The SRS Assured Organisational Connectivity (AOC) scheme

Tony Chapple and Andrew Engeli
Introduction

1. The Policy Wrap-Around: the Five Safes Framework
2. Safe settings
3. How Assured Organisational Connectivity Works
4. Assured Organisational Connectivity agreements and certification
5. How to sign an Assured Organisational Connectivity agreement
6. Certification
7. Access
8. Breach policy
The Secure Research Service (SRS)

• Formerly known at the VML, service in existence since 2003 to provide secure access to official sensitive data

• Service allows linkage of datasets on common variables/UI under conditions that guarantee confidentiality (non-identification) of research subjects

• Data held are derived from three sources:
  ✓ ONS-owned datasets (e.g. Census)
  ✓ Datasets with external IAO (e.g. IBRD, NPD)
  ✓ Datasets ingested by Accredited Researchers

• Research Services and Data Access (RSDA) has lead role in accrediting researchers and projects under Digital Economy Act, 2017 (‘The Act’)
The Act

• Gives Public Bodies a clear way to share data, for research, for the first time
  ✓ Comparable with established ONS approach

• UK Statistics Authority to accredit Researchers, Projects and Processors
  ✓ ONS is a Data Processor

• UK Statistics Authority to act as the secretariat for the national Statistician’s Data Ethics Committee (NSDEC)

• Public Bodies still need to be assured that data will be kept confidential at all times, and that research will only be permitted when judged to serve the public good
The Policy Wrap-around: the Five Safes
Safe settings

Researchers can access data in the SRS in two ways

**Safe rooms**

- Located at ONS sites, other government departments, academic institutions, or ESRC Safe Pods
- Controlled access for Accredited Researchers from host and other organisations

**Assured organisational connectivity**

- Safe settings set up in academic or business premises after agreement with ONS, complying with our security standards, annual certification
- Access for designated Accredited Researchers from the assured organisation only

Access arrangements are subject to Data Owners’ agreement
# How AOC works

<table>
<thead>
<tr>
<th>Number of people who can access where machine is located</th>
<th>Number of accredited researchers who are credentialled on machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>one</td>
<td>one</td>
</tr>
<tr>
<td></td>
<td>Typically a single office</td>
</tr>
<tr>
<td></td>
<td>Single office with access to other members of a team</td>
</tr>
<tr>
<td>many</td>
<td>many</td>
</tr>
<tr>
<td></td>
<td>Open plan office or lab where others may be non-ARs</td>
</tr>
<tr>
<td></td>
<td>Often found in Government departments</td>
</tr>
</tbody>
</table>
Assured Organisational Connectivity works within a two-part framework; the AOC agreement and the AOC certification

- The AOC agreement is typically signed for a period of five years
  Each organisation will typically only ever have to sign one agreement at a time.
  After five years, organisations may apply to renew their agreements.

- AOC certification takes place on an annual basis
  It will typically be granted as long as all requirements are met.
  Before any accredited researchers can apply for remote access an organisation will need to have current AOC certification.
To apply for an agreement

Organisations will commit to keeping a current and up to date:

a) Register of machines (MAC addresses)
b) Register of locations (IP addresses)
c) Register of researchers and accounts authorised for access
d) Breach policy

Agreements will be signed by:

a senior decision maker with financial and legal authority

and

a named senior IT decision maker with legal authority
Certification

- Registers to be kept up to date
- Changes communicated to Security and Operations team at SRS
- Site inspection to be permitted within 5 working days of notice
- Compliance with all conditions of AOC agreement
- Named individual to keep registers and named individual for operational and security questions
Access

• Access permitted to staff on permanent or long-term contracts
• Must be Accredited Researchers under the Digital Economy Act 2017 or Approved researchers through ONS scheme
• AR’s will request access by filing AR Access registration form, countersigned by organisation
• No connectivity to machines which are not wholly owned and under the control of the organisation
• Connectivity only through fixed connections (no wifi)
• No connectivity through VPN
Breach policy

• The Breach Policy needed for an agreement to be signed must address organisational processes to address:
  a) Cases of individual researcher misconduct
  b) Cases of systematic researcher misconduct
  c) Cases of IT breaches

• Provision in place for confidential peer to peer reporting of major cyber attacks/breaches
Questions?