Open Data Strategy 2012 – 2014 for the Home Office

Contents

Introduction

The government's ambition is for Britain to have "the most open, transparent government in the world". Transparency is central to the way that the Home Office, and all organisations associated with it, deliver services and engage with the public. That has to be balanced, of course, with the need to protect the public, minimise bureaucracy and ensure value for money. Transparency is enabling the public to hold us to account in a meaningful way, and the re-use of data will help to drive growth, efficiency and improvements, which in turn will help reduce the deficit. Although there is some information we cannot publish[1], where we can, we will.

Information assets are essentially collections of data which are of value to the organisation, and are organised and managed in a systematic way, appropriate to the information they contain. Our publicly available Information Asset Register is published on the Home Office website, and accessible via data.gov.uk[2]. Information assets are reviewed by the relevant Information Asset Owners[3], in collaboration with others, to assess opportunities to provide re-usable data to support transparency, whilst considering the operational risk of doing so.

The Home Office, and its executive agencies and non-departmental public bodies (NDPBs), are externally assessed on an annual basis using the Information Assurance Maturity Model. During 2012/13, we developed and piloted an Information Management Maturity Model (I3M) to provide an evidence-based approach to assessing the Home Office's wider information management policies, procedures and practices. We plan to roll this out across the organisation in 2013/14. This model is aligned with both our knowledge and information management strategy[4] and the seven key Information Principles[5] which form part of the government's ICT strategy to which the Home Office is committed. These principles are hierarchical, with those at a lower level (such as information being recognised as a valued asset and managed accordingly) building up towards the final three principles that are integral to transparency and open data:

• information is re-used;
• public information is published; and
• citizens and businesses can access information about themselves.

The Home Office is committed to handling information as a valued and valuable asset. This applies to both an individual's personal data which must be held securely and protected from unauthorised access, and to ensure that the maximum value is derived from other data by

---

1 Examples of information that cannot be published include those that would impact on national or operational security, as well as those relating to the personal privacy of individuals, including the victims or witnesses of crime.
2 http://data.gov.uk/dataset/home-office-information-asset-register
3 The terms of reference for SIROs and IAOs in the Home Office are included at Annex A.
4 https://www.gov.uk/government/publications/home-office-group-information-management-strategy
5 http://www.cabinetoffice.gov.uk/sites/default/files/resources/Information_Principles_UK_Public_Sector_final.pdf

ensuring its re-use[6] within the department, across government, and wherever feasible, by the public and developer community. To support these twin objectives, we have developed a robust set of information policies[7], which reflect the lifecycle approach to information management. These policies are regularly reviewed, and align closely to the Information Principles.

The Home Office is committed to ensuring that public information is published in line with the public data principles[8], including the requirement to publish data free and in an open format to enable re-use, and in line with the requirements of the Open Government Licence.

During 2013/14, we also plan to explore ways in which we can move our work on transparency beyond the issue of 'open data'. For example, as part of the policy profession action plan, we will be developing a more open approach to policy making and engagement, which advocates enabling key stakeholders and the public to have a real opportunity to contribute to policy development, helping to define the problem and not just the solution.

---

6   Where appropriate the joint requirements of personal privacy and transparency can be met by means of anonymising data, or publishing data at a higher level of granularity to maintain anonymity.
7   High level information policies cover the creation, storage, use and disposal of information.
8   http://data.gov.uk/opendataconsultation/annex-2

2. Governance

Leadership of, and the ministerial drive for, transparency across the Home Office is provided by our Transparency Minister, Lord Taylor of Holbeach, who combines this role with his responsibility for disclosure and barring, criminality information, safeguarding vulnerable people, statistics and research, freedom of information and correspondence.

Within the Home Office, the governance of transparency and open data is aligned with that relating to information assurance and risk, and is managed within both the core Home Office and our executive agencies and arm's length bodies by our Senior Information Risk Owners (SIROs). They combine this role with that of Transparency Champion to ensure that information assets, data and issues relating to the management of these are considered in an integrated manner as 'two sides of the same coin', as well as meeting our legal obligations regarding the management of information[9].

The Home Office is working with its executive agencies and NDPBs to maximise their contribution to the transparency agenda, and the further development of this Open Data strategy.

The Home Office is a joint member, with the Ministry of Justice, of the Crime and Justice Transparency Sector Panel. This is chaired by Dr Kieron O'Hara from the University of Southampton and provides external scrutiny and challenge to our work on transparency in the crime and justice area.

This strategy will be updated as required to incorporate future developments regarding transparency, particularly those relating to open data. The requirements of the transparency agenda are incorporated into the Home Office business planning schedule when individual business units consider what new data they can publish, and other departmental processes such as the inclusion of the 'presumption to publish' in contracts and tender documents. During 2013/14, we will seek to also incorporate this into our guidance on programme and project management.

---

9   The Home Office has robust procedures in place to meet our legal obligations regarding public access to information, particularly relating to the Freedom of Information Act and the Data Protection Act.

3. Big Data

In line with the emerging trend as described in the Policy Exchange report on Big Data[10], the Home Office is moving from the broad brush approach of 'opening up data' to a more targeted approach. This focuses on publishing the big iconic datasets we hold that will capture public interest, and that will enable new products or services to be developed by data users. Datasets for publication are identified by business units across the Home Office and our executive agencies and NDPBs as part of a regular review of assets for the information asset register. Consideration of priorities will be included in the annual departmental business plan. Business units are also required to include their approach to transparency in their group business plans. Members of the public and developers are also able to request the release of data through data.gov.uk. We will consider such requests in line with the government's 'presumption to publish' all data that falls outside personal privacy, national and operational security considerations.

3.1 Crime mapping and other crime data

To date, the best example of Big Data within the Home Office is the national crime mapping website, Police.uk[11], which enables members of the public to access street-level information about crime and anti-social behaviour. This includes information on what happens after a crime has been committed, from police action to court outcomes. The website also provides contact details for neighbourhood policing teams and Police and Crime Commissioners, as well as details of forthcoming beat meetings and other engagement events. This information empowers communities to hold their local police and Police and Crime Commissioners to account. In addition, the public can use the website to access information about how their local police are performing, at both their local area level and at force level, as part of reforms to improve public accountability. Since its launch in January 2011, Police.uk has received over 53 million visits.

Police.uk has also received more than 5,000 items of feedback from the public about the site and development they would like to see, and recent developments reflect these. For example:

- from October 2011, the public has been able to access information about how their local police is performing against categories such as crime rates, quality of service and victim satisfaction, via the CrimeComparator tool on the website of Her Majesty's Inspectorate of Constabulary (HMIC);
- further crime categories were added to police.uk in October 2011, to provide more meaningful information and to align with other sources of crime statistics, such as HMIC. The public now has access to a more detailed breakdown of crimes in their area, such as criminal damage and arson, drugs offences and shoplifting, as previously reported in the "other crime" category;
- from January 2012, the number of points where crimes are shown on Police.uk were doubled to provide an even greater level of information and the website now shows all incidents of crime and anti-social behaviour recorded at all train stations;
- January 2012 also saw the start of the process to map incidents which occurred on or near a range of locations such as shopping areas, nightclubs, hospitals and parks to provide the public with more information and context about where crime is occurring in their local area;

---

10 http://www.policyexchange.org.uk/images/publications/the%20big%20data%20opportunity.pdf
11 http://www.police.uk/

- since October 2012 Police.uk has also provided more locally-specific information through its Compare My Area tool, which allows the public to compare crime rates in their local area[12] with other similar areas, and to see how crime rates in their local area have changed over time;
- in November 2012, crime and anti-social behaviour data was added for the Police Service of Northern Ireland (PSNI);
- from January 2013 the public have also been able to 'draw their own area' on Police.uk crime maps, enabling them to tailor the information provided by the website to their precise area of interest, rather than relying on a standard one mile radius from a given postcode. Police.uk also now provide 'See Your Stats' –which displays a pictorial summary of the crimes, anti-social behaviour and outcomes, for the user's drawn or postcode area. This enables them to see visually the breakdown of different crime and outcome categories month on month;
- from April 2013, the website includes key information which Police and Crime Commissioners are required by law to publish, including salaries, office budgets, and Police and Crime Plans; and
- the Application Programming Interface (API) has been opened up to over 1,500 developers and a number of applications have been developed using this data, including Crime Finder, which uses augmented reality to give the user a visual sense of the crimes around them. The apps page on Police.uk shows further examples of apps built using the data accessible through the Police.uk website.

3.2 Equality data

The cross-government lead on equality, the Government Equalities Office (GEO) has now transferred to the Department for Culture, Media and Sport, who will be including equality data in future updates to their Open Data Strategy. This topic has therefore been removed from the Home Office Open Data Strategy.

Within the Home Office, our Strategic Diversity Action Team and Human Resources teams, work with business partners across the Home Office and its agencies, on our equality objectives. These objectives, together with information that demonstrates how the department is considering equality in its policy and decision making, have recently been published on the Home Office website. This is the culmination of three years' work to improve data quality, analysis and reporting. The annual Employment Monitoring Report for 2011/12 has been significantly extended to include all monitoring activities across HR areas of responsibility (rather than reporting by exception as was the case in the previous two years' reports). In addition, and for the first time, supporting data sets have been published in line with the department's commitment in the Open Data Strategy.

3.3 National Statistics

A significant and growing amount of Home Office data is now published and can be referenced from both the Home Office website and UK National Statistics Publication Hub maintained by the Office of National Statistics (ONS). Much of this data can rightly be regarded as Big Data, in particular data such as our crime and migration statistics fall into this category. The coverage and publication schedule for these statistical releases is decided by the Home Office Chief Statistician. Data published on the Home Office website, both National Statistics and other information, can also be found via data.gov.uk.[13]

Home Office Statistics already publish a wide range of data on crime, policing, drug seizures, terrorism, animal science, alcohol licensing and migration.
As recommended by the National Statistician in her recent review, from April 2012 responsibility

---

12 Community Safety Partnership area
13 http://data.gov.uk/

for publication of crime statistics moved from the Home Office to the ONS, with ONS also being responsible for the 'Crime Survey for England & Wales'. The Home Office has retained responsibility for the collection and validation of the Police Recorded Crime series and works closely with ONS to support them in producing National Statistics publications on crime that bring together both series.

Also retained are the maintenance of the Home Office Data Hub, Home Office Counting Rules and support to National Crime and Force Crime Registrars (including the arrangements to identify the data statutorily required under the Police Annual Data Requirement (ADR)), as well as statistics on detections, recorded crime open data sets, hate crime and commercial victimisation data.

3.4 Migration data

Home Office Statistics (Migration Statistics) publish the quarterly National Statistics on immigration. Topics covered include: Work; Study; Family; Before Entry; Admissions; Extensions; Settlement; Citizenship; Asylum; Removals and Voluntary Departures; European Economic Area; and Detention. Following consultation with users, a new format for data release that provides detailed data broken down by individual nationality has been introduced. This has been welcomed by key users as a huge improvement on what was previously available.

Migration data is also published by the Home Office as part of its transparency framework indicators, and via the regular supply of information to the Home Affairs Select Committee (HASC). Other departments also publish data on a range of migration related topics – for example, national insurance numbers issued to migrants (Department for Work & Pensions, DWP), the labour force survey (DWP) and immigration / emigration patterns and trends (ONS) - which can usefully be used in combination with this data. Close collaboration between departments has resulted in the cross-referencing of data between different outputs, resulting in more coherent reporting.

Home Office Statistics continues to expand on the detail of the data currently published and also publish new sources of data. For example, publication of a more detailed breakdown of types of visa issued by nationality in the "Before Entry" topics was introduced in early 2012, and more detail on removals and voluntary departures was published later in the year. Home Office Statistics has also published new sources of data (for example certificates of sponsorship issued to migrants).

More generally, data will be systematically released in response to regular demands for particular information through freedom of information requests, parliamentary questions and other requests. The Home Office is analysing data from such sources with a view to categorising these into common themes, and identifying potential new data for publication, or integration into existing publications.

3.5 Scientific and social science data

In addition to scientific data that is published as National Statistics, Home Office Science also publishes social science research reports, and the underlying data within these is published in open format. Home Office Science is also actively exploring what further data it holds that can be published, commensurate with the needs of national security and personal privacy. The Home Office regularly publishes information about the records held on the National DNA database. We plan to release more details including figures on the retention of convicted people's DNA profiles and the removal of profiles taken from the innocent. We are investigating adding DNA match information to this dataset so that the public can make their own informed assessments of DNA retention.

Home Office Science also ensures that independent scientific advice from scientific advisory committees is made available on our website.

Other datasets produced by Home Office Science are already published in the UK Data Archive, which is accessible on registration by individuals and researchers; during 2013/14, we intend to extend this access by publishing this data more widely on data.gov.uk using the Open Government Licence where possible.

3.6 Administrative data

The Home Office publishes monthly spend data regarding financial expenditure over £25,000 and items purchased using the Government Procurement Card (GPC) over £500. We also publish data on salaries for individual members of the Senior Civil Service at Director level and above, plus aggregate salaries and details of the remit of teams below that level. In addition, we publish monthly workforce information[14], provide Cabinet Office with data relating to subjects such as grants and procurement, which are consolidated with returns from other departments and then published. We are now publishing the underlying data to our annual Employment Monitoring Report[15], and are exploring the feasibility of increasing this to include quarterly sick absence information as well as some People Facts information, with the proviso that this does not breach an individual's right to privacy under the Human Rights and Data Protection Acts.

---

14 http://data.gov.uk/dataset/workforce-management-information-home-office
15 http://data.gov.uk/dataset/employment-monitoring-report-home-office

4. My Data

My Data is information held by the Home Office and its related organisations which can potentially be made available to the individuals to whom it relates, with the facility for individuals to correct data, if appropriate, without the need to make subject access requests. At a basic level, this data may simply be individual names and addresses, but at a more advanced level it could include details of transactions between the individual and the organisation, and advice as to when particular services will be received.

The processes for the release of personal data must be robust, reliable, secure and reflect legal obligations regarding access to such data; the Home Office approach to this will accords with requirements in the Open Data white paper[16]. In particular, these processes must ensure that data is only released to those who have a right to the data, normally the individual to whom it relates.

Data held by the Home Office Group which could potentially be made available to enable members of the public to search for and access their own data includes:

- Identity & Passport Service (IPS) – a passport applicant using the new online channel (available during 2013) will be able to view the status of their application online;
- security industry applications – the Security Industry Authority (SIA) is introducing a facility for applicants to receive updates regarding the progress of their applications via text message, if they wish. Similar information is available to organisations who have submitted applications on behalf of their employees; and
- the Home Office plans to increase the range of information about their activities and performance which is available to the public. They will also explore whether it is possible to allow sponsors, employees and other citizens to interact with their systems. A steering group has been established to provide oversight of this work, and engage with relevant parts of the organisation.

The units identified above will be considering the feasibility of enabling the public to access their own data as described above within the lifetime of this Parliament.

The Disclosure and Barring Service, DBS (formerly the Criminal Record Bureau and Independent Safeguarding Authority) already provides details on request on the progress of disclosure applications and referrals to both the individual and to lead/counter signatory. Requests can be made either by telephone or online. Similarly, disclosure numbers are provided on request to the individual. In exceptional circumstances, application forms and copies of the DBS check may be provided to lead/counter signatories when requested in writing (e.g. for court purposes), although exemptions to this may apply. After spring 2013, volunteers and employees will no longer need to apply for a new criminal records check each time they apply for a new job if they subscribe to the 'Update Service'. The new service will allow an organisation to carry out an online status check, with the individual's consent, to establish if any relevant criminal information has been identified since the individual's DBS Check was last carried out. An employer or organisation, when presented with a DBS certificate, will be able to log on to the Update Service where they will need to enter key details. They will then be presented with a status update in relation to that individual's

---

16 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf

criminal record status. The Update Service will not automatically alert an employer or organisation if an individual's status changes. The onus is on the employer to conduct status checks as frequently as they require in line with their own policies.

5. Satisfaction and Experience Data

This is data which provides an insight into customer satisfaction with Home Office services and the customer experience. This data helps us analyse and address concerns of users, customers or other stakeholders and improve our services. It includes both figures collected directly by the Home Office and its associated organisations and data collected by others on our behalf.

Details of actual data already held will be made available to the public in line with the public data principles. Possible data includes:

- passport delivery data:
  - performance reporting on customer service is assessed through customer satisfaction surveys which run a minimum of twice a year; and
  - customer intelligence findings about customer behaviour and expectations are published as collected.
- DBS Disclosure publishes data regarding the time to complete checks and the customer experience of the process, by both individuals and organisations. This data is included in the IPSOS MORI research reports along with the DBS performance figures, which include customer service, and police performance standards;
- crime mapping: since its launch in January 2011, the Police.uk website has received over 5,000 items of individual feedback, primarily via the site survey. We continually review user feedback to assess how we might improve the site. We have also opened up the raw data underlying the website to more than 1,500 developers. and in early 2013 we will be setting up a web forum to improve our engagement with developers and others who wish to use Police.uk data and ensure that the data provided is as user-friendly as possible; and
- if public opinion polling is commissioned within the Home Office, then the outcomes will be published.

Data regarding some aspects of customer satisfaction are already published. For example, figures relating to complaints against the police are published by the Independent Police Complaints Commission (IPCC); details of the percentage of passports delivered to target by IPS; and the clearance of passengers through the border are published as part of the impact indicators agreed in our 2011/12 business plan.

In addition to National Statistics on migration, published by Home Office Statistics, the Home Office also publishes information about its transparency indicators, its asylum system and its performance in dealing with customer complaints and correspondence. This data includes details of the percentage of migration applications decided within published standards, and the cost of these.

6. Creation of dynamic Information Markets

This aspect of transparency relates to work with external stakeholders, including developers, academics, voluntary organisations and the business community, to maximise the use of public data and the benefits derived from this. This work will build on existing relationships, for example with members of the Crime and Justice Transparency Sector Panel, set up by the Home Office and Ministry of Justice, and chaired by Dr Kieron O'Hara, which provides external challenge, support and advice in shaping the work on transparency in the criminal justice system. We will also be working closely with the Open Data Institute, following its launch in December 2012.

Relevant work relating to this aspect of transparency includes:

- opportunities which transparency and open data present to support the Home Office in meeting its objectives. For example the Home Office is exploring the feasibility of using an 'open policy making' approach to develop effective policies on preventing fraud and corruption, strengthening the rule of law and increasing deterrents;
- participation in events and initiatives which enable engagement with developers and other stakeholders (e.g. UK GovCamp, hack days, the Crime and Justice Transparency Sector Panel, and the Open Data Institute's "Immersion Programme" for developers). We continue to work with data developers and social media entrepreneurs to identify more ways to drive transparency and culture change;
- we will be working closely with the Open Data Institute to consider with developers and other interested parties what more we can do to stimulate a dynamic and creative market in crime and justice data;
- work with 'trailblazer' areas across the country, which build on the success of Police.uk, to drive even greater transparency across crime, policing and justice at a local level. This involves commissioning research to better understand public and practitioner experiences of local innovations. We are currently working with West Yorkshire police to publish details of local offenders on Police.uk. The 'In the Dock' initiative, which is currently being piloted, provides the public with some offenders' details, including photograph, name, offence and sentence. We are looking to extend this initiative to further forces during 2013. We will also be working with North Yorkshire police to help them map CCTV images of crime suspects onto Police.uk crime maps, and Surrey Police to explore the use of QR codes to drive up community engagement and the reporting of crime and anti-social behaviour;
- our commitment to publishing the underlying data which supports Police.uk has led to some exciting innovations including the trailblazing app Surrey Police Beat,[17] which allows Neighbourhood Police Teams to 'tweet on the beat'. In addition, SafeTrip,[18] one of the winners of Silicon Valley Comes to the UK Appathon, uses the Police.uk API to calculate a statistically safe route home. Further examples can be viewed on the Police apps[19] page on Police.uk;
- work with other government departments to maximise re-use of data, e.g. Cabinet Office/HM Treasury regarding the use of spend, organogram, salary and workforce data. For example, IPS shares data with other government departments including DWP and the Department of

---

17 http://itunes.apple.com/gb/app/surrey-police/id451120732
18 http://itunes.apple.com/us/app/safe-trip/id436319378?mt=8
19 http://www.police.uk/apps?q

Health as well as law enforcement agencies to help in the prevention of fraud and identity related crime. Passport validation services are also provided by IPS to the legal and financial services sector to help prevent money laundering and detect fraud. In addition, IPS shares civil registration data with ONS for statistical and administrative purposes; and

- this work may include progress on the linking of different datasets, where demand from the user or developer community highlights this requirement. It will also include work to publish reference data, where this is needed.

7. Improving the quality of data

The continuous improvement of data quality is important in driving forward the benefits of transparency, as well as increasing public confidence in government data. Home Office work on this will build on previous work to ensure that data published by the Home Office is fit for purpose, and is described, recorded and communicated consistently.

The Home Office is committed to publishing data in open format, and has policies and guidance in place to support this. The Home Office is now in the process of standardising on the use of Open Document Spreadsheets (ODS) for the publication of data. This format has been selected as the one that maximises the usability of data for both computer and human use, whilst maintaining the commitment to publish in an open, re-usable, non-proprietary format. The move to publishing in ODS will be managed on a progressive basis as new data is published, or existing data updated.

Data is published on the most appropriate website for the subject matter concerned (for instance, the Home Office website or Police.uk) and digital continuity is provided through the application of guidance produced by The National Archives. Published data is also linked from data.gov.uk, which is used as the principal mechanism for promoting re-usable data published by the Home Office. We have a documented process on opening up government data, and review this on a regular basis to ensure that the need to publish data to open standards and on an appropriate technology platform is included at an early stage in the publication process. We will work with other government departments during 2013/14 to ensure that the transition to GOV.UK as the single domain for government information operates smoothly in relation to the accessibility of Home Office data currently on data.gov.uk.

As part of its regular programme of monitoring and assessment, the UK Statistics Authority assessed the Home Office's crime statistics and confirmed their re-designation as 'National Statistics'. (Responsibility for these subsequently moved to ONS in April 2012). Implementation of the recommendations of the independent National Statistician's review of crime statistics is intended to lead to further improvements to improve the public's understanding of official crime statistics, and their confidence in them. During 2011, Her Majesty's Inspectorate of Constabulary (HMIC) conducted a review of police crime and incident recording. The results of that inspection were published in January 2012. Assurance of the integrity of police recorded crime figures will continue to be part of the Inspectorate's work programme. The assessment of immigration statistics[20] is complete and the UK Statistics Authority has assessed and confirmed their re-designation as 'National Statistics'. Assessments and confirmation of animal science and policing statistics have been completed and re-accreditation is expected after implementation of a limited number of requirements.

To further improve the quality of the data underlying Police.uk, during 2013/14 we will work with the Open Data Institute to provide technical support to forces with a view to further improving data processing and ensuring that any changes which might affect historic data are captured, recorded and clearly explained to data users. We will also establish a web forum so developers can post and receive prompt and open replies to queries about Police.uk data.

---

20 http://www.statisticsauthority.gov.uk/assessment/assessment/assessment-reports/report-177---statistics-on-immigration.pdf

Work will also be undertaken to further embed the application of the Public Data Principles, and the Information Principles, which have recently been published as part of the government ICT strategy, into the way that the Home Office works in terms of its processes, policies and procedures.

8. Privacy issues relating to the publication of data

The Home Office is committed to ensuring the fundamental rights of individuals to privacy, and to maintaining an appropriate balance between the government's 'presumption to publish' data and this 'individual right to privacy'. This balance is achieved by:

- governance structures, in particular the role of SIROs in assessing and monitoring information risks within the organisation and ensuring that these are addressed. Inclusion of both information assurance and transparency in the corporate Governance Statement by the Permanent Secretary, as the Home Office Accounting Officer, means that this commitment is led from the top of the office;
- external engagement with privacy experts, in particular the Chair of the Crime and Justice Transparency Sector Panel. The Information Commissioner's Office is also represented on this panel;
- Privacy Impact Assessments (PIAs), which are required when significant datasets are to be published, to ensure that personal data is not released, and that appropriate anonymisation processes are in place when considering the release of datasets containing personal data. The guidance on PIAs will be reviewed during 2013/14 in light of the recent publication of the ICO Anonymisation Code of Practice;
- training: annual training on information assurance is mandatory for all staff in the Home Office. The training was updated in 2012/13 to include consideration of data which can be published, and what cannot, to support the government's transparency agenda; and
- agreed sign-off procedures at an appropriate level within business units for data releases, including where necessary, sign-off by ministers.

Annex A: Terms of Reference for Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs) in the Home Office

SIRO Terms of Reference:

Role

The Home Office Senior Information Risk Owner (SIRO) is a member of the Home Office Board who has responsibility for ensuring that information risks are managed appropriately, balancing this with the requirement to make public data open and re-usable. The SIRO is accountable to the Permanent Secretary and is required to submit an annual report providing an assessment of information risks in the Home Office.

Responsibilities

The SIRO is responsible for leading and fostering a culture that values, protects and uses information for the public good. This includes:

- ensuring that the department has a plan to achieve and monitor the right culture, across the department and its partners, balancing the requirements of the effective management of information risks and the benefits of greater transparency of public data;
- taking visible steps to support and participate in that plan (including completing own information assurance training);
- ensuring that the department has Information Asset Owners (IAOs) who are skilled, focussed on the issues, and supported; in addition to any specialists the department needs.

The SIRO owns the overall information risk policy and risk assessment process, tests its outcome, and ensures that it is used effectively. This includes:

- ensuring that the risk policy comprehensively provides for the department to implement at least the minimum mandatory compliance measures in force from time to time; that it covers its own activity and that of its delivery partners; and specifies how compliance will be monitored;
- ensuring that a departmental risk assessment is completed at least quarterly taking account of extant Government-wide guidance (as provided by the Cabinet Office) and of a threat assessment provided by DSU;
- taking account of the risk assessment, understanding the information risks carried by the department through its delivery chain; ensuring that they are addressed, and establishing that they inform investment decisions;
- ensuring that risk assessment and actions taken in mitigation benefit from an adequate level of independent scrutiny;

- considering any requests from the department to deviate from the policy (the SIRO is the only person who may approve deviations).

The SIRO leads within the Home Office in championing greater transparency of public data. This includes:

- providing advice to the Home Secretary, ministers and the Home Office Board on the implications of transparency initiatives for the Home Office;
- responding to requests for greater transparency from other government departments, and the public;
- ensuring that all business units within the Home Office assess data within their control based on the assumption of transparency;
- oversee the transparency section in the Home Office business plan and ensure delivery of this.

The SIRO is responsible for advising the Accounting Officer on the information risk aspects of his statement on internal control. This includes:

- receiving an annual assessment of performance, including material from the IAOs and specialists, with reference to Government minimum mandatory measures as well as department-specific measures;
- providing advice to the Accounting Officer on the information risk elements of the statement on internal control;
- sharing assessment and supporting material with Cabinet Office, to support cross-Government work in this area.

Relationship with Agencies and NDPBs

Agencies and NDPBs are responsible for their own information risk management arrangements and input to the government's Transparency Agenda. They are required to comply with:

- the Home Office Risk Management Policy and Guidance (HORMPG);
- the Home Office Information Risk Management Policy and Guidance;
- the Home Office policy on Open Access to and Re-use of Public Data (draft).

The Chief Executive or Chair (depending on the constitution of the Agency / NDPB) is accountable to the Home Secretary and Permanent Secretary for the work of their organisation, including transparency and information risk management. The Chief Executive may appoint their own SIRO to support them in this.

The Home Office SIRO will include in their report to the Permanent Secretary, the information risk associated with the Home Office family which includes its Agencies and its NDPBs. The process for this will be in accordance with the HORMPG and the working arrangements set up for the sponsorship of Agencies and NDPBs. Thus:

- Agencies and NDPBs will have a sponsor or sponsor unit in the Home Office responsible for managing the relationship with that body. The sponsor is responsible for understanding the Agency/NDPB's most significant risks and risk management capability. Where appropriate, the sponsor will escalate these risks within the Home Office in accordance with the HORMPG;
- IPS does not currently have a Home Office sponsor unit. However, for risk management (including information risk) the Performance and Delivery Unit will fulfil the sponsor function.

References

"Managing Information Risk: a guide for accounting officers, boards and SIROs" The National Archives. March 2008

"Working in Partnership for a Secure and Resilient UK Information Infrastructure". Cabinet Office CSIA. 2005

"Public Data Transparency Principles". www.data.gov.uk

Home Office
OCIO
March 2011

IAO Terms of Reference:

Role

Information Asset Owners (IAOs) are senior people involved in running a relevant business area which uses a registered Home Office Information Asset. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO annually on the security and use of their asset.

Responsibilities

Lead and foster a culture that values, protects and uses information for the public good

- understand the Home Office's plans to achieve and monitor the right culture, across the Department and its partners;
- take visible steps to support and participate in that plan (including completing own training);
- participate in and contribute to activities of the IAO community, identifying best practice and opportunities for continuous improvement.

Know what information is held in the asset, and what is added and removed and how

- keep understanding of the asset and how it is used up to date;
- approve and minimise transfers while achieving the business purpose;
- approve arrangements so that information put onto removable media such as disks or laptops is minimised and protected appropriately with approved encryption methods where required;
- approve the disposal mechanisms for paper or electronic records from the asset, in accordance with DSU guidance.

Know who has access to the asset and why, and ensure their use of it is monitored

- understand the Home Office's policy on use of the information;
- be aware of and understand relevant statutory requirements with regard to handling information;
- check that access provided is the minimum necessary to achieve the business purpose;
- consider requests for access to information from other business users, and maintain log of requests and decisions;

- receive records of checks on use and assures self that they are being conducted;
- report breaches promptly in accordance with HO procedures.

Understand, identify and control risks to the business in relation to their asset(s), and provide assurance to the SIRO

- contribute to implementation of the Information Risk Management Policy in their business area;
- contribute to the department's risk assessment;
- provide an annual written assessment to the SIRO on the use and security of the information assets they are responsible for and the information they hold;
- make the case where necessary for new investment to secure the asset.

Ensure the asset is fully used for the public good, including responding to requests for access from others

- consider whether better use of the information could be made;
- receive and log requests from others for access;
- ensure decisions on access are taken accordingly.

Further guidance on carrying out these responsibilities is available via the IAO Toolkit on the Information Assurance Programme website.

Annex B: List of data to be released for first time 1 April 2012 to 31 March 2014

Dataset Name	Description of data (including fields)	To be first published on (i.e. date, including month and year)	Frequency of update (e.g. monthly, quarterly, annually)	Issued under the Open Government Licence (OGL) Yes or No[21]	Notes
Beat meeting engagement	People engaging with local beat meetings	Done [first published November 2012]	Quarterly	Yes	Published in ONS Focus on Perceptions.
Costs of crime	Estimated scale and costs of organised crime to the UK, broken down by crime type (drugs, fraud, etc)	2013/14	One-off publication	Yes	Publication delayed due to complexity in data and the need to ensure it is robust.
Disruption of crime	Number of substantial disruptions to organised crime groups in the previous 3 months	2013/14	Quarterly	Yes	Publication delayed due to need to reach agreement with all law enforcement partners in defining what counts as disruption, and resolution of data quality issues.
Hate crime	Hate crime offences	Done [first published September 2012]	Annual	Yes	
Police action after crime	Police. uk updated to include information on what happens after a crime has been committed in terms of police action and court outcomes	Done [first published May 2012]	Monthly	Yes	
Equal Civil Marriage	Response to public consultation on same-sex marriage	End 2012	One-off publication	Yes	Responsibility transferred with the Government Equalities Office to Department for Culture, Media and Sport.

Dataset Name	Description of data (including fields)	To be first published on (i.e. date, including month and year)	Frequency of update (e.g. monthly, quarterly, annually)	Issued under the Open Government Licence (OGL) Yes or No[21]	Notes
Sick absence information	Sick absence information reported quarterly to Cabinet Office. Includes breakdown of sick absence by long and short term sick, cost of sick, staff employed during the period, staff with no sick together with a breakdown by: geographic region, gender, grade, and absence reason.	Autumn 2013	Quarterly	Yes	Publication delayed until Autumn 2013 due to complexity of automatic redaction of information to comply with the Data Protection Act; to ensure that any small numbers published are not disclosive.
People Facts	Exploring the feasibility of further publication of management information including workforce planning, sick absence and equality and diversity data.	Autumn 2013	Monthly	Yes	Publication delayed until Autumn 2013 due to complexity of automatic redaction of information to comply with the Data Protection Act; to ensure that any small numbers published are not disclosive.

---

21 The OGL allows the public and business to, for free: copy, publish, distribute and transmit the Information; adapt the Information; exploit the Information commercially for example, by combining it with other Information, or by including it in their own product or application. The full licence can be found at http://www.nationalarchives.gov.uk/doc/open-government-licence

Annex C: Aspects of this Open Data Strategy that have been revised in relation to the previous version, published June 2012

General

Changes to reflect the reintegration of the UK Border Agency into the Home Office have been made throughout the document.

Section 1: Introduction

This has been updated to reflect the following changes:

- Information Principles especially relevant to Transparency, and work within the Home Office to assess compliance with these Principles as a whole; and
- plans to extend our work on Transparency beyond Open Data, for example in open policy making.

Section 2: Governance

This new section summarises the responsibilities for Transparency and Open Data with the Home Office.

Section 3: Big Data

This section has been updated to reflect the following changes:

- developments in Police.uk and future plans regarding this facility;
- the transfer of the Government and Equalities Office to the Department for Culture, Media and Sport;
- introduction of a new sub-section on migration data;
- introduction of a new sub-section on scientific and social science data; and
- the publication of the underlying data to the Home Office annual Employment Monitoring Report.

Section 4: My Data

The changes to the Disclosure and Barring Service (DBS, formerly CRB) relating to the introduction of a service that will enable individuals to use the same DBS check for more than one post or role has been added.

Section 6: Creation of dynamic Information Markets

This section has been updated to reflect the following changes:

- work with the Open Data Institute to stimulate a creative market in crime and justice data; and
- work with 'trailblazer' police forces to drive greater transparency and community engagement.

Section 7: Improving the quality of data

This section has been updated to reflect the following changes:
- transition of the Home Office website to GOV.UK;
- move to publishing Home Office data in Open Document Spreadsheet (ODS) format;
- assessment and re-designation of statistical datasets by the UK Statistics Authority; and
- work with the Open Data Institute (ODI) to improve data processing, in particular with regard to Police.uk.

Section 8: Privacy issues relating to the publication of data

This new section summarises steps the Home Office is taking to ensure an appropriate balance between the government's 'presumption to publish' and the individual's right to privacy.

Annex B: List of data to be released for first time 1 April 2012 to 31 March 2014

The table has been updated to reflect the current position regarding publication of datasets listed. A notes column has been added to enable the provision of explanatory detail where required.