CabinetOffice

Individual Electoral Registration

Privacy Impact Assessment Report

May 2012

Document information

Master location	:	Cabinet Office
File name	:	IER Privacy Impact Assessment Report
Distribution	:	Public Document
Author(s)	:	Narelle Lee, Victoria O'Neill

Version control

Version no.	Version date	Summary of change	Author
0.1	30/03/2011	Document drafting commenced	Narelle Lee
0.2	28/04/2011	Input from key stakeholders	Narelle Lee
0.3	04/05/2011	Comments from Programme SRO	Narelle Lee
0.4	18/05/2011	Input from key stakeholders	Narelle Lee
1.0	30/06/2011	Published alongside White Paper	Narelle Lee
1.1	28/03/2012	Document updated to reflect policy changes	Victoria O'Neill
1.2	12/04/12	Document sent to PBL Committee	Victoria O'Neill
1.3	10/05/12	Published alongside Electoral Registration and Administration Bill	Victoria O'Neill

Contents

Section 1 – Executive Summary

Background

Individual Electoral Registration (IER)

The coalition agreement contains a promise to "*reduce electoral fraud by speeding up the implementation of individual voter registration*"). This is a fundamental change to our system of electoral registration; it will improve accuracy, requiring electors to register to vote individually rather than by household. Before an individual can be added to the register, they will need to be verified through the cross checking of their information against trusted public data sources.

This change will make the system less vulnerable to fraud and provide an opportunity to support the completeness of the register by tackling under-registration. It is our intention to use data matching to allow Electoral Registration Officers (EROs) to compare their registers against other public databases. This will help to simplify the transition process for the majority of individuals, using the approach set out on page 7, and will potentially help to identify people not currently registered to vote, as well as providing a means of checking the accuracy of the register. Data matching pilots were carried out in 2011. The evaluation of these pilots highlighted a number of benefits of data matching as well as areas for further refinement. The lessons learned have informed the policy development detailed below and the second series of pilots, which, subject to Parliamentary approval, will take place over the next year.

Objectives

The objective is to speed up the introduction of IER in Great Britain during this Parliament to ensure that electoral registration is trusted and secure. Success will be measured by a reduction in the vulnerability to fraud after 2014 and an improved public perception of the security of electoral registration. IER should improve the accuracy of the register to allow us to address the current level of completeness and help people currently missing to get on the register.

Consultations

This policy has and will continue to be tested through ongoing consultation with various key stakeholders including the Information Commissioner's Office, Electoral Commission, Association of Electoral Administrators, Society of Local Authority Chief Executives, Electoral Registration Officers and groups interested in privacy issues. Consultations have also taken place with the Metropolitan Police, Association of Chief Police Officers, Serious Organised Crime Agency, HM Revenue and Customs and the Department for Work and Pensions. These proposals have also been subject to a full public consultation in summer 2011 and subjected to pre-legislative scrutiny.

Findings

The Privacy Impact Assessment (PIA) has found that there will be privacy impacts as a result of the implementation of IER due to:

- Introduction of individual rather than household invitations to register, so that individuals will not be required to share personal information with others when making an application.

- Transmission of current electoral registers to enable these to be cross matched against public data sources during the transition to IER.

- Collection of additional personal data for some electors (estimated to be approximately a third of those electors currently on the register) which they are not currently required to provide. All new applications for registration may require the collection of personal data.

- Transmission of data provided by an elector in response to an IER form, for the purposes of verifying an elector's entitlement before they are placed on the electoral register.

- Transmission of match reports and confirmation information from the verification service to an ERO.

- Retention and disposal of personal data collected for the purposes of electoral registration increases the risk of unauthorised disclosure.

- Introduction of a civil penalty for those who fail to make an application when invited to do so after an ERO has taken prescribed steps to encourage an application, including imposing a requirement to make an application by a specified date.

The Government is aware of the above impacts and the following mitigations are being put in place to address these:

- We are putting in place a system whereby electors on the register whose information can be verified through data matching (we estimate that this will be approximately two thirds of current electors) will not need to provide any additional information during the transition to IER.

- Additional personal data collected will not form part of the electoral register – the information currently captured on the register will remain the same.

- There will be no new national database created as a result of implementing IER.

- A wet signature will no longer be required when an individual makes an application to register to vote.

- A data management policy has been developed which will set out clear rules on the storage, use, transmission, retention and disposal of personal data. This will be a living document and will be updated to reflect all relevant policy developments.

- The solution for the storage and transmission of the personal data is still being developed, but the necessary design features to securely, move and store personal data if necessary will be a requirement of any solution implemented for this purpose.

- Continued engagement with key stakeholders to ensure security of personal data and appropriate risk and impact assessment and mitigation.

- Proposed new offence for the disclosure of personal data provided by an applicant in their electoral registration application, or the information provided by any entity in the verification process to any person not involved in the process.

It is important to note that any impacts will necessarily need to be balanced against security and fraud concerns and that both impact and mitigation strategies will continue to be developed.

Recommendation

It is recommended that consultation with key stakeholders and the public continues to fully understand the privacy impacts – particularly following the new approach to simplify transition and the introduction of a civil penalty for individuals who fail to make an application when required to do so after an ERO has taken prescribed steps to encourage an application - and to enable us to continue to develop appropriate mitigation strategies. It is intended that this PIA will be a living document and will continue to develop over the period of policy development and implementation.

Review Process

This Privacy Impact Assessment will remain under review throughout the passage of the Bill to ensure that it takes into account any amendments.

Section 2 – Introduction

Background

A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. The primary purpose of a PIA is to visibly demonstrate that an organisation acts responsibly in relation to privacy. The deliverables and benefits of undertaking a PIA can be summarised as:

- identification and management of risk;
- avoidance of unnecessary costs;
- prevention of inadequate solutions;
- avoiding loss of trust and reputation;
- informing citizens and partners of the organisation's communications strategy;
- meeting and exceeding legal requirements.

Objective

The objective of conducting this PIA is to identify any data protection issues with the proposed system of Individual Electoral Registration. It is important to remember that ultimately the focus of a PIA is compliance with the Data Protection Act (DPA). However, compliance with any other relevant legislation should also be considered.

Underlying principle

Data collection, sharing and testing must be undertaken within a clear legal framework, with any intrusion upon an individual's privacy to be kept to a minimum. The Electoral Registration Transformation Programme is undertaking this PIA to ensure this principle is met.

HMG requirement

The Data Handling Review, published in June 2008, states that all Departments will "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start, and those planning services are clear about their aims. Similarly, information risk management will be considered as part of the Government's "Gateway" reviews that monitor progress of the most important projects". The Data Handling Review has now been subsumed into HMG Information Assurance Standard No 6 – Protecting Personal Information and Managing Information Risk.

PIA Process

The process for conducting a PIA is described by the ICO as follows:

1. Initial assessment (i.e. the Screening Process) – Examines the project at an early stage, makes an initial assessment of privacy risk and decides which level of assessment[1] is necessary. This has been undertaken and the assessment is referenced in this report.

2. Where necessary, conduct either:

    - Full-scale PIA – a more in-depth internal assessment of privacy risks and liabilities. It includes the need to identify stakeholders, analyse privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them; or
    - Small-scale PIA – Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project.
    - Review – Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should result in an updated PIA.

This report deals with the PIA for Individual Electoral Registration. The screening process identified that a Full Scale PIA is required.

[1] Full Scale PIA, Small Scale PIA or no PIA.

Section 3 – Individual Electoral Registration

Overview

What is Individual Electoral Registration (IER)?
The coalition agreement contains a promise to "*reduce electoral fraud by speeding up the implementation of individual voter registration*". This is a fundamental change to our system of electoral registration; it will improve accuracy, requiring electors to register to vote individually rather than by household. One of the findings of the data matching pilots carried out in 2011 was that when the pilot areas cross matched their electoral register against trusted public databases an average of 66% of entries can be confirmed to a sufficient degree of certainty that we can verify an individual's information as accurate. Based on this evidence, a new approach has been developed to simplify the transition to IER for the majority of individuals. This is something we are minded to introduce, subject to further testing in the second set of pilots. Under the new approach, all electoral registers will be cross matched against trusted public data sources. Those electors whose entries on the register can be individually matched will be confirmed as entries on the new IER register and will need to take no further action (there will continue to be individual registers held for each Local Authority rather than a central register being created). Those individuals whose information cannot be matched will receive a personally addressed invitation. In returning this, they will be asked to provide information which will be used to verify that they are a genuine person and entitled to be registered. Only once a person has been verified can they be added to the register. This will also apply for new applications made during and after the transition period has finished around 1 December 2015. It must be noted that a person's ability or inability to present certain personal information for the purposes of verification is not a determining factor of their right to register e.g. if a person does not have a National Insurance Number it will not prevent them being able to register to vote as alternative methods of verification will be available.

The White Paper on IER set out the proposal that when invited to register to vote, an individual could indicate that they did not wish to be chased again during that canvass period. This led to concerns about a potential drop in the register. Following the pre-legislative scrutiny, and having also taken the concerns of those responding to the public consultation into account, we have decided to remove this 'opt-out' proposal. In addition, to ensure the completeness and accuracy of the register, a civil penalty will be introduced for those who fail to make an application when required to do so, after an ERO has taken prescribed steps to encourage an application, including imposing a requirement to make an application by a specified date.

The change to IER will make the system less vulnerable to fraud and provide an opportunity to support the completeness of the register by tackling under-registration. It is hoped that, in addition to using data matching to verify an individual's information, it will help identify people not currently registered to vote,

in particular specific target groups including attainers, students and home movers, as well as providing a means of checking the accuracy of the register. This is being tested further as part of the second wave of data matching pilots. We acknowledge that the introduction of a civil penalty could be seen to change the privacy impact of using data matching to identify those not currently on the register. However, the introduction of a set of prescribed steps an ERO must follow before a civil penalty can be issued will limit the amount of people who become liable for a penalty and will also ensure that it is only those individuals who persistently refuse to make an application who are liable to pay a fine. Our position remains that we will not criminalise those who do not register to vote and the civil penalty will bring the advantage of retaining a threat of a financial sanction on an application form without the introduction of a criminal offence for those who choose not to individually apply.

The provisions in the Political Parties and Elections Act 2009 (PPE Act) provide for the phased introduction of IER on a voluntary basis from 2011, although it would not allow IER to become compulsory before the 2015 general election. The current proposal would see the implementation of IER occur in 2014, prior to the 2015 general election and the voluntary phase outlined in the PPE Act abolished.

What is the main purpose for introducing IER?
The objective is to speed up the introduction of IER in Great Britain during this Parliament to ensure that electoral registration is more trusted and secure. Success will be judged by a reduction in the vulnerability to fraud after 2014 and an improvement in the public perception of the security of electoral registration. IER should improve the accuracy of the register, allow us to address the current level of completeness and help people currently missing to get on the register.

Screening Process
A formal screening process was conducted on 30 March 2011, which identified that a full scale PIA should be undertaken. A full impact assessment, including a PIA, for IER was published alongside the White Paper and draft legislation on 30 June 2011. This can be found at http://www.cabinetoffice.gov.uk/resource-library/individual-electoral-registration-draft-bill. It should be noted that work to identify and mitigate privacy impacts has been underway since the policy began to be developed and has continued since that time.

Previous Impact Assessments
A general small scale Impact Assessment dated 20 July 2009 was conducted for the Royal Assent stage of the Political Parties and Elections Act 2009. This provided an overview of the impacts of the previous government's proposals for the introduction of IER and included brief information regarding privacy impacts. This is available to view or download at http://www.ialibrary.berr.gov.uk.

Business case

What data will be collected?

The data will be collected from those electors whose information cannot in the transitional period be verified through the cross checking of the electoral register against trusted public data sources and those making IER rolling registration applications both during and after the transitional stage. The information to be collected will be:

- Full name (first name, middle name or initial(s), Family name)
- Full residential address including postcode
- Nationality
- Declaration of truth – declaration that all information provided is true and correct.

- Date of birth (new requirement)
- National insurance number (NINO) – where possible (new requirement)
- Immigration status – if non-British or non-EU citizen (new requirement)
- Declaration as to whether they are/have been registered elsewhere in the last 12 months (new requirement)
- Previous address where registered in the last 12 months (new requirement – currently requested but not mandatory on annual canvass forms)

Information of a sensitive nature will be collected on individual forms – this includes date of birth, national insurance number, nationality and immigration status.

It is important to distinguish between franchise and eligibility, and verification. Information such as nationality and immigration status are required to determine a person's franchise and eligibility whereas other information such as date of birth and national insurance number will be used specifically for verification purposes.

It is important to note that although additional information will be collected, this will be used for processing the electoral registration application only and <u>will not</u> form part of the electoral register. The information currently captured on the electoral register will remain the same.

Through data matching, EROs will be sent name, address and date of birth information which will be taken from a range of public databases.

Why is it being collected?

The system for registering to vote in Britain has remained constant since the early twentieth century. Electors register to vote through the annual canvass of households conducted by the ERO in the autumn of each year, although since 2001 electors have also been able to register through rolling registration at any time throughout the year.

Aside from the other drivers for the move to IER, it is desirable as a matter of principle that a person's ability to vote is not dependent on whether another person has placed their name on a form for them. The household registration

system is increasingly outdated and Britain is almost unique in continuing this system. Whilst individuals can register in year using the rolling registration system, only a small proportion of people do so (approximately 2% per annum) and households are required by law to respond to the annual household canvass.

IER will improve a person's ability to keep their personal information private, as one person in the household will no longer require the information from other occupants in order to complete an electoral registration form. This is particularly the case in houses of multiple occupation, where occupants are less likely to be family members and potentially less comfortable with sharing information within the household.

Data matching to find people is being pursued to increase the accuracy and completeness of the register.

Reducing Fraud

While proven electoral fraud is rare, any fraud undermines public confidence. The current system of electoral registration is unacceptably exposed to the risk of fraud and this is why the coalition government agreed to speed up the introduction of individual registration to improve security. From 2014, any person wishing to apply to be included in an electoral register who has moved, is registering for the first time or has changed their name will be required to provide additional information to the electoral registration officer so that this can be cross checked and the application verified. Subject to further testing, we anticipate that the majority of existing electors will be confirmed through the cross matching of electoral registers against trusted public data sources. Those whose information cannot be confirmed will be required to provide additional information to enable their application to be verified.

There remain a significant number of people who perceive fraud to be a problem (36% of people surveyed for the Electoral Commission's public opinion research 2011[2]) and this can have a corrosive effect on trust in our political system.

A key vulnerability in the system is the fact that the household canvass does not require any evidence to prove that the persons listed on the form are real, reside at the property, or that they are not registered elsewhere. Outside of the annual canvass, electors may register to vote by way of rolling registration which requires each eligible elector to complete and submit a form to their ERO. Again, there is no requirement to verify the person trying to register. This has led to accusations that large numbers of alleged fraudulent rolling registration forms are being submitted close to the poll and in a number of cases, the Police have successfully prosecuted people for doing so.

---

[2] TNS-BMRB public opinion research findings winter 2011 (Electoral Commission, March 2012)

IER will tackle these sources of fraud by introducing a requirement for people to register individually and for EROs to verify aspects of the entitlement of the person making the application to be registered. Only those persons who pass the verification checks will be added to the register.

Who will it impact?

The information will be collected from every person whose entry on the existing register cannot be matched during the transition phase and for all individuals who make new applications to register to vote in Great Britain once the transition phase has begun.

Data Management

A data management policy has been developed which sets out the arrangements for the management of electoral registration data by EROs (for England and Wales) and Assessors (for Scotland) upon commencement of IER. The policy applies to the information, which includes NINOs and dates of birth, that will be collected as part of the IER registration process in order to verify electors. There will also be cases where some electors do not have a NINO and will need to provide other evidence to verify their application.

The policy will continue to be developed over time and sets out the approach for the secure capture and storage of personal information and the rules for the retention, disposal, access, supply, use and reuse, validation, and refresh of this information. Any technical solution put in place will comply with this policy and current data protection legislation and policy.

This policy will continue to be tested through ongoing consultation with various key stakeholders including the Information Commissioners Office, Electoral Commission, Association for Electoral Administrators, Society of Local Authority Chief Executives, Electoral Registration Officers and organisations interested in privacy issues. A public consultation has been undertaken and consultations have also taken place with the Metropolitan Police, Association of Chief Police Officers and the Serious Organised Crime Agency. As such, the policy is expected to develop throughout the lifetime of the project. Relevant Government departments are and will continue to be involved in the development of this policy to ensure the security of information.

Retention and Disclosure

Electoral Registration Officers will be required to retain all IER application forms for 12 months and then securely destroy records of NINOs.

There will be strict rules around the disclosure of the information and regulations will provide that the following will be an offence:

- Disclosure of the information provided by an applicant in their electoral registration application, or the information provided by any entity in the

entitlement verification process to any person not involved in the registration or verification process.

The additional information collected as part of the electoral registration application will not appear on the electoral register. The details currently captured in the electoral register will remain the same.

Verification of Data

EROs will be required to verify the details supplied by an applicant within a standard framework – that is to say within the framework of a policy, that will be expressed in legislation, setting out the level of assurance that must be achieved and the evidence required to achieve it.

The objective of the verification approach is for EROs to assure themselves that an applicant for electoral registration is a real person, with a real address and a real association between the two. It is proposed that this will be determined by the use of connecting addresses with the Local Land and Property Gazeteer (current practice which determines whether an address is real and correct), the issuing of confirmation letters which will contain an instruction to inform the ERO if the named individual does not reside at the property in question, and data matching with local and national public databases to verify the application.

An appropriate balance must be struck between security and accessibility. The test endured by citizens must not be so high that electors are dissuaded from registering but must be high enough to sufficiently harden the electoral register as a target for fraud.

On the balance of probability, EROs must determine that the applicant is a genuine person with a genuine association at a genuine address.

Authentication will be achieved from a cumulative process derived from two or more pieces of evidence from trusted sources.

Verification will therefore be derived from a mixture of direct evidence of the applicant being resident together with validating a standard set of biographical data either through the cross checking of the entire electoral register or through information supplied by the applicant (at the outset, in most cases this will consist of name, address, date of birth and NINO) which is mapped against one or more trusted data sources.

Alternatives for Verification Process

Whilst the above describes how the verification of applications is likely to operate for the majority of electors at the outset of IER, EROs will have the power to require further or different information and accept assurances from trusted sources in an effort to avoid duplication and requiring excessive amounts of personal data to be supplied by individuals.

Impact on Individuals

Notice will be given to all individuals of the need to provide additional information when registering to vote through a public information campaign at the time of implementation. From the time IER commences, the application form for electoral registration will require additional information in order to verify applications. As part of an electoral registration application, individuals will be provided with a fair processing notice which will set out how their data will be used. Individuals will have access to their own data through the standard procedures under the Data Protection Act. Those individuals who do not wish to or cannot provide this information through one of the main channels will be offered alternatives such as attending in person and providing alternative documentation.

System users

The users of this system are set out in Section 4 – Data Flow Analysis. These users will have access to the information for the purposes of verification only. Users will be security cleared to appropriate levels and systems will provide access only to those users who have such clearances and will also contain audit trails of access.

It must be stressed that additional personal data collected as part of the electoral registration application under IER will not form part of the electoral register. The current information that forms part of the electoral register will remain the same under IER. The additional information collected will be used for the purposes of verification only.

A system solution to manage this information is being developed. Security is a critical component of the development process and privacy impact assessments and mitigation will be an ongoing process.

Organisational relationships

The additional personal data will be shared with organisations external to the Electoral Registration Officer for the purpose of verification only. The information will not be re-used for any other purpose. Electoral Registration Officers and external organisations (as applicable) will store this information securely whilst in use and will dispose of the data securely after a defined period, in compliance with the Data Protection Act and other legislation. External organisations include the Department for Work and Pensions and other areas of the local authority.

Data matching will be used for three specific purposes. The first is for 'data mining' – using data matching to find potential electors who do not currently appear on the electoral register; the second is for verifying an individual's application; the third is for confirming the accuracy of the register i.e. cross checking against trusted public data sources to identify any entries which are out of date .

The data that will be shared for the purposes of verification only is:

- Electoral registers
- Name
- Date of birth

- Address
- Nationality (plus immigration status where appropriate)
- NINO
- Previous and / or alternative address

Date of birth, nationality and national insurance number data will not be shared with any external organisations other than for the purposes of verification (although it should be noted that name and address appear on the electoral register and therefore are shared with other external organisations under current legislation).

The data that will be shared for the purposes of data mining includes:

- Name
- Address
- Information regarding how many individuals live in a specified property
- Information about other individuals who live in the same property

IER forms will be retained for a period of 12 months after which National Insurance information will be destroyed. Further information regarding the storage and destruction processes of this information will be set out in secondary legislation.

The electoral register is currently shared with other organisations under legislation and this is not anticipated to change under IER. The additional personal data provided will form part of the elector record but will not form part of the electoral register.

Technology employed

A solution for the storage and transmission of personal information collected from electoral registration applications is currently being determined. A project team is working to determine user and security requirements, user access to the system and information, auditing procedures and safeguards, and user training. The PIA for this solution will be developed and assessed as the project progresses.

The Government takes the handling of personal data and the prevention of identity fraud very seriously and as such, any solution will ensure the secure storage and transmission of personal data, in accordance with standard legislation and policy requirements.

Users of the system will be local authority employees who will be trained in the appropriate use of the system and security of personal data.

Legislation and policies

IER policy does not create any adverse affects under the following legislation:

- Privacy and Electronic Communications Regulations 2003.

- Human Rights Act 1998
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 1998

Solution adopted

A solution for the storage and transmission of personal information collected from electoral registration applications is currently being determined but will be in place for implementation.

Data protection/risk reducing designs

As the solution is still being developed, it is not possible to document the specific data protection or risk reducing design. The design features to secure, move and store personal data (if necessary) will be a requirement of any solution implemented for this purpose.

Section 4 – Data flow analysis

Business data flow diagram and description

Personal data will flow between three defined groups of organisations under IER. These are:

- Individual electors;
- EROs; and
- Data holders.

Data flow tables

These tables list the data flow and organisations involved in transmitting and receiving data for both the application based and simplified routes.

Individuals using the application based route

Organisation	Data Flow
Elector	Transmits: - Provides information on Household Enquiry Form, detailing who lives in the property. - Provides information for individual electoral registration application (see section 3 for further detail) to ERO. Provided by mail or online, or potentially via alternative assisted digital channels such as telephone, or face to face.
Verification Service	Receives: - Information from individual electors who have made an online individual registration application (from 2014 onwards). - Information from EROs and third parties relating to electors who have made individual registration applications via other channels. - Data from data holder, received via secure methods.

	- Match report from data holders. Transmits: - Request to data holder to match data. - Match report to an ERO.
Electoral Registration Officer	Receives: - Information from individual electors on individual registration application (from 2014 onwards), received by mail, or potentially online, telephone or face to face. Household enquiry information on occupants of households (from 2014 onwards). Received by mail, potentially online or telephone. - Match reports from verification service, received via secure methods. Transmits: - Confirmation of registration to elector in certain circumstances (also, requests under alternative procedure).
Data Holder	Receives: - Request from verification service to match data, received via secure methods. Transmits: - Data to verification service sent via secure methods. - Runs match and sends match report to verification service, sent via secure methods.

Individuals added through the simplified transition process

Organisation	**Data Flow**
ERO	Receives: - Match reports from the verification service on

	electoral register cross-checks, received via secure network. - Household enquiry information on occupants of households (from 2015 onwards). Received by mail, potentially online or telephone. Transmits: - Electoral register to the verification service to check names and addresses of electors, sent via secure network.
Verification service	Receives: - Electoral registers from EROs. - Match reports from data holders. Transmits: - Electoral registers to data holders. - Match reports to EROs.
Data Holder	Receives: - Request from ERO to match data (including a full electoral register), received via secure network. Transmits: - Data to ERO, sent via secure network. - Runs match and sends match report to ERO, sent via secure network.

Note:

A solution for the storage and transmission of personal information collected from electoral registration applications is currently being determined. It will be in place for implementation from 1 July 2014, however specific methods of transmission cannot be detailed at this time.

Section 5 – Data protection analysis and risk management plan

Stakeholders/participants

The following organisations and key stakeholders have been involved in the assessment of data protection risks for this policy:

- Information Commissioner's Office
- Metropolitan Police
- Association of Chief Police Officers
- Serious Organised Crime Agency
- HM Revenue and Customs
- Department for Work and Pensions
- Electoral Commission
- Association of Electoral Administrators
- Society of Local Authority Chief Executives
- EROs

Analysis process

This process has involved both formal and informal engagements to determine the risks to personal data and controls and mitigation strategies to manage these risks.

Technology

A solution for the storage and transmission of personal information collected from electoral registration applications is currently being determined but will be in place for implementation. The necessary design features to secure personal data will be a requirement of any solution implemented for this purpose.

Verification

The policy proposes the provision of NINOs by some individuals to assist in the verification of applications, as well as a new process to register to vote. The identity of 'at risk' electors who may suffer physical harm if they are found e.g. anonymous electors will be protected at all times.

A significant amount of work has been conducted with various stakeholders on the security risk to personal information and appropriate mitigation strategies which have and will continue to be incorporated into policy and business processes.

Multiple Organisations

The policy requires data sharing between multiple organisations for the purposes of verification of entitlement, identifying potential electors who do not currently appear on the register and checking the accuracy of current entries. The breakdown of information silos in this instance will be tightly controlled, within the law, and aim to reduce fraud and for fraud detection. The personal data will be shared only for data matching purposes to determine if an elector has provided genuine information on their application.

Data and Data Handling

The policy involves the handling of personal data in a new way. Currently, the personal information that is provided (name, address, nationality) is not verified. This policy will require some individuals applying to register to vote to provide additional information which will be used to verify their application before they are added to the electoral register. With approximately 46 million people currently on the electoral registers in Great Britain and our expectation is that approximately a third of these electors will need to provide information during the transition phase, this policy affects a large proportion of the population.

The verification process will involve data matching of personal data, possibly from multiple sources. Additional personal data will only be shared for the purposes of verification and not for commercial purposes such as consumer marketing.

The overarching data protection principles will not be changed by this policy. Data collection policies and practices; quality assurance processes and standards; security and access arrangements; and data retention arrangements will be made clear and extensive and will meet current legislation and policy requirements.

Exemptions and Exceptions

The policy **does not** propose:

- data processing that is exempt from legislative data protection measures;
- disclosure of personal data to third parties who are not subject to comparable data protection regulation; or
- new or changed data handling that is exempt from data protection measures.

The only exemptions and exceptions that will be lawful are those that are permitted under current legislation, for example disclosure of information for the

purposes of law enforcement. There is no intention to add to the current list of exemptions.

Risk management

The Government takes the handling of personal data and prevention of identity fraud very seriously. The changes that are being proposed to electoral registration are intended to prevent fraud and maintain the integrity of the electoral system. Below is an overview of the data protection and data sharing risks and the controls and mitigation strategies which are or will be put in place. We will ensure that all data governance standards and processes as set out by CO and CESG are adhered to:

Risk Description	Controls/Mitigation
Data security breach – data mishandled by Local Authority or other authorised users.	Data management policy in place and monitored. Engagement with IT suppliers to ensure systems appropriate to protect data. Continued engagement with key stakeholders to ensure security of personal data is built into policy and processes.
Data is used for unauthorised purposes or shared inappropriately.	Data management policy in place and monitored. Will conform to data protection principle of data being processed for specific and lawful purposes. Engagement with IT suppliers to ensure systems appropriate to protect data. Continued engagement with key stakeholders to ensure security of personal data is built into policy and processes. Offence for onward disclosure of information.
Data is accessed by unauthorised persons.	Data management policy in place and monitored. Engagement with IT suppliers to ensure systems appropriate to protect

	data. Continued engagement with key stakeholders to ensure security of personal data is built into policy and processes.
Inappropriate retention of the data.	Data management policy will clearly set out retention and disposal schedules and will conform to data protection principle of not keeping data for longer than is necessary.

It must be noted that due to the nature of the personal data being collected, there are specific risks around the data being used for identity and other fraud. Significant work has already been conducted with key stakeholders on assessing and mitigating these risks and will continue throughout the development of policy and processes.

Section 6 – Communication/publication strategy

Communications

The PIA will be published alongside the Bill and will be disclosed in full.

Publication strategy

The Bill and associated narrative and impact assessments will be published upon introduction.

It is intended that this Privacy Impact Assessment will be a living document and develop over the life of the project.

Section 7 – Approval of report

Approval of:	**Individual Electoral Registration – Privacy Impact Assessment**
Minister	Mark Harper MP, Minister for Political and Constitutional Reform
Date of approval	4 May 2012