2011 Census Security: Report of the Independent Review Team

Contents

Covering Letter

TO THE NATIONAL STATISTICIAN FOR ENGLAND AND WALES, AND THE REGISTRARS GENERAL FOR SCOTLAND AND NORTHERN IRELAND

Dear National Statistician and Registrars General,

We have pleasure in presenting to you the report of the Independent Review Team on 2011 Census Security.

You have given firm undertakings to the public and to your respective parliaments and assemblies that census data will be used solely for statistical purposes and that it will be treated in strict confidence. In support of this, you jointly commissioned our review with terms of reference which included a report on the adequacy of the information assurance arrangements for the 2011 UK Censuses.

The review team is completely independent and has substantial experience of public sector audit and information assurance. Over the past year we have thoroughly familiarised ourselves with the arrangements for the Censuses in each part of the United Kingdom and examined in detail the arrangements that are being made to protect the information provided by the public.

We would like to acknowledge that, in undertaking this work, we have had complete access to everyone in your organisations and in your contractors who we thought it necessary to meet. We have also had access to census sites and to any documentation we requested, including risk registers, audits and test results. The co-operation and openness of your staff and their evident commitment to ensuring the security of the censuses, reflects the highest professional standards.

Public confidence that the information in their returns will be securely handled is vital for the success of the Censuses. We believe that the results of our review will make a substantial contribution to engendering that confidence and that the public can be assured that the information they provide to the 2011 Censuses will be well protected and securely managed.

John Dowdall
Harvey Mattinson
Peter Fagan

January 2011

Executive Summary

This report presents the findings of an independent review of the protection to be applied to personal information gathered as part of the 2011 Censuses across England and Wales, Scotland and Northern Ireland.

The key conclusions of the review are that:

- There is a sound basis of commitment, knowledge and personal responsibility underpinning the information security management aspects of 2011 Census operations.
- There is solid management resolve within all three organisations towards ensuring that the 2011 Censuses should build upon previous experience in securely managing census operations and data.
- The assurances given to the public by the Census Offices regarding the USA PATRIOT Act are consistent across the legal and operational arrangements set in place with their commercial partners. The issue of potential access to census data under the Patriot Act has been well addressed.
- There has been a significant increase in the level of public awareness of data security and the need for demonstrable protection of personal information. Against that background, all three organisations have risen to the challenge of implementing effective information security as part of their respective Census operations.
- Online data gathering is expected to account for approximately 25% of the total number of returns in the 2011 Censuses. The review team are satisfied that the Information Assurance measures put in place for this relatively new aspect of census operations are appropriate and can be expected to be effective.
- The review team made suggestions for improvement, mostly in terms of achieving greater consistency across the three operations, which were welcomed by all three Census Offices. The short timescales in which the suggestions were taken up demonstrated both commitment and capability.
- All three organisations have undertaken assurance activities, not just as a matter of adopting a professional approach and implementing best practice, but as a crucial part of the preparation for the Censuses.

It is clear to the review team that from the outset, ensuring the protection of the personal information provided by the public has been a core objective in the planning for the 2011 Censuses. The review team have had the opportunity to thoroughly review planning, management and implementation aspects, with the full cooperation of the staff involved, and have had complete access to 2011 Census staff, sites and documentation.

As a result of our review, we are very satisfied that the three Census Offices are managing Information Assurance pragmatically, appropriately and cost-effectively. We are, therefore, confident that they are capable of delivering their IA objectives and that information will be held in secure environments and that it will be handled in line with best practice and Government standards. The public can be assured that the information they provide to the 2011 Censuses will be well protected.

1. Setting the Scene

1.1. Background to the Review

The UK Censuses constitute one of the most important data collection exercises undertaken by the UK Governments. Much depends on the accuracy and completeness of the information gathered, which is used to underpin a great deal of planning and decision making in both the public and private sectors.

Public confidence that personal census information will be securely handled is a vital ingredient for success. All three Census Offices have given firm undertakings that this data will be used solely for statistical purposes, and that it will be treated in strict confidence. The purpose of this report is to present the findings of an independent review of the extent to which these undertakings will be met.

1.2. The Review Team

The review team were chosen to provide the necessary balance of audit, security and management skills. The Independent Information Assurance Review (IIAR) team was made up of:

- John Dowdall. Mr Dowdall has recently retired as Comptroller and Auditor General for Northern Ireland, responsible for independent audit of the devolved functions in Northern Ireland. He has been closely involved with the management of public expenditure and economic issues throughout his career. He was Head of the Northern Ireland Audit Office from 1994 to 2009. During this period he worked closely with the Public Accounts Committee at Westminster and, after devolution, with the Northern Ireland Assembly. He is an Honorary Member of the Chartered Institute of Public Finance Accountants and, since 2002, Visiting Professor in the School of Accounting of the University of Ulster. He was awarded a CB in 2003.

- Harvey Mattinson. Mr Mattinson spent 5 years as Head of Infosec Consultants at GCHQ before being seconded to the Cabinet Office as Deputy Director of the Central Sponsor of Information Assurance, responsible for security policy and standards, and inaugural head of the profession of accreditation. Prior to his retirement, Mr Mattinson established a number of key integrative groups in IA, including GIPSI and CIPCOG, he introduced the Claims Tested (CCTM) Scheme and he was responsible for the pan-Government accreditation of many large scale networks and services including the Government Secure Intranet, the Government Gateway, and Airwave. Mr Mattinson is a Chartered Engineer, Chartered Mathematician and Chartered IT Professional, a Fellow of the Institute of Mathematics and its Applications, and a Fellow of the BCS and Associate of the IISP. He is also an external examiner for the Government certification with the IISP, and lectures in all aspects of IA at the National School of Government.

- Peter Fagan. Mr Fagan has extensive experience in Government security, having been a founder member of the CLAS Scheme. His experience includes a number of years as the Government Gateway security manager, an extended period as lead assessor for the GovConnect programme reviewing Local Authority applications to join GCSx, and he was selected twice for the assessment of security aspects of bids for the National Lottery franchise. Mr Fagan was a key figure in the establishment of the TIGER Scheme. He has contributed to UK e-Government standards and was awarded an SC Europe prize in 2007. He has two first degrees and an MBA from Warwick Business School.

1.3. Scope of the Review

Within the UK, census activities are undertaken by three organisations: a census for England and Wales, conducted by the Office for National Statistics (ONS); a census for Northern Ireland carried out by the Northern Ireland Statistics and Research Agency (NISRA); and a census for Scotland, carried out by the General Register Office for Scotland (GROS). The review looked into the Information Assurance (IA) activities of all three organisations, and principally the IA management processes.

Information Assurance encompasses all those processes implemented within an organisation which ensure that information security measures are effective. Without genuine senior management commitment, without a comprehensive integration of security issues into project plans, and without an appropriate level of impartial review and assessment, the straightforward implementation of security measures can be no more than a paper exercise.

The review team therefore critically assessed the degree to which IA was being managed in each of the 2011 Census operations, starting from the level of senior management knowledge and commitment, through to a review of responsibilities and ownership, taking in a review of documentation and project plans, down to site visits at the major processing centres. At each stage the team were seeking confidence:

- that the stated commitment to protecting personal information had been reflected into all areas of planning, implementation and operations;
- that the risks to the security of personal census information were well understood and were being managed; and
- that the importance of protecting information which had been entrusted to each organisation was also clearly understood.

It is important to note, therefore, that the review was not a simple review of the security measures which had been put in place; it was a review of the processes and choices leading up to the implementation of those measures, with the aim of ensuring that the measures had been based upon a clear understanding of the need to protect information entrusted to the Census Offices.

The conduct of the review reflects the understanding within all three Census Offices that increasing levels of public awareness regarding data protection require openness and demonstrable levels of protection, which in turn must be based on independent assessment.

1.4. Areas Out of Scope for the Review

UK Government security processes recognise an approval stage for IT systems and supporting processes, known as accreditation. Accreditation is a formal statement that the operation of the IT system being accredited will not present an unacceptable risk.

In line with UK Government policy, all in-house and outsourced systems underpinning 2011 Census operations are subject to formal accreditation by the relevant authority within the respective organisations.

The Independent IA Review was not intended to act as a 'double accreditation', or to review the decisions of the Accreditors. It was however, intended in part to confirm that the accreditation process was robust in each case, and that due care and diligence had been exercised in both the preparation and conduct of the accreditation exercise.

1.5. How the Review was Carried Out

The review was carried out in a number of stages, with the aim of gaining incremental confidence at each stage.

1.5.1. Stage One: IA Governance

Stage One was concerned with the confirmation of an appropriate level of IA governance across the three Census Offices. The review took as its basis the Information Assurance Maturity Model (IAMM) developed by the Cabinet Office and adopted throughout the UK Governments as a means of assessing the effectiveness of IA management and governance.

Use of the IAMM approach is itself recognised as a reflection of best management practice. Its application provides a definitive statement on the ability of an organisation to implement an appropriate information security regime. The use of IAMM in this case therefore, can be taken to indicate that the work conducted in Stage One was not an ad-hoc review based on experience, although clearly the experience of the review team was a factor; rather, it was a review of the IA capability of each organisation, against an established benchmark.

The IA Maturity Model addresses the following areas:

- Leadership and Governance;
- Training, Education and Awareness;
- Information Risk Management;
- Through-life IA Measures;
- Assured Information Sharing;
- Compliance.

The review team requested that each organisation self-assess to Level One as a minimum, Level One being the baseline level for demonstrating compliance with the recommendations of the HMG Data Handling Review.

Stage One of the review was based on interviews with key personnel within all three Census Offices, in addition to a comprehensive review of available documentation.

1.5.2. Stage Two: Detailed Assessment

Stage Two widened the assessment and looked at the effectiveness of the relationships between the three Census Offices and their commercial partners, insofar as it related to Information Assurance.

The Stage Two work went into more detail on the design of Census operations. It took into account a review of progress against the findings of Stage One, it reviewed the lessons learned in relation to IA from the Census rehearsal activities, and it included a further review of IA documentation.

The Stage Two activities also included interviews with personnel from key commercial partners across all three Census Offices, in addition to site visits at all major processing centres.

1.5.3. Stage Three: Report Production

Stage Three reviewed the progress of the three Census Offices towards meeting their stated IA objectives, so that the independent report (this document) could reflect the most up to date position on IA, while still being issued prior to the Censuses. The work included one site visit that could not be arranged within the timescales of Stage Two, a number of final meetings with all three Census Offices to confirm points arising during the drafting of the report, and further document reviews, including the review of updated IA documentation.

1.5.4. Stage Four: Closedown and Review

Stage Four, to be conducted after the Censuses, will confirm that the respective closedown plans include an appropriate IA decommissioning component, and that there has been a 'lessons learned' exercise in the area of Information Assurance. The key deliverable from this stage will be a report on the assessment of the closedown plan and an overall assessment of the effectiveness of IA achieved for the 2011 Censuses.

1.6. Timing of the Review

The review began in March 2010. Stage One concluded in June 2010, with a series of meetings to discuss the conclusions from Stage One. Stage Two commenced in August 2010, and concluded in October. Stage Three commenced in September 2010 and concluded with the issue of this report.

The review team were engaged by the National Statistician and the Registrars General a year in advance of the Census date for all three organisations (March 27th 2011), to allow time for a thorough review of IA, and to allow any key findings to be reflected into the ongoing preparatory activities.

This report represents the findings of the review work conducted by the review team, up to and including 14th December 2010.

2. Key Issues for the Review

2.1. The UK Government Security Environment

There is no doubt that over the past few years, certainly during the period of preparation for the Censuses, there has been a focus within the UK Governments on improving the handling of data by Government agencies, particularly in the area of personal information. The general public's awareness of security and IA issues has risen significantly over the past few years, partly as a result of Government data losses. Media interest in the Government's approach to information management has risen also. During the timescales of the independent review, the Wikileaks issue has been instrumental in highlighting the importance of Government data handling and at the same time, the issue of data access.

These factors place increased emphasis on the demonstrable effectiveness and transparency of the IA operations of each census organisation and, although each has clearly demonstrated their commitment to openness, public perception of the effectiveness of security management can often differ from practice. There is an obligation upon each organisation to ensure that the weaknesses uncovered by previous incidents elsewhere in the public sector, such as incomplete procedural control over bulk data transfers, inadequate control over information held on laptop computers, and incomplete control over items of removable storage media, have been comprehensively and demonstrably addressed.

It is the view of the review team that ONS, NISRA and GROS have risen to this challenge.

The review team were not engaged to provide an accreditation statement, and therefore this report cannot provide a statement of approval regarding measures taken in relation to previous public sector incidents. Nevertheless, it is the opinion of the team that all three organisations have taken on board the lessons learned from previous incidents in the public sector.

2.2. The USA PATRIOT Act

The USA PATRIOT Act (commonly referred to as the Patriot Act) has been a key issue in the 2011 Census preparations. Section 4 of this report sets out the contractual arrangements for the 2011 Censuses and within that, the role of Lockheed-Martin UK as a contractor to ONS and NISRA, and the role of CACI (UK) as a contractor to GROS. Both companies are subsidiaries of US companies. Under the provisions of the Patriot Act, in certain circumstances US companies can be required by the US security agencies to disclose information under the company's control or to which the company can obtain access.

The involvement of US contractors in the census process has been dealt with by the census authorities in other countries, for example, Canada in 2006. In the UK, government data processed by any company whether UK or foreign owned must be protected to the standards required by the 1998 Data Protection Act. The issue was, therefore, recognised from the outset by ONS, NISRA and GROS and was addressed when defining the contractual and operational arrangements with contractors.

The review team are aware that this has been a matter of public interest and note that the use of UK and EU subcontractors places Lockheed-Martin UK at arm's length from the data gathered in England and Wales, and Northern Ireland. Once the data capture infrastructure has been completed, there will be a 'scrubbing' stage in which all routes of access for Lockheed-Martin UK employees will be removed, and the Census Offices will formally assume control, with Steria, an EU company, undertaking the necessary data management and administrative functions. There have been public assurances that the contractual arrangements have been structured to ensure that only sub-contractors registered and based in the UK, and either UK or EU owned, will have access to personal census data. No Lockheed-Martin staff (from either the US parent or UK company) will have access to any personal census data. The approach adopted by GROS has been similar, and GROS will play a major role in controlling access to the infrastructure used for processing data supplied in the 2011 Census. It is a condition of the contract with CACI (UK) that personal census information will not leave the UK. GROS have confirmed that CACI (UK)'s sub-contractors with access to 2011 Census data have no US links and that the Act, therefore, does not apply to them. GROS have also given public assurances on contractor confidentiality in this area.

It is the view of the review team that the assurances given by the Census Offices are consistent with the legal and operational arrangements set in place with their commercial partners, and that the issue of potential access to 2011 Census data through the application of the Patriot Act has been well addressed.

2.3. The Use of Online Data Gathering

For the first time, in 2011 individuals will be able to complete their census form online. The use of online data gathering is a new factor for census operations in the UK. It has required all three Census Offices to extend their IA activities to cover a new set of technologies, and it has required each to amend existing IA processes. In the 2011 Censuses, online data gathering is expected to account for approximately 25% of the total number of returns.

Through their respective contractual arrangements, all three Census Offices have imposed a security approval regime on the services and systems provided by their commercial partners, to be demonstrated through evidence of compliance supplied by the prime contractor, together with Census Office assessment and review, and through evidence assembled by independent third party assessments.

The accreditation regime imposed by each Census Office extends to encompass all systems and processes to be used for online data gathering of personal census information.

It is fair to say that the Internet remains a medium with inherent risks, i.e. risks that are an inseparable part of the use of the medium itself. However, it is also fair to say that those risks are known and understood, and that best practice in defending against the underlying threats is both established and widely available. As stated at Section 1.4, it was not within the remit of the review to deliver an accreditation statement; nonetheless, the review team do wish to make it clear that the evidence assembled during the review shows that the Internet access route has been implemented using best information security practice, also that its reliability will be verified using independent testing, and that the team are convinced that

any recommendations made as a result of the testing will be taken on board and implemented in order to protect data provided through this option.

3. Information Assurance in The Census Process

3.1. Introduction

The Census Offices (GROS, NISRA and ONS) have provided a description of the census process (see the attached Annex, "Census Offices Description of the Census Operation").

This section examines the IA implications and requirements of the component processes.

3.2. The Legal Framework

Details on the legal framework for census activities in the UK can be found in a number of publicly available documents. The key points are reproduced here.

The statutory authority for taking a Census in Great Britain (that is in England, Wales and Scotland) is the Census Act of 1920, as amended by the Statistics and Registration Service Act 2007. The Act gives power to the Government of the day, if Parliament agrees, to ask the Queen to make an Order in Council directing that a Census be taken on a particular day.

The duty for carrying out a Census rests with the UK Statistics Authority (for England and Wales) and the Registrar General for Scotland. Similar, but separate legislation (the Census Act (Northern Ireland) 1969) applies in Northern Ireland, where the Registrar General for Northern Ireland, whose office is part of the Northern Ireland Statistics and Research Agency, is responsible for carrying out the Census. Regulations specifying the detailed arrangements for the conduct of the census, separately in England, Wales, Scotland and Northern Ireland are also approved by each respective legislature.

Participation in a census in the UK is a statutory requirement, and the confidentiality of the information supplied by the public is protected by legislation. In England and Wales, the Census Act 1920 (as amended by the Statistics and Registration Service Act) and provisions set out in the Census Regulations, lay down penalties for the unlawful disclosure of information from the census by anyone involved in taking a census. The Census Act 1920 also provides the protection for the census in Scotland. The Census Act (Northern Ireland) 1969 provides the protection for the census in Northern Ireland.

The confidentiality of personal information provided by individuals as part of the Census is therefore taken very seriously indeed. It is unlawful, for example, for the Census Offices to pass any personal census information to other Government departments or to any other organisation except for legitimate purposes under the Census Acts themselves or under the Public Records Act 1958. Census records are currently kept confidential and closed to public inspection for 100 years (Census records are permanently closed in Northern Ireland).

Throughout the conduct of the review, the team saw that the three organisations were always fully aware of the legal framework ensuring the confidentiality of personal census information, and that staff in all three organisations were conscious of the weight of responsibility placed upon them by the consequent obligations and undertakings relating to the protection of that information.

3.3. Questionnaire Development

Well in advance, each organisation undertook a questionnaire development exercise, including an element of public consultation. It should be understood that in this case, 'well in advance' means a period of the order of four years in advance of the Censuses.

Census preparation clearly needs to take into account a number of factors, such as Government information requirements over the coming decade, applicable legislation in e.g. the area of equality, and relevant parallel and planned Government initiatives, in order to ensure that the final questionnaire is not only robust but that it meets its purpose. However, the review and consultation also must ensure that the resulting questionnaire is 'acceptable', including a consideration of whether or not a question could be considered too intrusive, and whether or not a question might be considered too burdensome.

All three organisations have made public the results of their consultations. The documents can be accessed using the links below:

http://www.ons.gov.uk/census/2011-census/2011-census-questionnaire-content/recommended-questionnaire-content-for-england-and-wales.pdf

http://www.nisranew.nisra.gov.uk/census/2011_census_consultation.html

http://www.gro-scotland.gov.uk/files2/the-census/policy/2011_census_recommendation_paper.pdf

Following the consultation period, each organisation published a document setting out the objectives for their 2011 Census, and also setting out the questions to be asked and the nature of the information to be gathered. The documents were placed before the respective Parliaments and Assemblies in order to obtain the necessary mandates to proceed with the Censuses.

Each document contains a section setting out both the need for privacy and the obligations and responsibilities placed upon each organisation and upon individuals, in relation to the privacy of personal information. These documents too, are publicly available:

http://www.gro-scotland.gov.uk/census/censushm2011/policy-and-methodology/2011-census-gov-statement-and-supporting-docs/scotlands-census-2011-a-government-statement.html

http://www.ons.gov.uk/census/2011-census/2011-census-questionnaire-content/2011-census-white-paper--english-.pdf

http://www.nisranew.nisra.gov.uk/census/pdf/proposals.pdf

Each organisation also developed a Privacy Impact Assessment (PIA), looking at the privacy requirements applying to their Census operations, the relationship of those requirements to the questionnaire content, and the impact on census operations arising from the need for privacy. The PIA's were also made public for ONS, NISRA and GROS, and can be accessed using the links provided below:

http://www.ons.gov.uk/census/2011-census/2011-census-project/commitment-to-confidentiality/privacy-impact-assessment--pia--on-2011-census.pdf

http://www.nisranew.nisra.gov.uk/census/pdf/Privacy Impact Assessment.pdf

http://www.gro-scotland.gov.uk/census/censushm2011/policy-and-methodology/index.html

In setting out these details, the review team do not intend to develop a case for any or all of the Census Offices in terms of their openness, or in terms of their commitment to privacy. However, the evidence available to the team showed that the nature of the information to be gathered was known to each organisation prior to the consideration of the security controls required to protect it, which is a *sine qua non* of the discipline of Information Assurance. Furthermore, there is clear evidence of oversight and of a publicly stated commitment to the protection of personal information, both of which were considered by the review team to be major drivers for senior management interest in the effective management of IA throughout the 2011 Census operations.

3.4. Rehearsal and Lessons Learned

Each Census Office undertook a rehearsal exercise as preparation for their Census, in order to ensure that systems and processes worked as expected, in order to familiarize staff with the operation, and in order to investigate any potential areas for improvement and risk reduction. Each also produced a report detailing the findings of their rehearsal exercise, and each made their report public:

http://www.statistics.gov.uk/articles/population_trends/evaluationofthe2009rehearsal.pdf

http://www.gro-scotland.gov.uk/census/censushm2011/preparations/2009-census-rehearsal/09-census-rehearsal-eval-report/09-census-rehearsal-eval-report-lvl2.html

http://www.gro-scotland.gov.uk/files2/the-census/preparations/rehearsal/2009-cre-security.pdf

http://www.nisranew.nisra.gov.uk/Census/pdf/2009 Census Rehearsal evaluation.pdf

The information gathered from the rehearsals was assessed as part of the review team's work. The review team were also given access to individuals who had worked on the rehearsals, and were given access to security operating logs maintained during the rehearsals.

A key part of the rehearsals was that lessons should be learned, including of course in the area of Information Assurance. The rehearsal operations therefore included a stream dedicated to logging security-relevant events for later analysis. For ONS and NISRA, one event (partial duplication of the Internet Access Code printed on each questionnaire) could, under certain circumstances, have led to unauthorised access to partially completed online returns. As a result of the post-rehearsal review, extensive additional measures were taken by ONS and NISRA, and their suppliers, to prevent this happening in the Census proper. As each questionnaire leaves the production line it is now checked by camera to ensure that the code is unique.

On the basis of the evidence, the review team were satisfied that the protection of information gathered during the rehearsals was an integral part of the rehearsal

operations, and that furthermore, all three organisations were, and remain committed to seeking improvements wherever possible, in order to fully ensure the protection of personal information entrusted to them.

3.5. Printing, Distribution and Return

Paper questionnaires for the 2011 Censuses are being produced in controlled printing environments with processes to ensure that no 'spoils' leave the area. The forms each have a unique identification code printed on them, and each page is uniquely identifiable; this ensures that should there be a mistake in subsequent questionnaire processing, it will not escape the notice of the processing teams. Once printed, the forms are stored in a physically secure area and are logged out by shipment number.

Questionnaire printing requires address information, which could be considered to be publicly available. However, good security is made up of measures which protect against corruption and which ensure availability, as well as protecting against disclosure. In the case of the printing operations, security issues therefore encompass e.g. the correct transfer and interpretation of address information, and the safe transport and storage of printed materials. There is also a general consideration that security problems with these operations will have the potential to affect the public's perception of the protection provided to their personal information. The review team were pleased to note therefore, that the printing operations for each organisation were subject to the development, approval and implementation of an appropriate information security policy.

On previous censuses throughout the UK, census forms were distributed by hand. For their 2011 Censuses, ONS and NISRA will use Royal Mail services to distribute the forms, and will also use the Royal Mail to log their return. For GROS, distribution will be mostly via staff recruited for the purpose ('enumerators'), with Royal Mail being used to deliver a small percentage of forms, to remote addresses. The review team noted that the ONS and NISRA operations were subject to a formal statement from Royal Mail concerning the assurance activities to be undertaken. GROS have set in place corresponding formal personnel and procedural measures for enumerators, including mandatory awareness training, a requirement to sign a formal Census Confidentiality Undertaking, and the application of baseline reliability checks.

For ONS and NISRA, returned paper questionnaires will be scanned by the Royal Mail (through the window in the sealed envelope) in order to register the unique questionnaire ID. This will allow the package to be tracked and batched by geographical area before being returned to the forms processing centre. The review team noted that the main processing sites were each covered by an approved security policy, and that at each site, processes were in place to ensure the integrity of the returns, such as: each shipment of forms will be tracked by driver, by lorry number and by time; any shipment failing to meet these criteria on arrival will not be accepted at the processing site, and will be quarantined until the discrepancies have been investigated. The team also noted that the paper data capture sites have been subjected to independent physical and procedural audits.

Returned forms will be held in a controlled environment until they are ready for processing, at which time they will be moved into a temperature and humidity controlled area for 24 hours to condition them. They will then be fed through a

high capacity guillotine to separate the pages, each of which will then be scanned and registered using the unique questionnaire identity number. The scanned pages will be retained until such time as the contents have been confirmed by the Census Office as having been processed, whereupon the paper versions will be shredded and environmentally recycled.

3.6. Online Data Capture

The online data capture systems for the 2011 Censuses are sited in locations which are either dedicated to the purpose, or which are commercial data centres shared with systems of a similar level of sensitivity. In each case, the team saw that building entry was controlled, CCTV was in place around the perimeter of the building, and entry into the data hall holding the system was controlled (visitors will be escorted at all times and only allowed into the area once their bona fides have been confirmed).

Individuals using the web site to complete their questionnaires will be linked using the same level of encryption as is used for online banking.

Transfers of information between sites will be by fully encrypted hard drives transferred by Census Office staff or by approved courier, or alternatively via links protected using Government-approved encryption equipment.

It is not the place of the review team to provide accreditation of these facilities; nonetheless it should be noted that the team visited each of the sites, were provided with the opportunity to review the physical and procedural measures in place, and were also provided with plans and schedules for technical security vulnerability assessments. The team also noted that the Internet Data Capture sites have, or will have been subjected to independent technical and physical audit.

3.7. Support to the Public

Where it has not been possible to deliver a paper questionnaire, or where there has been no return from a household, field workers will visit to provide a questionnaire, or to provide assistance to complete the questionnaire.

The team noted that:

- If a paper questionnaire is completed with the help of field staff, the completed form is either held in the possession of the field operator, or it is sealed upon completion and therefore not available for access until it is opened in the secure environment of the forms processing centre.
- None of the IT equipment used in support of these field staff will be used to hold personal census information.
- Training (including confidentiality awareness training) will be provided to all individuals recruited as part of field operations across all three Census organisations.
- Reliability checks will be carried out on each individual recruited for field operations, and each will be required to sign a formal Census Confidentiality Undertaking prior to commencing work.

3.8. Support to the Census Operations

During the course of the Census, inevitably there will be a requirement for spare or replacement questionnaires to be provided to the public, and for other materials and consumables to be supplied to the field workers. GROS, NISRA and ONS therefore also each have a 'field fulfillment' operation. The review team noted that although the field fulfillment operations will involve the handling of only limited information, they were also the subject of agreed security policies.

3.9. Census Quality Survey

After the Census data gathering, an additional exercise will be undertaken to validate a small sample of the responses gathered, in order to provide a measure of the quality of the Census data. Laptops used to carry out this task will necessarily hold personal census information. The review team noted that:

- All laptops used in the Census Quality Survey will have encrypted hard disks, and will be securely wiped when the exercise has completed.
- Training (including confidentiality awareness training) will be provided to all individuals carrying out the Census Quality Survey.
- Each individual recruited for the purpose will be required to sign a formal Census Confidentiality Undertaking prior to commencing work.

3.10. Data Processing

The scale of the data processing task for the 2011 Censuses should be appreciated in order to understand the context for the IA requirements. For ONS and NISRA, for example:

- The paper data capture exercise requires 300 million pieces of paper to be processed, checked, and individually tracked.
- Paper data capture operations will be housed in a building with 180,000 square feet of floor space.
- The facility will support a dedicated IT infrastructure with some 300 workstations.
- The processing of the information into a useable database, including the reconciliation and amalgamation of information provided through the Internet Data Capture mechanism, will take from May 2011 until around December 2011.

For the GROS operations, the central facility comprises 56,000 square feet, with over 35 million pieces of paper being processed in the course of the Census.

At the end of the data processing exercise, it is planned that all IT equipment used in the processing of 2011 Census information will be either cleansed or destroyed, and that all buildings which are no longer to be used for census purposes will be securely decommissioned.

The team noted that despite the scale of operations, all three Census Offices were conscious of the fact that the disclosure of a single return would have significant consequences.

The main data processing sites were all visited by the review team in the course of their review. The review team saw that all three organisations had mechanisms in place to ensure that each item of information supplied during the course of their Census could be both tracked and protected. In particular, all had implemented strict levels of control over bulk data movements, and procedures had been set in place to ensure safe physical transport of data between sites.

3.11. Downstream Processing

The cleansing, quality assessment and anonymisation of the collected census data is referred to as 'downstream processing'.

Downstream processing will take place on systems owned by the Census Offices, and not on systems managed by commercial partners. The review team noted that all three Census Offices have a regime dictating that prior to having any personal census information loaded onto those systems, formal security approval to operate (accreditation) must have been achieved for the system.

Following the paper data capture and the reconciliation of the material gathered through the Internet route, the data is anonymised into a database that can then be used to carry out statistical analyses. Only anonymised data is made available for statistical analysis.

Before that however, there is a further, critical step, known as 'statistical disclosure control'. All three organisations will review the information to ensure that no individual or small group of individuals can be identified from the Census outputs, even where there is a degree of prior knowledge; that is, steps are taken to ensure that it will not be possible to selectively refine searches in order to produce a set of results where that result can only apply to one (known) individual.

Achieving this requires ONS, GROS and NISRA to perturb the information to a small degree, which will affect its validity for research purposes. That small amount of inaccuracy is considered by all three Census Offices to be a reasonable price for ensuring the privacy of the individual.

The mechanisms underlying the process are set out in a document available from the ONS, NISRA and GROS web sites. It can be downloaded using the link below:

http://www.nisranew.nisra.gov.uk/census/2011_census_sdc_policy.pdf

For the 2011 Censuses, ONS, NISRA and GROS will be aligning their approaches on statistical disclosure control, in order to ensure consistency.

3.12. End Users of the Data

The review team noted that only anonymised census databases (and not the raw data) are used for analysis, and access is only granted for bona fide research. Any individual or organisation wishing to conduct such research must apply and be formally accepted, and must demonstrate an appropriate level of protection for the information entrusted to them; part of the conditions of applying for access include a statement on confidentiality, and a statement of the purpose for which access is being sought.

The ONS version of the application form is publicly available and can be accessed using the link below:

http://www.ons.gov.uk/about/who-we-are/our-services/vml/accessing-the-vml/how-to-access-the-vml/approved-researcher-pack.pdf

4. Contractual Arrangements for the 2011 Censuses

4.1. General

Each of the three Census Offices has engaged with commercial partners to support critical census operations. Each has approached their contractual arrangements in a different way, reflecting their differing circumstances and requirements. The corollary is that in order to be effective, Information Assurance activities must be managed by each in a way that is aligned with their chosen approach.

It was not within the remit of the independent IA review to examine the contractual relationships in general; however, clearly the nature and effectiveness of the relationships could have a direct bearing on the Information Assurance activities of the commercial partners. The nature of the relationship in each case therefore bore some examination.

As part of the independent review, the contractual requirements relating to Information Assurance in the services provided by each of the major partners were reviewed by the team, and taken as part of the evidence and context for 2011 Census IA management. In addition, the contractual aspects were addressed in all discussions with commercial partners. The review team were focussed especially on the nature and effectiveness of the management of IA responsibilities across the contractual links.

4.2. ONS

ONS have contracted with:

- Capita, for the recruitment of field staff and the management of the associated payroll services;
- Royal Mail, for the distribution and return of questionnaires;
- 3M UK, for the printing of non-questionnaire materials (including address books, leaflets, etc.) and the operation of the field and public fulfilment centres;
- TNT, for secure distribution;
- A number of organisations in the areas of advertising, translation and communication activities;
- Lockheed-Martin UK, for the principal data capture and online operations.

As noted in Section 2.2 of this report, Steria are also resourcing the personnel to manage the data capture systems.

Lockheed-Martin UK Ltd, and their security advisers Logica, are the principal commercial partners for ONS. The contract with Lockheed-Martin UK covers the printing of questionnaires, Internet data capture, online help facilities, questionnaire tracking and operation of the Census helplines.

Acting in their role as managers and co-ordinators, Lockheed-Martin UK have subcontracted with the following organisations:

- Cable and Wireless UK, for the hosting and management of the Internet Data Capture facility;

- WTG Ltd, as sub-contractors to Cable and Wireless, to develop the online census interface and online help facility;
- Barron McCann, who will be providing laptops for field staff managers;
- Polestar, for the printing of Census questionnaires;
- UK Data Capture, for the operation of the Paper Data Capture site;
- Royal Mail, for the receipting of returned questionnaires;
- BSS, for the provision of the census helpline.

The contractual arrangements for the conduct of the 2011 Census in England and Wales are therefore quite complex, and this carries with it the potential to complicate the Information Assurance activities, and in the worst case, to raise inconsistencies of approach.

4.3. GROS

The primary commercial partner for GROS is CACI (UK) Ltd, who will be providing services for paper data capture and Internet data capture, including managing the printing of questionnaires, processing returned questionnaires at a dedicated Paper Data Capture site, and creating and operating the necessary Internet presence.

CACI (UK) have partnered with SecureWorks, a company with whom they have an established relationship, to act as their security assurance partners.

CACI (UK) have also contracted with the following organisations to provide the main Census services:

- Internet hosting aspects have been contracted to bright**solid**;
- The Internet facility development will be undertaken by TNS;
- The questionnaire printing has been subcontracted to DCK in Dublin, who were the CACI (UK) subcontractors for two successive Irish Census operations.

All other aspects, such as field staff recruitment, payroll functions and the operation of a contact centre, will be managed by GROS themselves.

The arrangements reflect the general approach by GROS, which is to retain a significant majority of the co-ordination work within their own organisation, buying in services where necessary. Of course, CACI (UK) are still responsible for managing the delivery of their contracted services, and also have an obligation to work as a partner to GROS, to ensure close cooperation. Nonetheless this is a relatively simple contractual relationship, and in IA terms it does place increased emphasis on the role of GROS as risk owners.

4.4. NISRA

At an early stage, NISRA reviewed the options available to them, and concluded that the best value for money solution would be to approach ONS with a view to combining key elements of their requirements into a single contract. This had worked satisfactorily in previous censuses and the review team recognise that

given the relatively small scale of the Northern Ireland project, the case for jointly procuring with ONS was compelling.

As a result of this decision, NISRA are joint signatories with ONS to the contracts with TNT and Royal Mail, and with Lockheed-Martin UK (and hence their subcontractors), as described in section 4.2 of this report. NISRA are however managing their own field force and fulfillment requirements. Completed questionnaires will be receipted at the sorting office at Mallusk, prior to being transferred to the UK Data Capture processing site.

NISRA have also agreed that the downstream processing of data gathered for the Northern Ireland Census will be conducted on ONS servers. This is being managed through a Memorandum of Understanding between ONS and NISRA. A link will be established between the NISRA offices and the ONS downstream processing systems, to allow NISRA staff to work on the quality of the data gathered.

These arrangements clearly do have valuable simplifying aspects both generally and in terms of Information Assurance. However, they also place the onus on NISRA to ensure that their organisation-specific aspects are reflected in both the contractual arrangements and in the delivery of the services.

5. Management of Information Assurance

5.1. General

The review team were charged with assessing the degree to which IA was being managed in each of the 2011 Census operations, starting from the level of senior management knowledge and commitment, through to a review of responsibilities and ownership, taking in a review of documentation and project plans, down to meetings with local teams at the major processing centres.

The team found solid management commitment within all three organisations to the aim of ensuring that the 2011 Censuses should maintain, and build upon the existing successful track records of securely managing previous census operations and census data. This commitment manifested itself throughout the management chain:

- The United Kingdom Census Committee (UKCC), the top level co-ordinating body for census activities across England, Wales, Northern Ireland and Scotland, invited members of the review team to present interim findings as the review progressed, and were active in tracking progress.
- Senior managers in GROS, NISRA and ONS attended all scheduled meetings with the review team, and took a keen interest in the development of the review as it progressed.
- At the operational level, each individual consulted within the project management and technical streams of ONS, NISRA and GROS was fully cognizant of the overriding importance attached to the protection of personal data gathered as part of the 2011 Censuses. Furthermore there was a keen sense of public expectations, and an understanding of the potential impact on the Censuses themselves, and upon the reputation of each organisation, that could arise from an incident involving personal data.
- All three Census Offices, under their accreditation process, established similar sets of personal, technical and physical IA measures.

During the course of the review, the review team made a number of observations to ONS, NISRA and GROS, as part of the terms of reference of the study. Those terms mandated that where the team felt that improvements could be made, there was an obligation to communicate those findings.

The team therefore offered up some suggestions, including:

- There was room for a more harmonized approach in some areas, such as ensuring a consistent mapping across the organisations on perceived levels of the potential worst case impact that might arise from an incident.
- A combined list of residual risks (across the three Census Offices) should be drawn up and reviewed, to confirm that there were no synergies between risks that could increase the vulnerability or impact.
- Particularly within the area of ONS/NISRA operations, there were opportunities for closer alignment of parallel activities such as risk assessment.

- It is inevitable that while some security activities can and should be carried out at the earliest possible stage, others such as testing, review and final approval, must necessarily take place very close to the final 'go-live' point. This leads to some project risk. The review team felt that for the 2011 Censuses those risks, and any associated late pressure on the approval authorities, should be managed with close attention.

The review team have no hesitation in stating that where recommendations were made for potential improvements, they were enthusiastically taken up within short timescales, which demonstrated both commitment and capability.

The fact that these suggestions were welcomed by ONS, NISRA and GROS should of itself be evidence of commitment to the thorough and effective management of Information Assurance. The fact that not only were they welcomed and adopted, but that they were also actioned, and that there was a desire to provide the team with evidence of progress, is a testament to the importance attached by all three to secure data management.

The evidence assembled during the conduct of this review points unequivocally to the conclusion there is a sound basis for effective information security management within the 2011 Census operations. Successful information security management begins with commitment, knowledge and personal responsibility. Without those as a basis, the implementation of technical and other measures will inevitably be less effective.

5.2. ONS

The scale and complexity of Census operations across England and Wales requires effective and close co-operation between ONS and their major business partners. This is true in all areas, but perhaps especially true in the area of information security, and clearly in this case the performance of the prime contractor is a critical factor.

The review team found an exceptionally effective partnership in this case. Not only had the commercial partners formed an integrated security team with their ONS counterparts, there was also a very clear sense of shared risk ownership within the community of partners, and between ONS and the prime contractor. This extended across all subcontractors on the primary data-gathering path, including printing activities, the Internet Data Capture facilities, and form processing. The review team visited the prime contractor and all major subcontractors and locations, and were uniformly impressed with the level of attention to security management, the activities of the main partners in delivering a cohesive security team, and the professionalism and knowledge of the individuals involved.

This of course did not happen by accident, and has come about through the guidance and clear direction of the very professional management team in ONS, as well as the personal and corporate commitment of their commercial partners, in particular the very strong IA focus engendered by Logica as a co-ordinating hub.

For other aspects (primarily the non-questionnaire printing tasks and the field staff recruitment, payroll and training activities), it could be argued that these carry with them a lower potential impact, since only limited information is held in each case. Nonetheless ONS, in common with NISRA and GROS, are keenly aware of

the potential impact of any incident affecting public confidence during the run-up to the Census. ONS continue to take steps to ensure that these activities are managed with the same degree of care and transparency as those in other areas of Census operations.

There is no doubt in the minds of the review team that IA requirements have been fully reflected in the planning and implementation of Census operations for ONS, and that the relationship between ONS and their prime contractor is a very reliable basis on which to move forward.

5.3. GROS

The General Register Office for Scotland operates within the context of the devolved administration and seeks to ensure that the Census is tailored to Scotland's requirements. Although the population for the census in Scotland is approximately one tenth of that in England and Wales, the population density is significantly lower, and the problems of access significantly greater. Added to this is the fact that the budget for the census in Scotland, in line with the smaller population, is significantly less than the budget for conducting the census in England and Wales. Census operations are of course made up in large part by a preparatory phase, meaning that while there is an element made up of variable costs (costs per head of population) there is also a very significant fixed, unavoidable component.

GROS have developed the 2011 Census project to reflect local circumstances and take advantage of their own organisational strengths. Even though it is a specialisation, GROS have a high proportion of staff with experience of previous census operations. That very solid core has been used to form a management team to direct both in-house and outsourced operations. It has also enabled GROS to tightly bound the outsourced operations, which in addition to making best use of available resources, retains key skillsets within the management team.

GROS recognise that this approach has implications for security management, and have responded by using a number of mechanisms to ensure effective communication and co-operation, such as the Census Security Assurance Group (CSAG), which supports the normal day to day cross-organisation security management activities. The CSAG has engaged in regular meetings with GROS's prime contractor, throughout the preparations for the 2011 Census.

The critical issue is that GROS are keen to maintain visibility of risks in outsourced operations, and to maintain control over those risks. Their approach is based on a clear understanding that the outsourcing of operations does not include the outsourcing of risk ownership.

The review activities included visits to the prime contractor and all major subcontractors and locations related to the Census in Scotland, and in each case the visit was fully supported by the senior management of the organisation, by GROS personnel, and by appropriate technical resources.

There is no doubt in the minds of the team that GROS have taken complete ownership of the issue of information security. There is equally no doubt that although the approach demanded by the very specific requirements of Scotland's Census has implications for security management, those challenges are being met by a disciplined and focused management team. GROS have a considerable challenge to deliver on the promise that they have set out, that of delivering "the

most secure census in the country's history". Nevertheless the review team are confident that the central base of accumulated skills and aggregated experience are sufficient to meet that challenge, and to provide a level of protection for personal information which will exceed expectations.

5.4. NISRA

As described in Section 4.4, NISRA have combined much of their operations with those of ONS, including paper forms processing and online data capture. In terms of personal data protection therefore, the same collection and processing standards to be applied in the case of ONS will apply also to information collected and processed as part of Northern Ireland's 2011 Census.

This is a very cost-effective approach; however, it does introduce a number of key risks:

- Where security requirements are amalgamated into a single contract, there is a risk that specific requirements become diluted or overlooked.
- There is a risk that NISRA will not have an effective level of control or of visibility over the implementation of IA measures.
- There is an allied risk that one party could become complacent, assuming that security is being managed on their behalf.

The team therefore examined the ONS/NISRA arrangements with a particular focus on the management and maintenance of responsibilities.

The team noted that during the contract specification phase, and throughout the procurement, NISRA were active members of the combined management team, and that they continue to liaise closely with ONS, and that NISRA are joint signatories on all Integrated Project Teams (IPT's), working alongside ONS and the relevant commercial partners.

NISRA have also examined areas for which they are solely responsible, ensuring for example that responsibilities for the protection of personal data have been allocated in full, and that those responsibilities are being discharged. The review team were provided with the opportunity to review these activities, including the production and maintenance of a security project plan, the production and maintenance of a risk register and Information Assurance strategy and implementation plan, and reviews to ensure that the appropriate standards are being enforced.

The team also noted that NISRA have the support of the security team in their parent Department, the Department of Finance and Personnel (DFP). The DFP security team provide IA advice and guidance in line with the Departmental IA framework, and are working closely with their ONS counterparts in the accreditation process for shared aspects. During the timescales of the independent review, the DFP team expressed their full confidence in the IA work being undertaken by NISRA in respect of the 2011 Census.

The team conclude therefore, that the NISRA IA requirements have been fully reflected in the arrangements with ONS, and with their joint commercial partners, and that NISRA are maintaining an appropriate level of liaison to ensure that both the specific Northern Ireland and wider requirements continue to be reflected in those arrangements. As is fully recognised by NISRA, the arrangements with

ONS do not diminish their responsibility to ensure the security of Northern Ireland's census data.

The team also conclude that those activities which are not being operated in conjunction with ONS includes an appropriate level of security management.

6. Gaining Assurance

6.1. General

The term ‘assurance’ has a specific meaning within the security environment. Assurance is gained through activities confirming that the security measures that have been set in place are both effective and appropriate. It is not sufficient simply to set in place an assembly of technical and procedural controls; they must work, they must be seen to work, and they must be aligned to the underlying security problem.

All three organisations have undertaken assurance activities, not just as a matter of adopting a professional approach and implementing best practice, but as a crucial part of the preparation for the accreditation process.

The review team found that in all cases, the assurance processes were comprehensive and thorough. The range of activities undertaken encompassed the technical security measures to be put in place for data processing systems, the physical security surrounding processing sites, and the procedural and personnel security issues underpinning the other areas. In all cases, independent verification was sought for the security of outsourced operations. That verification was not limited to technical vulnerability assessments, but also included an independent assessment of physical and procedural measures. The findings of these independent audit exercises were reported directly into the parent Census Office, and were in addition to the audits conducted in each case by the commercial partner and their security advisors. These were of course also in addition to the reviews conducted by the accreditation authority, themselves removed from the Census development and operation process in order to provide a degree of impartiality and objectivity.

The importance of gaining an appropriate level of assurance cannot be stated too strongly. Assurance confirms that the security measures that have been put in place are aligned to the problems that they are intended to address, and that they can be relied upon to operate as expected. Gaining assurance also highlights to the organisation the risks that must be accepted as part of business operations, either because it is not possible to address those risks, or it is not economically feasible to do so. That focus enables the organisation to ensure that the risks remain, and will continue to remain within acceptable limits.

6.2. ONS

6.2.1. Overview

The review team found that the ONS team were very much aware of any issues that had been brought up during the assurance activities, and had in all cases moved swiftly to address them. The team were particularly impressed with the inclusion (by ONS) of contractual assurance aspects as part of the process. Possible risks to the deployment of effective security arising from contractual complexity in service delivery had been assessed and where it was felt necessary, additional documentation and processes had been set in place to reduce that risk.

The review team understand that ONS will accredit all Census-related IT systems prior to use.

6.2.2. Technical Assurance

Wherever appropriate, equipment relied upon to enforce security in technical solutions such as Internet data capture, e.g. firewalls, has been verified as reliable, using an internationally recognised scheme for Government network security components.

The ONS Internet Data Capture system for the 2011 Census data collection process will be the subject of two separate technical vulnerability assessments.

The first will be conducted by a contractor working on behalf of the main commercial partner, and will consist of both a network test and an application level test. The network test will confirm the security of the underlying technical infrastructure, encompassing servers, networking components, firewalls etc., and will ensure that these components have been configured appropriately, and that any relevant, known vulnerabilities have been patched. The application level test will confirm that any higher level vulnerabilities such as a weakness to web-based attacks, or processing vulnerabilities within the application itself, have been detected and corrected.

The second will be conducted by an independent company (Sopra) reporting directly to ONS. That too will address both network level and application level vulnerabilities, and will also consist of a code review and static analysis exercise. Critical parts of the software making up the systems will be examined by experts to ensure that the development, implementation and testing have all been carried out to the necessary level. Automated source code scanning will be employed to help ensure that mistakes in the production of the software have been eliminated, so as to provide assurance that the delivered system does not contain known problems such as buffer overflow weaknesses.

All other IT systems (including ONS systems) used in the collection and processing of data for the 2011 Census will be subject to a process of technical vulnerability assessment followed by remedial actions where necessary in order to achieve accreditation. The only exceptions to this are systems that have been designed as standalone systems (with no external connections) sited within a physically secure environment incorporating an appropriate level of access control.

6.2.3. Physical and Procedural Assurance

The main data processing site for ONS was selected as the result of a twelve-month search of candidate sites, the security of the location being one of the major criteria. Throughout the fit-out process, audits and progress reports were conducted and provided by the security advisors to the main contractor. The site will be subject to approval by ONS as part of the accreditation process prior to live operation. The Centre for the Protection of the National Infrastructure (CPNI) provided an independent audit of the site.

All other sites used as part of the main data gathering process (including the hosting site for the Internet Data Capture service, and the questionnaire printing facility) have been the subject of formal physical security reviews by the security advisors to the main commercial partner, in addition to reviews which have been

or will be conducted by ONS themselves, both as 'informal' assessments and as part of the accreditation process. These are in addition to independent assessments such as validation against the international standard for Information Security Management (ISO 27001 series).

All the sites used for the paper data gathering and Internet data capture processes have local security managers, local security procedures and a local approvals process.

Other sites (relating to non-questionnaire printing processes, and the recruitment process) have physical security measures and supporting procedural measures which are approved, or are in the process of gaining approval, against either the ISO 27001 standard or the relevant Government standard.

6.3. GROS

6.3.1. Overview

The review team found the steps taken by GROS to achieve assurance in Census operations to be in line with best practice. Rather than relying on a single party to provide assurance, the GROS team have employed a combination of supplier evidence, independent assessment through a direct contract with Logica, and in-house review.

The review team understand that GROS will accredit all Census-related IT systems prior to use.

6.3.2. Technical Assurance

Wherever appropriate, equipment relied upon to enforce security in technical solutions such as Internet data capture, e.g. firewalls, has been verified as reliable, using an internationally recognised scheme for Government network security components.

Technical vulnerability assessments will be conducted on all Internet systems used for data capture during Scotland's Census, and on all systems used in the processing of Census data.

Before live operation, all systems implemented by CACI (UK) or their subcontractors will have been the subject of technical security assessments conducted by their security advisors, with the results made directly available to GROS for discussion and review. This includes the systems at the main data capture site, the Internet public assistance service and the Internet data capture service. The Internet data capture service, in particular, will be subject to both infrastructure and application level tests. The infrastructure test will confirm the security of the underlying technical infrastructure, encompassing servers, networking components, firewalls etc., and will ensure that these components have been configured appropriately, and that any relevant, known vulnerabilities have been patched. The application level test will confirm that any higher level vulnerabilities such as a weakness to web-based attacks, or processing vulnerabilities within the application itself, have been detected and corrected.

All GROS IT systems used in the collection and processing of data for the 2011 Census will be subject to a process of a technical vulnerability assessment followed by remedial actions where necessary in order to achieve accreditation.

Drafts of the initial findings of the technical vulnerability assessments were made available to the review team.

6.3.3. Physical and Procedural Assurance

The CACI (UK) and subcontractor sites have been subject to a series of physical and procedural reviews by the security advisors to the prime contractor to GROS. This includes the main data processing site, the site hosting the Internet data capture services, and the printing facility. The results of the reviews have been made directly available to GROS for discussion. These are in addition to reviews which have been or will be conducted by GROS themselves, both as 'informal' assessments and as part of the accreditation process.

In addition, Logica have conducted an independent physical and procedural review of the Internet services site, a review of an example Field Office, the contact centre site, a review of the main data capture installation and a review of field office security.

All the sites used for the paper data gathering and Internet data capture processes have local security managers, local security procedures and a local approvals process.

6.4. NISRA

6.4.1. Overview

The assurance processes described for ONS apply also to the elements shared with NISRA, and NISRA have worked with ONS to define and review the assurance requirements as a combined work package. As stated in Section 4.4, these arrangements between NISRA and ONS place increased emphasis on the NISRA-specific elements of the IA measures.

The review team understand that the DFP security team will support ONS in the accreditation of all Census-related IT systems prior to use.

6.4.2. Technical Assurance

All NISRA-owned IT systems used in the processing of data for the 2011 Census will be subject to a process of technical vulnerability assessment followed by remedial actions where necessary in order to achieve accreditation.

Other than the systems used by ONS and their commercial partners, the review team understand that no other IT systems will be used by or on behalf of NISRA for the processing of 2011 Census information, before the data is passed on to NISRA-owned systems for output production.

6.4.3. Physical and Procedural Assurance

Two Government buildings will be used by NISRA to house their Census 2011 operations. Both are subject to the baseline level of physical and procedural protection applied to all Government buildings, which have been additionally strengthened with internal controls over areas used to house the information. These are subject to the normal DFP accreditation process.

Other than those used by ONS and their commercial partners, and the NISRA locations set out above, no other locations will be used by or on behalf of NISRA for the processing of 2011 Census information.

Annex: Census Offices Description of the Census Operation

Introduction

This Annex contains a description of census operations as provided by the three Census Offices. It is provided for information only.

The Censuses

The United Kingdom censuses are ten yearly compulsory counts of population and housing. The information obtained in a census is used by government, local authorities, health providers, commercial businesses and other users to develop their policies and plan services effectively. As billions of pounds of public money is distributed using census figures it is vital that we reach and engage with every individual. If, for example, people are missed, there may not be enough funds allocated for health care or education in a particular area.

A full census has taken place in Great Britain every ten years since 1801, with the exception of 1941. In 2011 Census Day in the UK is 27 March 2011.

The Office for National Statistics (ONS) is responsible for carrying out the 2011 Census in England and Wales. A census for Scotland is being planned and managed by the General Register Office for Scotland (GROS) and for Northern Ireland by the Northern Ireland Statistics and Research Agency (NISRA).

The ONS is overseen by the UK Statistics Authority and produces independent information to improve the understanding of the UK's economy and society. Reliable and impartial statistics are vital for planning proper allocation of resources, policy making and decision making to ensure a fair society. The UK Statistics Authority was established on 1 April 2008 by the Statistics and Registration Service Act 2007 as non-ministerial department, directly accountable to parliament.

The GROS is part of the devolved Scottish Administration. It is headed by the Registrar General for Scotland, who reports to Scottish Ministers.

The NISRA is an Executive Agency within the Department of Finance and Personnel (Northern Ireland). NISRA's Chief Executive is also the Registrar General for Northern Ireland.

Uses of the Census Data

Governments, local authorities, the health sector, businesses and market researchers, academic researchers and the education sector, community groups, genealogists and the public at large rely heavily on census results for a countless range of purposes. The six main uses of census data are:

- Resource allocation – for resource allocation it is crucial that population counts (both total counts and key characteristics) are accurate, consistent and comparable between areas.

- Targeting investment – for many government funding uses, data must be consistent nationally to allow investment to be made in the areas where it is most needed.
- Planning – basic population counts by key characteristics such as age, sex, ethnic group, household type and size are important for planning. If the different characteristics of an area's population can be identified, plans can then be made for the sort of services necessary. Information on small areas and small groups of the population are crucial in local planning.
- Policy making and monitoring – there is a clear drive across government for policy initiatives to be evidence based. Since many initiatives are implemented and assessed at a local level, census data on population size, age, sex, migration etc. are of key importance.
- Academic and market research – the ability to produce statistics for small areas is vital for many research uses. Basic population counts and counts by characteristic are also required.
- Statistical benchmarking – more generally, census data are employed to improve the quality of many other statistics, which may also be used for the above.

The 2011 Censuses: How Do the Censuses Work?

The Address Register

The address register underpins the entire census operation in England and Wales. Addresses are printed on each household questionnaire for postal delivery. Questionnaires are hand delivered to communal establishments (e.g. hospitals and care homes, or caravan parks). These addresses also provide the spine of the questionnaire tracking system, which is used to target non-response follow-up activity.

There is no single authoritative source of national address information in England and Wales that fulfils the requirements of the census. Therefore the census has developed an address register that brings together unique addresses from other data sources that have either national coverage (e.g. Royal Mail Postal Address File (PAF) or National Land and Property Gazetteer) or that cover a particular type of establishment. This information has been supplemented by a separate address check of approximately 15% of the postcodes in England & Wales, where there was least certainty in the address register.

In Northern Ireland, a single address database (POINTER) for use throughout government has been developed through the integration of a number of administrative sources such as those relating to valuation, domestic rates and Ordnance Survey Northern Ireland. NISRA has worked with other parts of government and Royal Mail to produce a Census Address Register, based on POINTER, that meets Census requirements. The linkage to POINTER provides a grid-reference for all properties which will support both enumeration processes and, ultimately, the creation of outputs. In the period immediately prior to Census Day, when Census forms are being delivered, enumerators will perform an address check based on the Census Address Register.

GROS also require accurate address and postcode based products for the Census operation in Scotland. A definitive high quality national address register is not yet available for Scotland but GROS has carried out research on the quality of address information and has identified suitable products. Residential addresses, non-residential addresses and communal establishments have been identified using the PAF. This has been supplemented with appropriate material from other sources such as Local Authority planning offices and the Assessors Portal.

GROS has created postcode look-up files and address files from the address register to manage the census field operation, to personalise questionnaires and Enumerator Record Books (ERBs), to support warehouse and processing operations and support creation of outputs.

Questionnaire Delivery

All households in England and Wales will receive a census questionnaire pack through the post. Questionnaire packs contain a census questionnaire together with an information leaflet and a pre-paid envelope for return by post direct to the census Data Capture Centre. Communal establishments (i.e. managed accommodation, such as care homes, army bases, hostels, etc.), and special groups (such as rough sleepers and travellers), will be hand delivered a questionnaire pack. Questionnaire packs for communal establishments are similar to household packs. In Wales, questionnaire packs contain both an English language and Welsh language questionnaire.

The delivery of questionnaires in Northern Ireland will follow the England and Wales model, with postal delivery to households and enumerator delivery to communal establishments. The single exception to this is households in rural Fermanagh where addressing issues have led NISRA to use enumerator delivery.

In Scotland 94% of census questionnaire packs will be hand-delivered by enumerators. The remaining 6% will be delivered by Royal Mail in mainly rural areas. New addresses found during the field operation will be added to the ERB and a questionnaire pack will be delivered to the address. Information obtained for new addresses and any address changes will be captured and used for subsequent statistical analysis and output creation.

Return and Collection of Questionnaires

In England and Wales householders can complete their questionnaires and return them by post or are able to complete an on-line questionnaire. Each household questionnaire is pre-addressed, and contains a unique internet access code (IAC, required to access the online census) and bar-code linked to the address. For household questionnaires that are returned by post, the identifying bar-code (which is visible through the return window) will be scanned by Royal Mail for ‘receipting’ purposes and this information uploaded onto the questionnaire tracking systems. Submission of the completed online census also updates the QT. Knowing that a return has been received from a household either on paper or online means that it does not need to be followed up.

In communal establishments, each individual is given a questionnaire pack which contains the census questionnaire, an information leaflet, and a privacy envelope. Questionnaires are collected by the special enumerator and transferred to the census data capture centre at a later time (either through the post or by secure

courier). Individuals within communal establishments also have the option of completing their questionnaire on-line in the same way as households.

The procedures in Northern Ireland for return and collection of questionnaires are exactly the same as in England and Wales.

Householders in Scotland can complete their questionnaires and return them by post to a local census field office or they can complete their questionnaire on-line. If a household is listed on the address register their questionnaire will have a pre-printed address and a unique internet access code (IAC) and the householder can use this IAC to access the on-line census. Enumeration of communal establishments is carried out by census team leaders. All questionnaires are completed on paper, collected by the census team leader, and included with the other completed paper questionnaires for their respective area.

It is likely that some households will require additional materials. Households with more than six people in England and Wales and Northern Ireland (or five people in Scotland) will require a continuation questionnaire; households may want to be sent assistance material, or may have lost or damaged their census questionnaire and need a replacement. Such materials can be ordered online or via requests to the census helpline – they will then be sent out by post (or hand-delivered in Scotland). Census field staff can also provide additional material on the doorstep.

The Questionnaire Tracking System

In England and Wales the Questionnaire Tracking (QT) system enables the tracking of every questionnaire from delivery until return to the data capture centre. The QT tracks each questionnaire by means of the unique ID number and barcode printed on each questionnaire, or by means of the IAC for returns submitted online. By scanning this unique barcode printed on each questionnaire the QT can be updated with any additional or replacement questionnaires delivered to households.

The QT will provide real time information on response rates, enabling census managers to direct field staff to areas where response is lowest. It also enables the ONS to know the response status of each address, both during and after the census.

The questionnaire tracking system in Northern Ireland is the same as that in England and Wales.

In Scotland, questionnaire tracking is carried out during enumeration and at the data capture centre. During enumeration tracking of questionnaires is the responsibility of field staff. Regular management reports are submitted by staff and collated by managers for their area. Summary reports are also provided to census HQ along with reports from Royal Mail. At the data capture centre questionnaires are tracked by unique questionnaire ID and daily progress information is supplied to GROS on internet questionnaires completed and paper questionnaires scanned.

Follow-up

In England and Wales census field staff will be employed to visit households that haven't returned a questionnaire and encourage and assist householders to respond. Each collector will be provided with a follow-up list, listing all non-responding households from the QT that require a visit. Census coordinators

(team leaders) will be monitoring response across their area and will be deploying the collectors to the areas with the lowest response to ensure that the variation in response is reduced. The follow-up period lasts until 6 May.

The Northern Ireland follow-up process is very similar to that in England and Wales, except that each enumerator will be allocated to a fixed area. The enumerator will already have conducted the address check within that area, and will then carry out all follow-up within the same area.

In Scotland non-responding households and households that fail to provide a acceptable level of response will be identified by enumerators via their ERB. The enumerator will make attempts to contact the householder to obtain the missing information, and if appropriate contact is made, will try to get the householder to complete the questionnaire immediately, or arrange a suitable time for collection or provide a return envelope for the questionnaire to be posted back. The follow-up period lasts until 25 April. After the end of follow-up, enumerators will carry out a final tally of questionnaires received and reconcile it with the ERB. Questionnaires are sorted, boxed and passed to the local census team leader with the ERB and a reconciliation summary for further checking by both the census team leader and the local census district manager. When these final checks have been completed, the boxed questionnaires and ERBs will be uplifted by the logistics contractor and delivered to the paper data capture centre.

Refusals

It is mandatory for members of the public to complete census questionnaires. Census field staff will encourage responses, and will provide assistance, but persistent refusals will be reported to the census coordinator for non-compliance procedures to be initiated. This may ultimately result in prosecution.

Assistance Completing the Questionnaire

Although the questionnaire has been designed and tested to be easy to complete, some households will need assistance completing their questionnaire due to language challenges, difficulty reading English, or a disability, for instance. A wide range of assistance is available, including: online help; online audio and British Sign Language clips; the online census is readable by commonly used screen readers used by the visually impaired; translation booklets of the questions in the most commonly used languages; etc. The census helpline can also provide help. Additional materials requested online or via the census helpline will be posted out to the household. Census collectors can provide help and additional materials, on the doorstep.

Census Coverage Survey

To ensure that the census produces the most accurate snapshot of the population, a Census Coverage Survey (CCS) is conducted immediately following the census follow-up period. The CCS is a short doorstep interview carried out in a one per cent sample of postcodes in England and Wales and a 1.5% percept sample in Northern Ireland and Scotland; the survey starts on 9 May in England and Wales and Northern Ireland and 7 May in Scotland. The CCS is used to estimate the number of people and households that didn't respond to the census; these households and people are then imputed into the final published results.

Data Capture and Coding

In England and Wales all paper census and CCS questionnaires are returned direct to the census data capture site in Manchester. Here the paper questionnaires are scanned and the data captured automatically using Optical Character Recognition (OCR) and Optical Mark Recognition (OMR) software. Any snippets of text that can not be automatically captured will be keyed from an image of just the relevant word or phrase. The write-in responses (e.g. country of birth; occupation, etc.) are also coded (i.e. given a standard classification number) – the majority will be coded automatically, with the remainder manually coded. The census data centre (which stores both the information captured from paper, and the online census returns) is based at the same site in Manchester. At the end of data capture, and only after ONS has given authority, the paper questionnaires are securely shredded and environmentally recycled.

Paper census forms and CCS questionnaires for Northern Ireland will be processed along with those for England and Wales at the same site in Manchester.

In Scotland all data capture and coding activities are carried out in geographical order at our data capture centre. Paper questionnaires are delivered in boxes by the logistics contractor from local field offices to the data capture centre. Boxes are receipted and reconciled with information from the field operation. Questionnaire images and data are captured using scanning and recognition technology and paper questionnaires receipted are reconciled with information from the field operation. Data that is not captured automatically is keyed by operators. Data from online questionnaires is amalgamated with captured data from paper questionnaires. Most textual responses are converted into coded values via classifications using automatic and computer assisted manual methods. Captured and coded data is validated using pre-defined rules. Finally, data outputs are generated in geographical order and delivered to GROS.

Downstream Processing

Once the census data is captured and coded the database is securely passed to the England and Wales census HQ in Hampshire, where the data undergoes further validation routines (e.g. to identify and correct incorrect responses – such as 3 year old dentists). The clean and corrected data then undergoes further quality assurance checks, for example checks against aggregate administrative data (e.g. are the number of children from the census in an area consistent with the number of children receiving child benefit in that area). The final stage of processing before publication is Statistical Data Control (SDC) – see below.

Data for Northern Ireland will also be delivered to the ONS site in Hampshire for downstream processing. While the data will held and processed at ONS, NISRA staff will analyse the Northern Ireland data.

Captured and coded data for Scotland is delivered to GROS in Edinburgh where cleaning, correction, quality assurance and SDC takes place.

Producing Outputs

The anonymised and Statistical Data Controlled census information is then passed to the census outputs statisticians, who aggregate the data into agreed table formats, and prepare the data for publication (primarily online, but also on other medium). The first census outputs are planned for release in July 2012, consisting of population estimates, as at census day, by age and sex for each local authority.

More detailed statistics for the rest of the information on the questionnaire, and for smaller geographies, will be released during 2013.

The smallest areas for which results will be published are 'Output Areas' – which typically consist in England and Wales and Northern Ireland of 125 households and about 250 people (50 households and about 120 people in Scotland). No identifiable individual information is published. No census personal information is made available to marketing companies, local authorities or government departments.

Protecting the Confidentiality of Individual Information in Published Results

Publishing data in any format does carry a risk, to some degree, that an individual, household, or organisation may be identified in the published statistics and confidential information released, and the risk increases as the level of detail in the published statistics increases. The UK Census Offices therefore will take a number of approaches to make useful data available, whilst protecting against such risks. Statistical disclosure control is an attempt to balance the utility (or statistical value) of published statistics against the potential for disclosure of confidential information. In order to achieve this balance the Census Offices will adopt a range of techniques which modify or summarise the 2011 census data. As in previous censuses, precautions will be taken so that published tabulations of census data are in line with the Census Acts, the Statistics and Registration Service Act 2007 and the Code of Practice for Official Statistics.

Extensive research has been undertaken by the Census Offices to determine the most effective ways of protecting published census statistics, drawing on academic and international expertise. This research has resulted in the following suite of methods to protect aggregated 2011 Census outputs:

- Restricting the number of output categories into which a variable may be classified, such as aggregated age groups;
- Where the number of people or households in a geographic area falls below a minimum threshold, the statistical output - except for basic headcounts - will be amalgamated with that for a sufficiently large enough neighbouring area;
- modifying some of the data before the statistics are released through 'record swapping', where records with similar characteristics are swapped with a record from another geographic area.

For some more detailed tables, where the impact of disclosure control on the usefulness of the data is too great, special access arrangements will be put in place for approved researchers, as defined in the Statistics and Registration Service Act.

Anonymised Micro-data Samples, and Safe Settings

Microdata are samples of individual and household records drawn from the census data, which have been anonymised to protect confidentiality. The microdata samples have been used by academics and researchers to develop more sophisticated analyses of population data than are available from the standard published census tables, for example in studies of the health and labour market status of specific groups within the population such as carers, the disabled and ethnic and religious minorities.

The availability of such samples was a major, and successful, innovation of the 1991 Census, and these were extended in 2001. Following the 2001 Census five samples of microdata were produced, each involving 5% or less of census records. Access to this data was controlled securely, with access to the samples containing a more detailed level of information being provided only under supervision in the safe setting of Census office premises.

Proposals for microdata samples for 2011 are at an early stage but will be developed in light of the disclosure control methodology applied to the underlying data, access arrangements and licensing issues.

Glossary

BCS	British Computer Society
CESG	Communications Electronic Security Group
CIPCOG	Civil Information Assurance Products and Services Co-Ordination Group
CLAS	CESG Listed Adviser Scheme
CCTM	CESG Claims Tested Mark
CSAG	Census Security Assurance Group
DCK	DC Kavanagh
DFP	Department of Finance and Personnel
GCHQ	Government Communications Headquarters
GCSx	Government Connect Secure Extranet
GIPSI	General Information Assurance Products and Services Initiative
GROS	General Register Office for Scotland
HMG	Her Majesty's Government
IA	Information Assurance
IAMM	Information Assurance Maturity Model
IIAR	Independent Information Assurance Review
IISP	Institute of Information Security Professionals
IPT	Integrated Project Team
ISO	International Organization for Standardization
IT	Information Technology
MBA	Master of Business Administration
MSc	Master of Science
NISRA	Northern Ireland Statistics & Research Agency
ONS	Office for National Statistics
PIA	Privacy Impact Assessment
SC	Secure Computing
TIGER	A not-for-profit security tester certification scheme
TNS	Team Netsol Ltd
UK	United Kingdom
UKCC	UK Census Committee
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism