Scotland's Census 2011
Shaping our future

Overview of security for Scotland's Census

January 2010

Table of Contents

1. Introduction

1.1 General Register Office for Scotland (GROS) has been responsible for collecting sensitive information and holding it securely for over 100 years, this is part of our core business. We have always had processes and procedures in place to manage and handle sensitive data securely.

1.2 GROS has its own Information Security branch which is responsible for the security of information across all GROS businesses. Their main tasks include ensuring that all GROS staff are appropriately trained in security procedures which our reputation relies on.

1.3 Security of census information has always been a high priority for each census over the years but in more recent times there has been keen interest by the media in publicising security incidents, mostly around the inappropriate handling of sensitive information by Government bodies. This has led to the general public having less confidence in the ability of Government bodies to look after the public information, which has a knock-on effect for 2011 Census.

1.4 This paper provides a high level view of how we are addressing security for the 2011 Census to ensure the public can be confident their census information will remain confidential.

1.5 A Privacy Impact Assessment report, "Considerations of the Impact on Public Privacy of Scotland's Census", is also being produced which will be published on our census website shortly.

2. Who's involved?

At GROS

2.1 We recognise that security affects every part of the census operation and our census security team now consists of four security experts. Although the team is dedicated to census they ultimately report to the Head of Information Security at GROS thus ensuring that the application of security controls across GROS is kept consistent and that both the Census Security team and other Information Security staff can keep up-to-date with the ever-changing Government security standards. They work closely with their IT Security colleagues in Scottish Government sharing good practise procedures.

2.2 GROS also contracts with Logica who provide expert security consultants to review the security measures we have put in place and to carry out specific security testing and risk assessments on our behalf. This provides GROS with external assurance that we are adhering to the relevant Government security guidance.

2.3 Technical - GROS needs to ensure all services conform to the mandatory requirements of Her Majesty's Government (HMG) Security Policy Framework. This is supported by compliance with the Communications-

Electronics Security Group (CESG) Information Assurance Standards 1,2,4,5,6.
In addition to these government standards, GROS will ensure the census complies with the International Security Standard (ISO27001) and the 2011 Census Confidentiality Declaration and Guidelines. All internet services will also be compliant with eGovernment Security Assurance Framework (eGSAF) where required.

2.4 The GROS Census Security Assurance Group (CSAG), which includes representatives from key operational areas across census and from the contractors, oversees progress and provides Information Security direction to the programme, making key security decisions at a strategic level as required.

Contractors

2.5 Census relies heavily on the expertise of contractors to deliver some of the main census services. These include printing the questionnaires, developing and hosting Internet services, transporting the questionnaires around the country, and capturing and processing the data. Our prime contractor, CACI(UK), has employed the services of DNS, an Edinburgh based security consultancy, to carry out security checks on all services which CACI(UK) are contracted to provide. DNS provide independent assurance to GROS that CACI(UK) is adhering to their contracted security requirements.

2.6 GROS is working closely with CACI(UK) to ensure that captured census data is processed and stored securely. Although CACI(UK) will have access to the full census dataset (for essential maintenance and support functions) this access will be controlled and managed by GROS. Their contract contains restricting sections to ensure that, for example, public concern over the existence of the US Patriot Act has been considered and acted upon.

Working with ONS

2.7 GROS participates at the ONS security board and our census security manager has regular updates with her ONS counterpart to ensure consistency of approach, where possible, and to share best practise.

External Assurance

2.8 In 2008 GROS agreed additional measures with other UK census organisations which would help ease public concern over Government ability to keep information safe. We collectively agreed that an external UK-wide census security review team would be commissioned to review the security arrangements in place for each census taking organisation. It would cover reviewing the security procedures put in place by both the organisation and by their respective contractors, advising each organisation of any further work required, and finally providing reassurance to the public through the best possible means.

This review is being led by John Dowdall, the former Northern Ireland Assembly Comptroller and Auditor General, who will appoint a team of expert security consultants to help him with this assurance.

3. What do we all do?

In the Field

3.1 GROS needs to ensure that the appropriate security arrangements are in place in all areas of the operation. These arrangements include background checks during recruitment of nearly 7,000 staff; security awareness training including the storing/handling of questionnaires in enumerator's homes; appropriate encryption of laptops and other hardware security; password protection for access to systems.

3.2 But there are some difficult decisions to make to balance the need to take heed of all security guidelines against the need to actually carry out the operation in the timeframe available. These are the types of risks that come before CSAG so that an informed recommendation can be made to the overall risk owner.

IT systems

3.3 All IT systems require to undergo security testing e.g. application and penetration testing and Risk Management Documentation Sets (RMADs) are produced for each service.

Internet

3.4 The Internet services undergo rigorous penetration testing both by DNS and by Logica. The services are hosted at brightsolid who are experienced in handling sensitive financial and defence information and with whom GROS has contracted before. The on-line completion service can only be accessed through a unique Internet Access Code and matching postcode, found on the front of the household's delivered questionnaire. This is supplemented by the creation of a personal password which always remains under the control of the respondent.

Processing Site

3.5 At the processing site the GROS Operational Management Team remain on site throughout the processing period. They carry out management and control functions which allow them to oversee activities at the site that require the contractor access to questionnaires and data. GROS is responsible for the data set wherever it resides, e.g. on the database; in transit to the microfilm processors; the backup tapes; in transit from the Internet Services site. GROS reviews the training programme for the operators and provides risk assessments of the site itself including where the paper questionnaires are warehoused and the operational processes on site.

3.6 Once the dataset and images are transferred to GROS they reside on an isolated area of the secure GIS network. Access is strictly limited to only those staff requiring sight of the data e.g. for downstream processing by the statisticians and for output generation and dissemination.

Helpline

3.7 All staff working on the Helpline are recruited through the Scottish Government contract with Pertemps and all sign the Census Confidentiality Undertaking. This ensures that all staff are contracted to keep conversations with the public confidential e.g. helping the public to complete the questionnaire over the phone, and this is a full part of their training.

3.8 More information on the security procedures in place across the programme can be read in the PIA document, "Considerations of the Impact on Public Privacy of Scotland's Census".

4. Summary

4.1 Security is at the heart of census operations and continues to be considered through all stages of design and development of services for 2011.

4.2 GROS strives to adhere to all security guidelines and continues to ensure that all staff and contractors across the operation are fully aware of their obligations to confidentiality.

4.3 This work is ongoing but GROS has the appropriate procedures in place to assure ourselves that the good work of our contractors and of our own teams continues to progress and that all security risks are properly assessed and agreed on at the appropriate level.