CONFERENCE OF EUROPEAN STATISTICIANS
Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality Session 1
29-31 October 2019, the Hague, the Netherlands 23 September 2019

Accessing Data in the ONS Secure Research Service: A Certification Regime for Remote Connectivity

Andrew Engeli (Office for National Statistics)
andrew.engeli@ons.gov.uk

Abstract and Paper

In line with the GBR Digital Economy Act, 2019 ('The Act'), the Secure Research Service of the Office for National Statistics has conducted a policy review of the conditions under which microdata may be accessed for research purposes in the public benefit, using a remote connection to the SRS data service. The SRS has developed a new certification scheme for allowing remote organisational connectivity which is replacing the ad hoc framework that has been used up to this point. The new certification scheme enhances the safety of remote settings through the sharing of risk and the monitoring of researcher conduct with the organisations who employ them. The certification scheme provides an additional guarantee to information asset owners (IAO) and enhances the ability of the ONS/SRS to acquire new official sensitive datasets for research purposes.

Accessing Data in the ONS Secure Research Service: A Certification Regime for Remote Connectivity

Andrew Engeli*

* Office for National Statistics (GBR), andrew.engeli@ons.gov.uk

Abstract: In line with the GBR Digital Economy Act, 2019 ('The Act'), the Secure Research Service of the Office for National Statistics has conducted a policy review of the conditions under which microdata may be accessed for research purposes in the public benefit, using a remote connection to the SRS data service. The SRS has developed a new certification scheme for allowing remote organisational connectivity which is replacing the ad hoc framework that has been used up to this point. The new certification scheme enhances the safety of remote settings through the sharing of risk and the monitoring of researcher conduct with the organisations who employ them. The certification scheme provides an additional guarantee to information asset owners (IAO) and enhances the ability of the ONS/SRS to acquire new official sensitive datasets for research purposes.

1 The Secure Research Service and the Five Safes Framework

The Secure Research Service (SRS) operates within the Five Safes Framework, a set of principles that safeguard access to the sensitive data that are available for use by appropriately trained and accredited members of the research community (Accredited Researchers - AR). Annex 1 gives a summary of the Five Safes Framework.

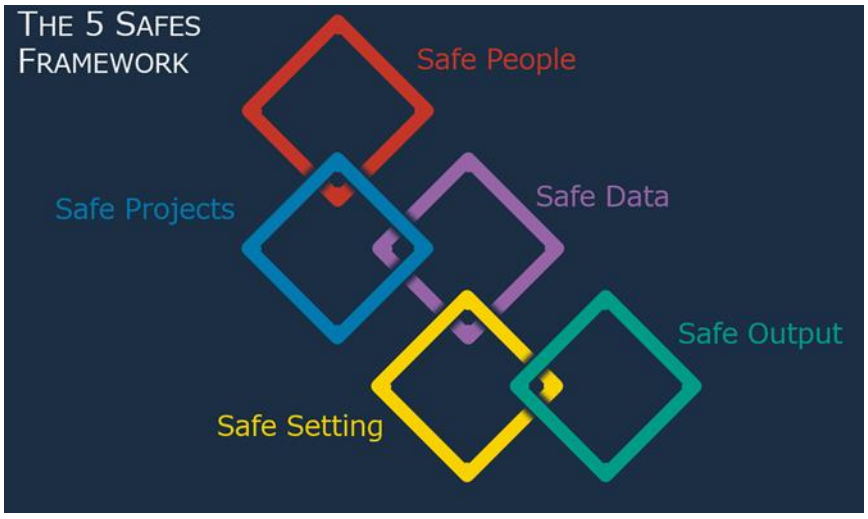

Fig 1.1 The Five Safes Framework

The SRS is an accredited data processor under the United Kingdom Digital Economy Act 2017 (the Act). This means that the SRS does not own the data that is made available through the service and information asset owners are separately identified in the Act. It is important that information asset owners have a thorough understanding of how the safe settings component of the framework operates as it is their responsibility to specify the conditions under which their data can be accessed (through the SRS Data Deposit Agreement).

Currently, the SRS supports access to data in two kinds of safe settings: safe rooms and through Assured Organisational Connectivity (AOC). Both methods operate alongside the other 'safes' in the framework to provide a secure research service, but there are important differences between them. This paper is a guide for external stakeholders interested in understanding the certification scheme, by explaining each in more detail and giving a summary of the security controls that are in place.

2 Safe Rooms

Fig 2.1 Safe rooms as safe settings

Safe Rooms are safe settings that have a number of fixed terminals that are dedicated for secure research and which are access controlled through a booking or reservation system. Safe rooms will typically be equipped with video cameras or other monitoring systems. Safe rooms are generally open to all accredited researchers irrespective of whether they are full time employees of the organisation operating the safe room.

The SRS maintains a safe room at each of its sites in Newport, Titchfield, and London. In addition, there are safe rooms available to accredited researchers in Belfast and Glasgow, and there is a growing Safe Room Network available at research sites across the UK (up to date details of locations may be obtained from us). ONS is interested in promoting the

regional and geographical reach of its services and in ensuring access to all segments of the researcher community and works with research organisations and data infrastructures who are interested in hosting safe rooms. Safe rooms share the following characteristics:

- Controlled access via key swipe/keypad
- Dedicated terminals without internet access
- Booking/reservation system
- Cameras and physical other security controls

UK Research and Innovation (UKRI), through the Economic and Social Research Council (ESRC), is investing in the provision of a network of safe rooms which share these characteristics through its 'safepod' programme at selected universities around the country. Safepods are purpose built modular enclosures that have all the features and security controls of safe rooms. They provide a cheap and efficient alternative to installing purpose built safe rooms and can be positioned in existing research facilities such as libraries. Once the safepod network has been installed and accredited by the ONS, it will provide additional safe room access to the SRS.

3 Assured Organisational Connectivity (AOC) agreements

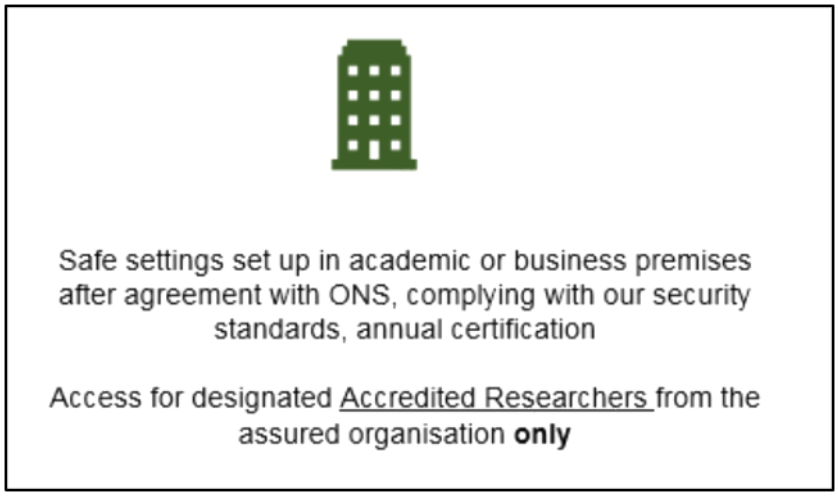

Fig 3.1 AOC agreements as safe settings

The Assured Organisational Connectivity (AOC) scheme has been created for those organisations, whether Government Departments or other public bodies, academic institutions, or third sector/commercial organisations operating within the research community, who wish to access the SRS securely from their own premises. The AOC operates as a mark of assurance to the SRS, information asset owners, and other stakeholders. It is intended to demonstrate that organisations hosting safe settings understand their obligations, can meet the technical requirements for connectivity, have

appropriate controls in place, and agree to maintain current and accurate records of connections and activity.

The SRS approach to Assured Organisational Connectivity recognises that every research institution or organisation wishing to connect to our services is different. For example, some institutions (typically but not always) academic institutions may have large, multi-site campuses that are largely open to members of the public. Other institutions (for example, many government departments) have strict access controls to all areas of their site and do not permit unaccompanied visitors. Certification means that, whatever the type of organisation seeking connectivity, information asset owners can be assured that the connections uphold the strictest technical and physical security requirements.

Certification demonstrates that organisations hosting safe settings understand their obligations, can meet the technical requirements for connectivity, have appropriate controls in place, and agree to maintain current and accurate records of connections and activity. It also means that organisations will oversee their researchers and that they have appropriate sanctions in place for any breaches of access policy.

In order to ensure the highest standards of accountability, only researchers who are on full-time or full-time equivalent contracts may apply for access, and only through their own organisation. If accredited or approved researchers are not under contract to an organisation (for example, they are fee-paying students or external advisors or consultants) they will need to access the SRS through a Safe Room.

AOC agreements are signed for a period of five years. As part of that agreement, organisations wishing to establish safe settings agree to maintain:

- up to date register of machines that will be connected to the SRS. They need to supply the MAC addresses of each machine to be connected, the client name, and the source IP address (a waiver for this provision may be granted upon request). All machines need to be wholly owned by the organisation and connectivity cannot be requested for any personal machines or devices.

- an up to date register of the location of each machine to be connected including the IP address. This register must include an accurate description the physical and technical access controls to each machine. Where machines are located in spaces that may be accessed by persons other than the accredited researchers named on a project, there will need to be an explanation of how the machine (and data and outputs) will be secured (for example, ask for a physical description of the space and of how entry and exit is monitored, and the use of privacy screens, desk dividers, etc. where other physical controls do not restrict access to connected machines).

- an up to date register of accounts for accredited researchers that will be requesting access to the SRS and an indication of which machines that they will be authorised to use by the organisation. Each researcher requesting connectivity must sign an Accredited Researcher Assurance Registration form that is countersigned by the responsible authority within their organisation and which attests to their understanding of the connectivity requirements and obligations.

4 AOC certification

Certification takes place annually and provides a robust guarantee to information asset owners that organisational safe settings continue to operate according to the required security standards and that all records and registers of authorised machines, settings and users are up to date and accurate. Where certification requirements are not met, connectivity will be suspended until ONS is satisfied that appropriate remedial action has been taken. In cases of repeated shortfalls in meeting certification requirements, agreements will be terminated.

In order to maintain certification organisations need to:

- Ensure all registers are current and up to date.
- Notify SRS of any changes to the current certification (e.g. adding machines or locations).
- Provide access to those registers to the SRS, if requested, within 48 hours (2 working days).
- Permit a site inspection from an SRS team, if requested, within five working days of the request.
- Demonstrate continued compliance with all aspects of the Assured Organisational Connectivity agreement.

5 What is prohibited under Assured Organisational Connectivity

The clear intention of the AOC certification scheme is to provide the SRS Security team and information asset owners with the reassurance that accredited researchers are accessing data under the highest standards of security consistent with the Five Safes framework. The AOC scheme specifically excludes certain forms of connectivity. Specifically, the policy prohibits:

- The use of any personal machines or devices to connect to the SRS.
- The use of wireless networks to connect to the SRS (a waiver for this provision may be granted upon request, where it can be satisfactorily demonstrated that the network achieves or exceeds the security standards of the GovWiFi network

and/or the Government Minimum Cyber Security Standard and that there is no satisfactory hard-wired alternative).

- The use of VPN to connect to the SRS (a waiver for this provision may be granted where an organisation-wide VPN is mandated as part of that organisation's security controls. Typically this provision will apply only to Government Departments and specialised Research Institutions, and will need to be verified by the SRS Security team as meeting ONS-compliant VPN security standards).

- Access to the SRS for any machine located in a public space (i.e. one where there are no physical controls or monitoring of access). Laptops may not be used for connectivity in any location other than the one for which they are approved and designated in the register maintained by organisations as part of certification.

Thus, under the AOC scheme, laptop computers will need to be connected via ethernet unless the conditions of the waiver policy can be adequately demonstrated and all location and access requirements in this policy have been satisfactorily met (typically this will only apply to Government Departments).

6 Summary of Security Controls / Responsibilities

The main features of the security controls and responsibilities for maintaining the safety of the remote access settings is provided in Figure 6.1 below.

		Safe rooms			Assured Organisational Connectivity
Security Controls		ONS safe room	OGD/organisation -hosted safe room	ESRC Safepods	
Physical Security	Secure Room/office	✔	✔	✔	✔
	Screens not overlooked by non-researchers	✔	✔	✔	✔
	Security monitoring (e.g. CCTV)	✔	✔	✔	✔
Where can SRS be accessed from?	Specific agreed room	✔	✔	✔	✔
	Appropriate space within agreed office	✕	✕	✕	✔
	Home/Public Place	✕	✕	✕	✕
Who can access SRS?	Accredited Researchers	✔	✔	✔	✔
Which data are accessible?	Data explicitly approved by data-owners	✔	✔	✔	✔
Digital Security	Real-time protective monitoring for suspicious activity	✔	✔	✔	✔
	Key-stroke recording of all internal activity	✔	✔	✔	✔

Responsibility for Controls	
	ONS Controlled and Guaranteed
	OGD/Organisation Controlled and Guaranteed
	ESRC and Safepod host Controlled and Guaranteed
	Research Organisation written commitment
	Researcher written commitment

Fig 6.1 Summary of security controls and responsibilities

Annex 1: The Five Safes Framework

The SRS safeguards access and use of data through the Five Safes Framework:

Safe People

Researchers must evidence understanding of research and statistics either through a relevant degree or through relevant work experience. They must also complete assessed training. Once these requirements are met a researcher will be considered an accredited researcher under the Digital Economy Act (DEA) and will be permitted to use the SRS for a period of five years.

Safe Projects

Each time an accredited researcher wants to undertake a project in the SRS it must be approved by the independent, cross-government Research Accreditation Panel (RAP). RAP will consider whether the project is feasible, legal, ethical and for the public good before giving approval.

Before considering a proposal, there must be agreement in principle from the data owner for their data to be used. Information asset owners can assess feasibility of a project requesting to use their data or delegate this responsibility to the SRS Statistical Support Team. Once the project is considered feasible and agreement is in place for use of the data being requested, the Statistical Support team will review the project application, including evidence of ethical approval, to ensure it is ready to be submitted to RAP.

Safe Data

To ensure that researchers don't learn anything about individuals or businesses whilst undertaking their research, all data made available is de-identified by removing personal identifiers. Information asset owners may also wish to consider what other variables within the data source may result in indirect re-identification.

Safe Settings

Once a project has been approved accredited researchers are provided access to the de-identified data within safe rooms or through Assured Organisational Connectivity.

Safe Outputs

Once a researcher has completed their analysis they can request for aggregated non-disclosive outputs to be taken out of the environment and used in reports. To ensure that confidentiality of data subjects is maintained two people independently check outputs to ensure they meet the confidentiality standards that ONS applies to all outputs published as Official Statistics. The SRS operates a threshold of ten for most of the data sources it holds. Information asset owners are however able to set threshold levels for their data. For instance, HMRC tend to operate a threshold of 30.