National Offender Management Service

National Security Framework Ref: NSF 4.5
INTELLIGENCE – REGULATION OF INVESTIGATORY POWERS ACT
Acquisition of Communications Data

This instruction applies to :-		Reference :-
Prisons		**04/2014**
Issue Date	**Effective Date**	**Expiry Date**
31/01/2014	31/01/2014	30/01/2018
Issued on the authority of	NOMS Agency Management Board	
For action by	All staff responsible for the development and publication of policy and instructions (Check in box as appropriate) ☐ NOMS HQ ☒ All prisons ☒ Contracted Prisons* ☒ Governors ☒ Heads of Groups ☒ Regional and Local Corruption Prevention Managers ☒ Establishment Functional Head of Security/Operations ***If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***	
Instruction type	***Service specification support/ Service improvement/ Legal compliance***	
For information	All staff	
Provide a summary of the policy aim and the reason for its development/ revision	This PSI replaces the relevant parts of the NSF Function 4. It sets out the process to apply for communications data under the Regulation of Investigatory Powers Act and highlights best practice.	
Contact	Security Group CAB hotline: 0300 047 6354 - CAB E-mail: spoc@noms.gsi.gov.uk Policy: 0300 047 6171 - E-mail: barney.clifford@noms.gsi.gov.uk	
Associated documents	Acquisition of Communications Data Code of Practice PSI 16/2012 Information Risk Management Policy PSI 30/2011 Handling Phone and SIM seizures PSO 1300 Investigations PSO 9015 Information Assurance PSO 9020 DPA 1998, FOI 2000, EIR 2004 PSO 9025 Archiving, Retention and Disposal Policy Related Service Specification Related Operating Models Related Direct Service Costs and Assumptions paper Related Cost Spreadsheets See: http://www.justice.gov.uk/about/noms/noms-directory-of-services-and-specifications	

Audit/monitoring: - Monitoring of compliance will take place through the operational line. The arrangements are subject to inspection by inspectors of the Interception of Communications Commissioners Office (IoCCO).
Introduces amendments to the following documents: - This PSI, together with others on intelligence and powers under the Regulation of Investigatory Powers Act (RIPA) replaced guidance in the previous NSF Function 4 (Communications and Surveillance).

CONTENTS

Hold down “Ctrl” and click on section titles below to follow link

Section	Title	Applicable to
1.	Executive Summary	All staff
2.	Policy and Strategic Context	
3.	Operational Instructions	

1. Executive Summary

Background

1.1 The Regulation of Investigatory Powers Act (RIPA) came into force in 2000 and, amongst other things, provides prisons with a power to acquire communications data from Communications Service Providers (CSP) and Internet Service Providers (ISP) relating to telephones and/or computers. The legislation and associated Codes of Practice provide the framework for the acquisition of communications data and the application within prisons is set out in this PSI.

1.2 It is important to note that this PSI is not about the interception of communications under part 1 of RIPA and the Prison Rules but the gathering of data from mobile telephone use or Internet sites visited or postal services, in circumstances set out below.

1.3 The legislation and code of practice introduced the functions of Single Point of Contact (SPoC) and Designated Person (DP). Both functions are undertaken in HQ.

1.4 This PSI replaces guidance in Function 4 of the National Security Framework on communications data.

1.5 The acquisition of communications data is subject to inspection by the Interception of Communications Commissioner's Office (IOCCO).

Desired Outcomes

1.6 All prisons will acquire communications data where it is necessary and proportionate to do so for the purposes of preventing or detecting crime, preventing disorder, or on the grounds of public safety.

1.7 All prisons will have a local policy setting out the application process, including the need for identified members of staff to discuss and submit applications to the Single Point of Contact (SPoC) in Security Group.

1.8 The use of these techniques will form an integral part of the intelligence gathering system within prisons and will be considered as a tactical option in corruption or other investigations where necessary and proportionate.

1.9 Compliance with Part 1, chapter 2 of RIPA across the whole prison estate and for this to be confirmed annually by IOCCO.

1.10 All staff are reminded that if they use social networking sites, they are aware of their responsibilities and do not do anything which may conflict with their professional role in NOMS. Click here for guidance produced by HR.

Application

1.11 This PSI is applicable to all establishments, including contracted out prisons.

Mandatory Action

1.12 *Information defined as communications data in RIPA must only be acquired in accordance with the law.*

1.13 *All applications to acquire communications data must be made to the Single Point of Contact (SPoC) in HQ.*

1.14 *All applications must be written and contain a URN provided by the SPoC.*

1.15 *Applications to acquire communications data can only be authorised by the Designated Person listed in the 2010 RIPA order. Due to organisational restructure, this person is the Head of the Operational Intelligence Team, Security Group, HQ.*

1.16 *The use of these powers incurs a charge and the SPoC will provide indicative costs regarding each application. The Governor must be made aware of the cost at the time of the application and must pay promptly each invoice received from the CSP.*

Resource Impact

1.17 There may be a minor cost in updating local instructions to comply with this part of the overall intelligence policy but no new processes are being introduced so in effect this PSI is cost neutral.

1.18 *There will be a cost to establishments every time communications data is sought from a Communications Service Provider (CSP) and this must be paid for by the establishment budget.*

(Signed)

Digby Griffith
Director of National Operational Services, NOMS

2. Policy and Strategic Context

2.1 The Human Rights Act (HRA) 1998 incorporated into UK law the rights set out in the European Convention on Human Rights (ECHR). One such right is the right to respect for private and family life (Article 8). Where NOMS seeks to obtain private information by means of covert investigative techniques, it is likely that this right will be engaged. The authorisation procedures in RIPA are designed to ensure that any interference with this right is likely to be justifiable as being in accordance with law, necessary in pursuit of a legitimate aim, and proportionate.

2.2 NOMS has powers to acquire communications data for the purposes of the prevention or detection of crime or preventing disorder (RIPA 22 (2) (b)) or on the grounds of public safety (RIPA 22 (2) (d)).

2.3 The acquisition of communications data is a very powerful tool and forms an essential part of the intelligence gathering opportunities within a prison. *Before proceeding, proper thought must be given to whether this is the right tactic to use and whether all other information gathering opportunities have been tried or are considered to be inappropriate in the circumstances*.

2.4 It is essential that as threats to the security of prisons and the wider community continue to develop, that staff use all lawful means at their disposal to gather information to counter those threats. *This PSI is part of the series of PSI's on the gathering and use of intelligence and must be seen in that wider context.* These techniques are but one investigative tool at the disposal of managers and therefore should not be viewed in isolation but in a considered and objective way in order to gather information on key threats.

2.5 There will also be a closed PSI, which will be sent to the Governor for sharing to particular staff on a need to know basis.

2.6 This PSI does not effect in any way the data that we currently gather and use under the Lawful Business Practice Regulations 2000 (for example regarding staff use of business computers or telephones).

RIPA in NOMS

2.7 The powers to acquire communications data in prisons has led to a quite different authorisation process than covert surveillance or CHIS, which primarily have the applicant and authorising officer within an establishment. The fact that the relevant RIPA Code of Practice requires there to be a position of a specialised and accredited Single Point of Contact (SPoC), who in effect acts as tactical adviser for all operations, in HQ, it made sense in order to streamline the process to have the authorising officer in HQ too.

2.8 The SPoC maintains a central register of all applications and associated communications and correspondence. This is made available to the Interception of Communications Commissioner's Office (IoCCO) at the time of their inspection.

3. Operational Instructions

Text within shaded boxes indicate requirements from the "*Provision of a Secure Operating Environment*" bundle of specifications. All instructions below are mandatory.

Mobile phones found within a prison are interrogated.

Local Policy Document

3.1 *Every prison establishment must have a document which is available to staff, prisoners, and visitors stating that all lawful methods will be used for the gathering of intelligence and evidence within the prison.* The use of any intelligence gathering will be undertaken where it is necessary and proportionate to do so.

3.2 It is important that staff understand the escalation process when mobile phones are found (PSI 30/2011) and that there is a difference between powers to interrogate an illicit mobile telephone and the acquisition of communications data under Part 1, Chapter 2 of Regulation of Investigatory Powers Act (RIPA). Often, phone interrogation under PSI 30/2011 will precede the use of these powers but there will be occasions when that is not the case.

Intelligence informs actions in the prevention and detection of risks to prison security and the wider community.

Powers

3.3 Acquisition of data is governed by Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) and NOMS is one public authority named in the legislation as being able to use these powers.

3.4 These powers are exercised through a Single Point of Contact (SPoC).

3.5 *Data acquisition must be authorised by a named official in a public authority so designated by Parliament.* This person is referred to in Part 1 Chapter 2 of RIPA as the Designated Person (DP), who undertakes a similar role as the Authorising Officer for covert surveillance and use of CHIS (RIPA Part II). The DP nominated for NOMS is the Manager of the Operational Intelligence Team, in Security Group, HQ.

3.6 *Any application must be on the grounds that it is necessary for one of the reasons set out above and proportionate to what is sought to be achieved.*

Communications Data

3.7 Broadly, this is the "who", "when", and "where" of a communication but not the content of the communication. Communications data is held by Communications Service Providers (CSP) for their own business purposes (e.g. to send bills) and where it can be justified, we can apply to access some of the data.

Roles

Applicant

3.8 *The Applicant must be a person who has good knowledge of the matter under investigation and has access to all the relevant information.*

3.9 The Applicant in a contracted out establishment does not need to be the Controller or Deputy Controller but the person who has got the most knowledge of the matter under investigation.

SPoC

3.10 This is a position required under the Code of Practice that has a number of functions:

- tactical adviser to the Applicant
- quality assurance of applications
- central record keeper for all applications and associated communications
- adviser to the Designated Person
- contact point with CSP/ISPs on behalf of NOMS
- data processor

3.11 The SPoC undertakes this role for all prison establishments – public sector and contracted out.

Designated Person

3.12 *The DP is a statutory function and must be the person who holds the rank or position in prescribed by the legislation.* This role is undertaken by the Manager of the Operational Intelligence Team, Security Group, HQ.

3.13 The function of the DP is to assess the necessity and proportionality of an application and whether he/she believes that the acquisition of data can be justified.

3.14 The DP undertakes this role for all prison establishments – public sector and contracted out.

The Senior Responsible Officer

3.15 The Senior Responsible Officer for NOMS is the Head of Security Group in NOMS HQ. The SRO has responsibility for the following:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Part 1, chapter 2 of the Act and with the codes of practice;
- oversight of the reporting of errors to IOCCO and the identification of both cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections and;
- where necessary, to oversee the implementation of post-inspection action plans approved by the Commissioner.

3.16 This complies with Section 3.22 of the Acquisition of Communications Data codes of practice.

Data Protection

3.17 *All data, whether held by the SPoC or the applicant must be managed in accordance with the Data Protection Act and data principles.* PSI 16/2012 refers and PSO's 9015, 9020, and 9025.

Retention of Data

3.18 *All electronic and paper records must be retained for 6 years from the date of the DPs signature if the application was rejected or the date that the final piece of information was acquired from a CSP.*

3.19 *If data acquired is further processed (e.g. a Security Information Report is entered) the retention period for that document must be followed.*

Freedom of Information Act

3.20 General requests for policy information or statistics regarding the use of powers will be dealt with by staff in Security Group.

Arrangements are in place to share and disseminate information with criminal justice stakeholders lawfully.

3.21 The purpose of NOMS is not to conduct criminal investigations and it is important that we do not in any way impede or overstep our remit in the acquisition of data.