot be changed again) and released. Files with national security information are reviewed on-line by a separate section. Once the response has been sent, the requester has 60 days in which to appeal. Department attorneys review appeals. If the requester is still dissatisfied then the next step is litigation. The appeal and litigation process is built into the automated system so that, for example, a further release of records can be dealt with.

The task for agencies of identifying an FOI request is eased if a special form is used or the requester is required to cite the relevant FOI legislation. The Freedom of Information Act 2000 includes no such requirements, nor does the legislation governing FOI requests in:

- United States;
- Federal agencies in Australia (although the application fee must accompany the request);
- New Zealand;
- Sweden;
- Netherlands
- Mexico; or
- Finland.

In Australia and the United States requests must be in writing.[9] In Finland, Sweden, Netherlands and New Zealand, information can be requested in various ways, for example by telephone, in writing, by e-mail or by visiting the competent authority. The person requesting a document does not have to refer to legislation. In Mexico, a request can be submitted by writing a letter, by using the approved form or by the on-line request system.

There is a special form for submitting FOI requests to Federal government departments in Canada (Provinces have their own FOI legislation) but its use is not mandatory. However, the application fee must accompany the request. An optional form is also made available by the Health Authority in the Australian State of Queensland, where the request must be in writing but need not cite the Act. Requestors in New South Wales must cite the legislation in their request. No special form is needed by law but many agencies insist that such a form is used.

2.6   Time to respond to requests

Section 10(1) of the Freedom of Information Act 2000 allows public authorities a maximum of 20 working days to respond to requests. All countries contacted for this research also had statutory time limits within which agencies must respond. The limits ranged from two weeks in the Netherlands and Finland to 30 days in Canada and Commonwealth agencies in

---

[9] DoJ guidance states that 'requests must be in writing, either handwritten or typed. While requests may be submitted by fax, most components of the Justice Department have not yet developed the capability to accept FOIA requests submitted through the World Wide Web.'

Australia. Some operated more than one time limit: Finland increased the time allowed to four weeks for complicated requests while permitted response times in the Australian State of Queensland depended on the age of the document, whether it was a 'personal affairs' document, and whether formal consultation was required. As with the Freedom of Information Act 2000, the legislation in most countries contacted allowed for the response time to be extended in prescribed circumstances.

Alasdair Roberts felt that it was difficult to monitor compliance with time limits in Canada because it was not necessary for the requester to 'flag up' a FOIA request. He has detected 'systemic non-compliance' with time limits across agencies. This has a knock-on effect in swamping the system with complaints which leads to a break-down in enforcement because the Commissioner cannot keep pace.

The Canadian government is looking at patterns of non-compliance across departments using 'report cards' which they submit on the proportion of requests not dealt with within the allotted time. If this exceeds 20% (a 'red alert'), senior civil servants can be asked to give evidence about the problem. Processing times are routinely exceeded where there is a need to consult the Cabinet Office and where requests come from political parties and journalists.

Compliance with statutory time limits is even poorer among US Federal agencies. The OIP in the DoJ said that the only requests which they could respond to within 20 days were those where there had no responsive records. Various means were used to maximise the time available in which to respond. The clock only started when the OIP received and date-stamped a request, not when it was received by the DoJ. The OIP then informed the requester of the official date of receipt, reference number, the analyst's name and a central phone number. If it was necessary to ask the requester for more information then that stopped the clock. Requesters could ask for their application to be expedited but it was up to the OIP to decide whether to accede to the request. As mentioned above, the automated system used to manage requests held the data needed to calculate due dates but these were not displayed. One system report showed the median time taken to deal with requests but time compliance was not otherwise monitored.[10] The system could not report on the time taken to process requests by the tracks to which they were assigned. OIP staff estimated that response times for about 95% of requests exceed the statutory 20 days.

The performance of the FBI in this respect was even worse. The FOIA team said that it processed 'practically no' requests within 20 days. Congress had doubled the time allowed in 1996 but it was still insufficient. The FBI writes to requesters and explains that there will be a delay but makes no time commitment.

---

[10] Tom Blanton at the National Security Archive told us that published median response times were very poor indicators of the delay experienced by requesters.

2.7   Fees

The charging regime operated by agencies must be incorporated in their procedures. The Freedom of Information Act 2000 does not require charges to be made, but public authorities have discretion to charge applicants a fee in accordance with Fees Regulations made under sections 9, 12 and 13 of the Act in respect of requests made under the general right of access.

Alasdair Roberts thought that a nominal application fee was useful to discourage frivolous requests. Tom Blanton saw search and review fees as totally subjective and felt they were used to deter requests. If fees were necessary, there should be a flat fee upfront or realistic photocopying charges. He queried the accuracy of numbers of requests in departmental annual reports on the grounds that some agencies do not log in requests until they have received fees.

Agencies contacted had differing practices in respect of fees. In Canada, a $5[11] application fee is required. Other administrative tasks, such as translating and photocopying, can increase the fee to $25. No-one is exempt from fee payment. There is no further charge provided the effort involved in responding to the request does not exceed five hours. If it is estimated that the search will take longer, requesters are informed of the approximate cost. Alasdair Roberts reported that 90% of requesters in Canada pay only the application and administrative fee.

 US Federal government agencies do not charge an application fee for FOIA requests. Every agency has its own fee regulations but there is fee guidance (Office of Management and Budget 1986 amendments). Sheryl Walter in the DoJ (formerly of the National Security Archive) did not favour the levying of an application fee. She thought that the five hours of effort at no charge was appropriate and that no further work should be undertaken until the amount to be paid was agreed.

Daniel Metcalfe from the OIP described fees as a 'meaningful bulwark – we want to leverage fees as a barrier to very wide requests'. Institutional requesters are fearful of leaving something out and often submit sweeping requests. Daniel Metcalfe said that they will proceed without payment for the first $25. His office notifies requesters if the cost of the research is estimated to exceed $250. It breaks down estimates by the approximate number of pages to be copied and the cost of the search effort, using different rates according to the levels of staff involved. The office asks for a commitment to pay but if a request is too broad, work will not be undertaken unless the requester narrows the scope. Requesters can ask for a fee waiver and fees charged to the media are lower. If requesters fail to pay, their names are circulated to all FOIA offices across departments.

The FBI provides the first 100 pages free and the labour is free (it charges for responding to requests from commercial organisations but says these are rare). It is about to offer requesters the option of receiving information on CD rather than paper as this will reduce costs. They

---

[11] All costs are quoted in the currency of the country referred to.

will charge $15 for 2,000 pages (which would otherwise take hours to create and would cost $250 to photocopy).

In Australia, applications for access to documents will generally attract an application fee of around $30 and some agencies make additional processing charges. There are provisions for waiver of charges in certain circumstances such as financial hardship and where access would be in the public interest. The NSW Road Transport Authority told us that if the amount of time to locate and copy the documents will be more than three hours, it writes to the applicant and requests an advance deposit, estimated as two-thirds of the total price. The Authority considers that this ensures the applicant is genuine and gives them the opportunity to re-think their application if it is going to be expensive. The applicant is allowed 28 days to respond and the timeframe to process the application stops during that period. The Authority received 878 FOI requests in 2001-02. Processing costs were estimated at $54,611.00 and fees received totalled $34,207.00.

The Australian Securities and Investments Commission said simply that, in addition to the $30 application fee, charges may be imposed for the time spent in searching for and retrieving relevant documents, decision-making time, photocopying and postage. It makes a preliminary assessment of charges and seeks a deposit or full payment before proceeding.

Finland, the Netherlands and Sweden do not levy an application fee and do not charge for the work involved in responding to a request. There is no charge for studying a document in the offices of an authority although a charge may be made for copying documents.

Mexico also charges a fee to cover the cost of reproducing and sending information. Public information available electronically is provided to the requester without cost. Where appropriate, the requester will be notified of the existence of this information in the Ministry's or Entity's web page. Public bodies may charge the requester for information with a commercial value (e.g. statistics, books or cartography). In all cases, the requester must pay the appropriate charge before information is released.

In New Zealand, agencies have the option to charge. The Official Information Act states that, if a charge is made it 'shall be reasonable and regard may be had to the cost of labour and materials involved in making the information available and any costs incurred pursuant to a request for urgency'. The Ministry of Justice issues, with the approval of Cabinet, charging guidelines that represent what the Government regards as reasonable charges for the purposes of the Act, and which agencies are required to follow in all cases unless good reason exists for not doing so. If a requester thinks the charge is unfair he or she may complain to the Office of the Ombudsman. The State Services Commission indicated that most of the information it provides in response to a request is given free of charge. In general, the Commission would only charge if an exceptionally large amount of material was asked for either on one occasion or over a series of requests. MPs and their Party Research Units are not charged for information requests.

2.8 Report production

Some respondents produced no reports of any kind but most produced an annual report indicating, at the very least, the volume, nature and outcome of requests. Alasdair Roberts described the annual reports produced by each Canadian government department as 'not very informative'.

A variety of internal management reports were also generated, for instance NSW Department of Health has a weekly report on the status of current FOI applications and a fortnightly report on the status of current FOI applications to the Minister's office. This latter report is forwarded each fortnight to the FOI Coordinator of the Premier's Department.

The use made by the FBI of its flexible report generator was described above but perhaps the greatest report generation capabilities were provided by the Mexican SISI system. Details can be found in their response to our questions.

2.9 Benefits of existing investment and future plans

None of those from whom responses were received had formally evaluated the return their organisation had obtained from its investment in automated FOI systems although many felt that the benefits were self-evident:

> 'Without a doubt, the implementations of these automated systems reduce significantly the costs of transaction of an information request. As a fact, in the first two months following the introduction of the Law the number of information requests was around 12,000, of which more than 7,000 had already been answered. Without an automated system this would have been impossible and the capacity to respond would be significantly affected' *(Mexico)*

> 'Our efficiency has improved since acquiring the systems in terms of quantity of requests completed on time. Although we are sure that some of our improvement is due to these systems, we implemented a number of changes at the same time such as hiring more full time staff and restructuring our organization' *(Canadian Department of National Defense)*

> 'We have not assessed the return but I can tell you it is highly efficient as compared to paper-tracking' *(New York State)*

> '[The FBI] have been able to downsize the size of the group handling FOIA requests'.

For most organisations that had invested in automation the benefits had been in line with expectations. Mexico said its expectations had been exceeded. Planned enhancements were aimed at increasing the amount of detail recorded about each request, improving report generation and integration, either of separate FOI systems or of the FOI system with departmental records management systems.

3 SOFTWARE COMPANIES, PRODUCTS AND EXPERTISE

3.1 Introduction

This chapter draws on the responses of software companies approached in the course of the research to indicate the range and nature of available products and expertise relating to automated support for managing and processing FOI requests.

3.2 The companies

A list of questions was sent to a total of 21 companies identified through Internet searches or by FOI managers as potentially being active in the field of FOI software. The questions were also sent to British Telecommunications plc (BT) which has signed a confidentiality agreement with the DCA in relation to the development by BT of FOI related services it intends to introduce.[12]

By the time the deadline for inclusion in this report had been reached, eight companies had responded including one that indicated it had no FOI products or expertise. BT provided a demonstration of the Privasoft software and a discussion of its plans for the UK market. Positive written responses were obtained from:

- Privasoft
- Vredenburg
- Netsight
- Handysoft
- Tower Software
- Appligent.

3.3 Software products of responding organisations

Privasoft markets a suite of software applications, known collectively as the *Access To Information and Privacy (ATIP)* suite of products, for the management of information requests by public bodies. The constituent applications are:

- *ATIPflow*, for case tracking;
- *ATIPimage,* for document imaging;
- *ATIPconsole,* which provides a management overview;
- *ATIPliaison,* which supports workforce collaboration; and
- *ATIPcair,* for Parliamentary Reporting.

---

[12] A separate questionnaire was sent to Privasoft, the Canadian company with which BT is developing a strategic partnership.

Privasoft says that the ATIP suite (or at least some of the applications that make up the suite) is now in use by over 45 government agencies in Canada including the DND and the Royal Canadian Mounted Police.

BT plans to market the Privasoft suite in a form tailored to meet the specific needs of the UK.

Vredenburg provides information management services to Federal, State and local government organisations in the United States. It specialises in document imaging and records management and it claims to support all of the most complex and highest volume FOIA operations in US Federal government. Vredenburg has recently been acquired by AMS, a multi-national consultancy with a UK presence.

Vredenburg's key FOI offering is the VeFOIA Product Suite which it describes as 'a commercial, off-the-shelf solution expressly designed to meet FOIA request processing challenges'. The features offered include:

- a request tracking system
- standard customizable letter templates
- electronic Work Management
- electronic redactions and annotations
- fee estimation and payment management
- full-text search engine for document retrieval
- web-enabled customer request form
- web Reading Room
- web request status
- web-based collaboration with subject-matter experts; and
- an audit trail of work undertaken.

The system also claims to be database independent, scalable from one to 800 users, adaptable to each agency's IT infrastructure and capable of handling all all document and image formats.

Netsight is a UK-based company that develops bespoke content management systems of particular interest to organisations working to meet the requirements of the Freedom of Information Act 2000. Netsight offers a distinct set of tools based on the open source Zope and Plone[13] content management frameworks, details of which can be found at http://www.netsight.co.uk/services/foi-act-software. The FOI-specific features that can be

---

[13] Plone (http://www.plone.org/) is an intranet server built on top of the open source application server Zope (http://www.zope.org/), and the accompanying content management framework. Plone is a document publishing system and groupware tool for collaboration between separately located entities. Zope provides tools to integrate data and content into Web applications.

delivered are not clear from the description on the website but they do not appear to include tracking the processing of requests or redaction. Costs depend on individual requirements but start around £30,000. Netsight's most significant FOI client is Warwickshire Police (http://www.warwickshire.police.uk/) for whom it has developed a new public website. Warwickshire Police is using the Netsight system to store all of its information that must be made available publicly under the publication scheme described in Part 1 of the Freedom of Information Act 2000. The information is tagged with metadata, approved by reviewers and delivered using the integrated website.

The Handysoft Corporation markets BizFlow which it describes as 'a solution developed for business process management and workflow automation'. The product is aimed at multi-user environments in both commercial and government marketplaces. BizFlow supports most leading database products and can interface with existing document management systems. It provides a process designer employing a graphical user interface which allows the client to build and configure process models. These comprise, among other things, activities, participants and deadlines. BizFlow also includes a forms designer.

The BizFlow literature highlights its ability to 'support compliance with FOIA requirements' although the case studies provided of government departments that use BizFlow do not explicitly mention this aspect. A wide range of government clients is quoted but Handysoft asks that any contact is made through them. The general message is that BizFlow is a flexible process management tool that can be configured, among other things, to manage responding to FOI requests. It has not been designed with FOI explicitly in mind and does not include redaction facilities.

Tower Software produces a package called TRIM Context which offers records and information management features. TRIM is used for managing FOI requests by the NSW Department of Health. TRIM is in current use in the UK by the Department of Trade and Industry for electronic document and records management.

Appligent Inc. is the leading supplier of third-party software for Adobe Portable Document Format (PDF). Redax is a plug-in for Adobe Acrobat that is designed to completely remove text and scanned images from PDF documents. This makes it suitable for redacting documents that are available in or have been converted to PDF format. The full version of Redax costs $349.

3.4   Other software products

Despite acknowledgement of our request and reminders, no information was received from Metastorm, Valid Information Systems or AINS, all of which are active in the FOI marketplace.

Metastorm's process management application was used in 2000 by the US Department of Defense to manage and clear its backlog of FOIA requests.[14] The company's website, http://www.metastorm.com/products/, refers to only one product known as BPM (Business Process Management) although it claims that this is used by government organisations to manage FOI requests.

AINS markets FOIA*Xpress* which was recently selected for use by the US Department of Education (although that Department did not respond to our request for information). FOIA*Xpress* is aimed at US government agencies. It is a web-based product which electronically accepts requests from multiple requester types and keeps track of the requester details. It allows FOIA staff to search electronically for responsive records and redact where necessary. Details can be found at http://www.foiaexpress.com/sub/foia_ff.html. The redaction features are also available separately as the product Redact*Xpress.*

Valid Information Systems Limited is a UK-based developer[15] that markets R/KYV, an Electronic Document and Records Management System. Built on open standards, R/KYV has UK Public Record Office approval and Model Requirements for the Management of Electronic Records (MoReq)[16] compliance, and is designed to meet current and emerging e-Government standards including the Freedom of Information Act and the Data Protection Act. After an open competition, the Office of the Deputy Prime Minister selected R/KYV to manage its documents and records in March 2003. More information about R/KYV can be found at http://www.valinf.com/.

There are a number of off-the-shelf redaction packages available. A (slightly out of date) review of some can be found at http://www.gcn.com/archives/gcn/1997/October27/rev1.htm. The applications discussed include a free template that can be used for redacting Word documents. The template was developed by the US Department of Veterans Affairs and can be downloaded at http://www.va.gov/foia/redactor.

---

[14] See http://www.gcn.com/vol19_no21/software/381-1.html
[15] Valid was acquired by Hummingbird Ltd. of Toronto in July 2003.
[16] See http://www.cornwell.co.uk/moreq.

4   OTHER AUTOMATION AND IMPLEMENTATION ISSUES

4.1   Introduction

During the course of discussions, our attention was drawn to a range of issues that impinge directly on the implementation of the Freedom of Information Act 2000. Most of these impact, either directly or indirectly, on the provision of automated support for processing FOI requests.

4.2   System design

Interviewees stressed a number of FOI-related factors to be kept in mind when government agencies are developing or procuring new computer systems. The design of any system that holds information should address the searchability and accessibility of that information in responding to FOI requests. The features that need to be included may be more sophisticated than those required to meet the internal needs of the department concerned.

It is important that there is an audit trail of the work done by departments in responding to requests for the purposes of accountability and responding to possible appeals from dissatisfied requesters. Automated tracking systems should include the facility to create such logs recording, as a minimum, what was done, when, by whom and what parts of departmental databases were accessed. These logs may themselves become the subject of FOI requests.[17] Alasdair Roberts of Syracuse University has obtained activity logs through FOI requests and found, for example, no record of consultation with another department which he had been told had taken place.

Maurice Frankel of the Campaign for Freedom of Information stressed that any system procured to assist in processing FOI requests should not only support the efficient handling of such requests but also the interests of accountability, for instance to permit the authority's compliance with the Act to be assessed, if necessary, by the Commissioner or external requesters. He cited common problems in other jurisdictions as:

(a) delay in responding to requests;
(b) excessive charges (in the UK context this might include excessive refusal of requests on grounds that the cost threshold has been exceeded); and
(c) excessive reliance on particular exemptions.

Mr Frankel advocates that any FOI system should, if possible, allow these potential problems to be investigated. For example, in relation to delays:

---

[17] The FBI says it has never had a request for its activity log and considers it would not be disclosable.

- Are requests from particular types of requesters typically dealt with more slowly than the norm (in Canada there is some evidence that MPs' and journalists' requests are handled differently and more slowly than others because they are assumed to be more contentious and hold more opportunities for adverse publicity for politicians)?

- Requests involving third party information are likely to involve consultation with the outside party and therefore take longer. Are particular third parties causing particular problems, for instance is one particular industry or company or type of third party public authority responding significantly differently from the norm? Are specific topics causing particular problems? Or are there problems with particular types of records, such as those that are badly organised, or in archives?

- The response time may reflect the seniority of the official who handles the matter, as more senior staff may be more confident in taking decisions or have greater authority to release information. When ministers are involved in disclosure decisions, what effect does this have on timeliness, outcome, etc?

- The treatment of requests may vary between units within the same authority. Are problems occurring only within particular divisions and, if so, can these be traced to particular causes?

- Where delays occur, does the system help identify the cause? Are bottlenecks caused when, say, legal advice has to be sought, or by trying to develop a common position with other authorities or by internal review? Are particular exemptions unusually problematic?

- The normal 20-day response time can be extended when the authority has to consider whether the Act's 'public interest' test applies [s10(3)]. How prevalent are such delays? Is the delay in these cases actually attributable to consideration of the public interest issues, or is it more strongly correlated with other factors (eg the number of pages of material involved or the need to consult third parties) that also affect these requests?

In relation to charging, Mr Frankel suggests that systems should be capable of exploring whether particular types of requests or requesters are treated more or less generously in terms of charges.

Another important area in Mr Frankel's view is recording the help given to requesters. The Act requires authorities to provide advice and assistance to requesters (s16). Does the system prompt officials to record what advice, if any, they have provided? Officials are encouraged to phone up applicants to discuss their requests. Does the system encourage the recording of the outcomes of such conversations?

4.3   Automated support for oversight of the operation of FOI legislation

Before providing guidance to agencies in central government on FOI system procurement, it will be necessary to decide whether to adopt a centralised approach along Canadian or

Mexican lines or the more decentralised model used in the US Federal system. As described in the previous chapter, the Canadian CAIRS database allows the Treasury Board Secretariat to monitor the FOI activity of all Federal agencies. There is no comparable system in the US and this makes it difficult to assemble a total picture of how the US FOIA is operating. Moreover, the OIP in the DoJ felt the need of a system like CAIRS to assist in monitoring FOIA compliance of government departments and the associated inter-agency consultation that it undertakes.

4.4 Freedom of Information and Data Protection

In general, requests for personal information fall under the Data Protection Act 1998 rather than the Freedom of Information Act 2000 although there is a complex interplay between the two pieces of legislation.[18] Agencies may decide, for administrative convenience, to combine the management of FOI and personal information requests but systems should be able to distinguish between the two for accounting and other purposes. Agencies will need guidance on this point.

Other jurisdictions face similar problems. The OIP in the DoJ uses the same software system to manage FOIA requests and Privacy Act requests for personal records. Daniel Metcalfe said that departments will not advise a requester about his or her Privacy Act rights unless it is clear that it is a first-person request.

Alasdair Roberts reported that, in Canada, a decision has been made to treat an individual's request for health records as a FOIA request although formerly they were not considered to fall into this category. In contrast, assessments relating to whether property is contaminated are no longer treated as FOIA requests. Movement of categories of request into and out of FOIA have to be taken into account in analysing the number of requests reported by the Canadian government. Because of such re-categorisation, Professor Roberts has found it difficult to assess the true impact of FOIA fee increases on the number of FOIA requests in Canada in the late 1990s.

Tom Blanton of the National Security archive commented that about half of all FOIA requests to US Federal agencies are accounted for by the Department of Veterans Affairs which treats all requests as FOIA requests, even those relating to personal data. For example, veterans' requests for information about the timeliness of their payments are regarded as FOIA requests.

4.5 Electronic requests

The Office of the E-envoy is responsible for ensuring that all government services are available electronically by 2005, with key services achieving high levels of use. It follows

---

[18] For a discussion see, for example, P. Birkinshaw (2001)'Freedom of Information – The Law, the Practice and the Ideal' pp. 339-340, Butterworths.

that UK government agencies will be required, at some point, to accept requests for information submitted by e-mail or over the Internet. The facility to accept and progress such requests will therefore be a key requirement for any system aimed at supporting departments' FOI response.

At present, Canada does not accept e-mail requests because of the threshold payment. The US DoJ and FBI do not accept electronic applications because they fear being overwhelmed by the volume of requests this would generate, although they acknowledge that they will have to reverse this policy at some point in the future. Tom Blanton felt that electronic requests would be easier to handle as they can be migrated directly into the database. Moreover, the webpage could contain links to an electronic reading room and other websites thus diverting many requests for information that is already published. He remarked that it is a current failing that departments do not analyse how many responses to requests are met by information already in the public arena.

4.6   The status of e-mails

It is hard to see how e-mails generated or received by government personnel in the course of their duties can be excluded from the scope of FOI legislation. Nevertheless, the FBI told us that e-mails are not yet considered part of permanent FBI records but that if an e-mail forms part of an investigation, an agent is expected to print it out and include it in the file. If it is the equivalent of a phone call which would not be the subject of a file note, then it need not be printed out. The OIP in the DoJ said that was up to the holder of information to decide whether e-mails should be included in the search for responsive material.

Tom Blanton stressed the need for clarity as regards the status of e-mails. The National Security Archive has litigated to force one government department to archive e-mails. The government argued that they were the equivalent of phone messages. The court order required the government to save e-mails electronically rather than printing them out and scanning them in again for FOIA purposes. The falling cost of digital storage has removed the main objection to this practice. Indexing could be performed using an approach similar to the State Department's automated system for searching voluminous cable traffic and e-mail indexing could be integrated into FOIA systems.

Professor Blanton suggests that departments should be persuaded to adopt existing best practice in relation to the management of all electronic records, including e-mails. This would facilitate an efficient response to FOIA requests. In the US, the defence sector has led in this area, for instance a navy destroyer has all its records and automated databases for staff and contractor records on indexed CDs. He suggested bringing together the Office of the E-envoy, GCHQ and security agencies to shape policy on electronic indexing.

David Kinnaird of BT also drew attention to the e-mail issue. He pointed to the ever-increasing use of e-mail in the public sector and the current absence of mechanisms to ensure these are organised in a systematic manner. This will make it difficult to identify information in e-mails that is responsive to an FOI request.

Mr Kinnaird stressed that every organisation should have a policy in respect of e-mails. Tools already exist to help ensure compliance with such a policy.[19] Other tools can search e-mail content and could be used to identify e-mails responsive to a particular request.[20] It is important that public authorities develop and implement a strategy for e-mail management both to improve their FOI response and as a key aspect of good practice generally.

4.7 Reading rooms

Many US departments have both physical and electronic reading rooms.[21] Daniel Metcalfe explained that if the DoJ processes a request and receives a further two similar requests, or anticipates doing so, the material disclosed is placed in the paper or electronic reading room. Requesters are advised about information available electronically but are required to pay if they want a paper copy. He stressed the importance of having a flag (and preferably, also a reference number) in the records management system to indicate that a record has been disclosed in response to a request (whether or not it has been placed in the reading room). Many US departments have no such flag and a link is not made until or unless someone remembers handling a similar request before.

Tom Blanton argued that reading rooms could go a long way towards meeting public demand for information: they are 'a market-driven mechanism for prioritisation'. A pro-active policy to put documents in reading rooms is cost-effective as it can forestall or simplify many requests as well as according with the spirit of the legislation. It is important that such reading rooms are properly indexed and searchable by subject and reference number. The index should include a line of description for each document.

Professor Blanton commended the open approach taken at the reading room in the Prime Minister's office building in Stockholm, in which cabinet minutes are lodged within weeks of the meeting. It has also a computer index to the Prime Minister's correspondence with the date, the recipient or sender, a line of description and the name of the staff person responsible. During his visit to the reading room, Tom asked for an item concerning correspondence between the Swedish Prime Minister and President Clinton. The item was classified but the staff person named came to talk to Tom and outlined the contents. Tom already had the US end of the correspondence and showed this to the staffer, who passed on Tom's request for the Swedish component to be declassified. It was sent to him in the post very quickly.

Departments that receive a significant volume of FOI requests should consider creating and maintaining an electronic (and a conventional) reading room. The facility to do this should be included in any specification of requirements for a system to support their FOI response.

---

[19] See, for example, http://www.orchestria.com/plugin/.
[20] See http://www.orchestria.com/services/discovery.htm.
[21] A list of the electronic reading rooms within the DoJ can be found at http://www.usdoj.gov/04foia/04_2.html. The location of each agency's conventional reading room can be found on its FOIA page.

4.8   Redaction

Decisions on what to redact require human judgment and cannot be automated. Daniel Metcalfe told us that in US government agencies, decisions about redaction are generally made by the person with FOIA expertise rather than the person with policy responsibility for the document in question. In the past, large chunks of text were excised when exemptions were invoked. Such an approach is no longer acceptable but decisions are now more difficult as the disclosability of each word or phrase has to be assessed.

The actual process of redacting material can be automated, although many large departments, including Daniel Metcalfe's own office, redact manually. Whether or not an automated system is used, when a single word is removed it is important that proportional fonts do not make it possible to guess the redacted word.

In the past, the FBI redacted manually using marker pens, bleach (when lifting inappropriate marker pen deletions) and the coffee pot to dry off sheets of paper they had worked on. These were then photocopied, though staff had to check that text did not 'bleed through' and reveal what had been redacted.[22] Now, redaction of documents is automated and deletions can be annotated with lines drawn to the justification code in the margin. It is also considered a significant benefit to produce a 'crisp quality product' rather than the well-worn items that can result from manual redaction.

FOI request tracking systems are generally expensive and probably beyond the means of many public authorities (although less expensive automated approaches are discussed in an article at http://fs.huntingdon.edu/jlewis/Prof/FOIAtech-AR93.htm). In contrast, some redaction software is available at little or no cost and could be attractive to many public authorities that receive relatively few FOI requests. An in-depth evaluation of such redaction packages was beyond the scope of this study but may prove worthwhile in the future in view of the potentially large number of organisations that might benefit.

4.9   Departmental structures, staffing, selection and training

The UK government does not envisage that extra resources will be needed by organisations in order to comply with the terms of the Freedom of Information Act 2000. This view conflicts with the experience of other jurisdictions, at least in the case of organisations that receive large numbers of FOI requests. Many of those to whom we spoke referred to the range of tasks performed by FOI staff and the level of skill required. Some tasks are not susceptible to automation, for instance reviewing incoming correspondence to identify requests for information to which the FOI legislation applies, interacting with requesters to refine and narrow the scope of requests, deciding on who within the organisation might hold

---

[22] Daniel Metcalfe warned that some types of photocopier allow original text to be deciphered from the photocopy after the original has been redacted by hand. He suggested that each location handling sensitive information should have access to special photocopiers to prevent this happening. Availability of such equipment will need to be considered in implementing the UK FOIA.

records relating to a particular request, scrutinising responsive records for material that is exempt from disclosure and deciding which exemption applies to each redaction.

Perhaps the largest FOI workforce is in the FBI which currently has just over 600 staff dedicated to responding to FOIA requests and an annual FOI budget of $52 million.[23] It received over 15,000 requests last year and processed over 14,000. It now has a backlog of about 1,500. We were told staff levels are lower than previously. Vredenburg, the suppliers of the FBI automated system for processing FOI requests, attributes a 10 per cent reduction in the size of the FOI workforce in the last two years to automation.

The OIP in the DoJ has a staff of 40 just to handle requests relating to the work of the Attorney General and the 'leadership' offices of the Assistant Attorneys General. It deals with about 1,000 requests a year, but these tend to be complex in nature. Sheryl Walter in the Intelligence Policy and Review section of the DoJ told us of separate groups which prepare an annual report of declassified papers (information security oversight office); consider high level FOIA issues; and deal with inter-agency FOIA issues.

Training in FOI skills requires significant investment. The OIP said it takes a year to train an FOI analyst. Training is carried out on a one-to-one basis because everything must be reviewed. Staff handling FOIA requests are likely to be reluctant to speak to requesters but everyone to whom we spoke agreed that they should nevertheless be encouraged to do so. When requesters submit broad requests staff should be trained to explain the process, find out what is really wanted and assist in reframing the request more narrowly. This invariably saves work down the line.

OIP requires its FOIA staff to have a college degree. In addition to being able to write clear explanatory memos and possessing analytical skills, analysts must be good communicators because of their interaction with senior staff to whom requests must be explained. Daniel Metcalfe said that staff also needs to know what information is already publicly available.

The FBI disagreed about the need for a college degree and thought it was more important to recruit from those who were already familiar with the FBI's own record systems. The learning curve was shorter for in-house staff. Knowledge of current events and history was important, in addition to analytical ability. It is not a very exciting job – 'you have to want to do it'.

Interviewees stressed the importance of creating a FOIA career structure for departments which handle a high volume of requests. FOIA grades in the US go from civil service entry to senior levels.

---

[23] It should be noted that for many aspects of FBI work, the UK counterpart lies outside the scope of the Freedom of Information Act 2000.

FOIA awareness-raising should be aimed at staff who create and hold records as well as those managing requests. The FBI's in-house guidance is on-line. The OIP said that the senior staff and political appointees know nothing about FOIA and the principles governing disclosure. For this reason, there is a need to complement the training provided within agencies with training from the centre designed to create a common understanding of FOI principles and to harmonise the quality of response to requests across agencies.

Tom Blanton agreed. He told us that the differences in approach between agencies are not explained by mission but by leadership and the culture created by the first FOIA officers. The first incumbents are crucial in setting the tone. He favours bringing people in who have worked on public education and public relations and who have experience of working with the media.[24] He cited one department which had a pre-implementation FOIA task force, one of whose jobs was to identify the right person to be FOIA officer.

---

[24] Sheryl Walter recommends including a panel of journalists in training events for government employees.

ANNEX A

QUESTIONS FOR FOI MANAGERS

Main Issues

1   What automated systems do you use to support the processing of FOI requests?
2   What are the strengths and weaknesses of these systems?
3   Who developed the software?
4   Please describe system architecture (stand-alone, distributed network etc)
5   Are there any links to other systems (e.g. document management systems)?
6   What is the sequence of tasks involved in the processing of requests?
7   What quality control mechanisms do you use to protect the integrity of data, particularly from the threat of unauthorised changes to the information held on computer systems?
8   What reports do you produce:
    a. on the volume, nature and outcome of requests
    b. in respect of performance in processing requests?
9   Have you assessed the return your organisation has obtained from its investment in such systems, in terms of efficiency savings or in other ways? If so, please provide details.
10 Are the benefits in line with expectations when the systems were procured?
11 Please describe any plans future development and improvements to your system for managing FOI requests.

Background Issues

12 What are the legislative requirements relating to requests? We are particularly interested in whether the requester must use a special form that identifies the legislation under which the request is made, the time allowed for the response and whether you can charge a fee.
13 What volume of requests do you receive annually and how many staff are involved in processing requests?
14 How do you go about identifying whether an exemption applies to information requested? Do you have to provide reasons to the requester when exemptions apply?

QUESTIONS FOR SOFTWARE SUPPLIERS

Please e-mail your response to <u>woolfsonr@aol.com</u> by 19 September 2003. Other material can be mailed to the address above.

1. Do you have any software products or have you developed any software that could be used for managing the response of public bodies for requests made under freedom of information legislation?

2. If you have such software products, please provide a brief description covering:
   a) name of product
   b) system requirements for running the software (platform, operating system etc.)
   c) functionality of the software
   d) access control features
   e) other features aimed at preserving data integrity
   f) compliance with standards, including XML[*]
   g) capability to generate statistical and other management reports
   h) networking capability
   i) expandability
   j) cost
   k) ability to link with other systems, for example to generate bills or correspondence or for electronic management of records and documents
   l) any evidence of efficiency savings that have resulted from use of your product
   m) names and contact details of clients currently using the product.

3. If you have developed software applications for clients, please provide a brief description covering:
   a) name of application
   b) functionality of the software
   c) description of the system running the software (architecture, operating system etc)
   d) access control features
   e) other features aimed at preserving data integrity
   f) capability to generate statistical and other management reports
   g) expandability
   h) adherence to government standards, including XML[*]
   i) ease of migration to other platforms
   j) ability to link with other systems
   k) any evidence of efficiency savings that have resulted from use of your software
   l) names and contact details of clients for whom the software was developed.

Management of Freedom of Information requests in other jurisdictions

4. Does your organisation supply and support software in the UK?

We would be interested to receive any literature you have describing your software, including examples of input screens, and/or demonstration versions of the software.