STATES OF JERSEY

REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 2005 AND POLICE PROCEDURES AND CRIMINAL EVIDENCE (JERSEY) LAW 2003: REPORT OF THE INVESTIGATORY POWERS COMMISSIONER 1ST JANUARY – 31ST DECEMBER 2023

Presented to the States on 14th January 2025

STATES GREFFE

REPORT

INTRODUCTION

1. The Regulation of Investigatory Powers (Jersey) Law 2005 ("RIPL") and Part 11 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 ("PPCEL") set out the legal framework governing the use of certain law enforcement techniques which are described more fully below. The statutory framework is designed to ensure that those techniques are regulated by law, operated in a proportionate manner, and (because of their largely and necessarily clandestine nature) subject to external oversight.

2. As part of the regime of external oversight, Article 43 of RIPL requires the Bailiff to appoint one of the ordinary judges of the Court of Appeal as the Investigatory Powers Commissioner. Article 104 of PPCEL makes corresponding provision for the appointment of a Commissioner under that Law. Each of these Laws requires the Commissioner to carry out certain supervisory functions and to make an annual report to the Bailiff with respect to the carrying out of those functions.

3. The Bailiff has appointed me as Investigatory Powers Commissioner for Jersey in succession to David Perry KC. Mr Perry provided his third and final report, covering the calendar year 2022 in May 2023 and his report was presented to the States on 17 August 2023.

4. This is my first annual report. It covers the calendar year 2023. The overall conclusion of this report is that the investigatory powers which I describe below continue to be used lawfully, for legitimate purposes and in the public interest.

THE INVESTIGATORY POWERS COMMISSIONER

5. Part 4 of RIPL (Articles 43 to 52) is headed "Scrutiny Etc of Investigatory Powers". This provides for the appointment of the Investigatory Powers Commissioner[1]. In broad terms, the Commissioner's role is to keep under review the exercise and performance of the powers and duties conferred and imposed by RIPL and to make an annual report to the Bailiff[2].

[1] It also provides for the appointment of Assistant Investigatory Powers Commissioners and establishes the Investigatory Powers Tribunal, which has jurisdiction to hear certain proceedings, complaints and references arising as a result of the operation of RIPL.

[2] In addition to the responsibility to make an annual report to the Bailiff, the Commissioner may at any time make any other report to the Bailiff on any matter relating to the carrying out of the Commissioner's functions as the Commissioner thinks fit: Article 44 (5) RIPL. The Commissioner is also required to make a report to the Bailiff if at any time there has been a contravention of the provisions of RIPL in relation to any matter with which the Commissioner is concerned or it at any time it appears that the arrangements for safeguarding warranted intercept product or the key to encrypted information have proved inadequate in relation to any matter with which the Commissioner is concerned: Articles 44(2)(and (3) RIPL.

6. The Commissioner is required to keep under review the exercise and performance of the powers and duties conferred or imposed by RIPL on various public authorities and office- holders in relation to the following investigatory powers:

   (i) the interception of communications under Chapter 1 of Part 2 of RIPL (Articles 4 to 23);

   (ii) the acquisition and disclosure of communications data under Chapter 2 of Part 2 of RIPL (Articles 24 to 29);

   (iii) the use of "directed surveillance", "intrusive surveillance" and "covert human intelligence sources" under Part 3 of RIPL (Articles 30 to 42); and

   (iv) the investigation of data protected by encryption under Part 3A of RIPL (Articles 42A to 42H).

7. The Commissioner is also required to keep under review the adequacy of arrangements for safeguarding warranted interception product by restricting its use to the minimum necessary for the "authorised purposes" identified in Article 19(4) of RIPL (broadly speaking for intelligence gathering purposes or to facilitate the carrying out of the functions of the Commissioner or the Investigatory Powers Tribunal).

8. RIPL does not regulate entry on or interference with property or interference with wireless telegraphy. These activities are governed by Part 11 of PPCEL (Articles 99-104). Article 104 PPCEL provides for the appointment of a Commissioner to keep under review the carrying out by the Attorney General of the Attorney General's functions under Part 11 PPCEL and to make an annual report to the Bailiff.

9. Article 44(1) of RIPL imposes on all relevant public office-holders and public authorities a duty to disclose or provide to the Commissioner all such documents and information as the Commissioner may require in order to carry out the Commissioner's functions. Article 103 of PPCEL imposes on the Attorney General a duty to notify the Commissioner of authorisations given, renewed or cancelled under Part 11 of PPCEL and, where authorisation was given orally, of the reasons why it was considered urgent.

10. The Bailiff is required to cause a copy of the Commissioner's annual report to be laid before the States, together with a statement as to whether any matter has been excluded from that copy (in the exercise of the Bailiff's power, after consultation with the Commissioner, to exclude any matter if it appears to him that its publication would be contrary to the public interest, or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of Jersey or the continued discharge of the functions of any public authority whose functions include activities which are subject to review by the Commissioner).

11. As will be apparent from this brief summary, the Commissioner's role is designed to provide external oversight of the various public office-holders and public

authorities who are authorised to use intrusive (and for the most part clandestine) investigatory powers. That oversight enables the Commissioner both to scrutinise the compliance of those officials and authorities with the requirements of the legislation and to seek to promote best practice in relation to the use of those powers. The reporting requirements, and the obligation on the Bailiff to publish the Commissioner's annual report, are designed to enhance public confidence in the operation of the statutory scheme.

THE POWERS UNDER REVIEW

12. RIPL and Part 11 of PPCEL were enacted to provide a lawful basis for the use of intrusive investigative techniques. They provide a detailed statutory scheme regulating the use of those techniques. For the purposes of this report, it is sufficient to provide a summary overview of the various powers which I have a responsibility to keep under review.

Interception of Communications

13. Chapter 1 of Part 2 of RIPL regulates the interception of communications in the course of their transmission by a public postal service (for example, the opening of mail) or by a public or private telecommunications service (in simple terms, telephone tapping). In summary, RIPL makes it unlawful to intercept communications without proper authorisation. Interception may be authorised in one of two ways. The first is where the interception is authorised by or under Article 8 or 9 of RIPL[3]. The second is where the interception takes place in accordance with an interception warrant issued by the Attorney General under Article 10 of RIPL.

14. The Attorney General may issue an interception warrant only if it has been applied for by or on behalf of one of the persons identified in Article 11(1) of RIPL. These include the Chief Officer of the States of Jersey Police Force, the Agent of the Impots, the Chief Immigration Officer and a person who, for the

[3] In summary Articles 8 and 9 deal with the following situations:
(i) where the interception takes place with the consent of the sender and the intended recipient:
(ii) where the interception is by a person who provides a postal or telecommunications service for purposes connected with the provision or operation of that service;
(iii) where the interception takes place for certain purposes under the Wireless Telegraphy Act 2006 as extended to Jersey by the Wireless Telegraphy (Jersey) Order 2006;
(iv) interception of postal communications by an examining officer under paragraph 7 of Schedule 8 to the Terrorism (Jersey) Law 2002;
(v) interception of telecommunications to obtain information about the communications of a person in a country outside Jersey pursuant to legal requirements of that country;
(vi) conduct authorised by the Minister by Order and which appears to the Minister to constitute a legitimate practice reasonably required for the purpose of monitoring or keeping a record of business communications; and
(vii) conduct in the exercise of powers under the Prisons (Jersey) Law 1957.

purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside Jersey.

15. The Attorney General may not issue an interception warrant unless he believes: (a) that the warrant is necessary on grounds falling within Article 10(3) of RIPL; and (b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct. The grounds specified in Article 10(3) are: (a) the interests of national security; (b) the purpose of preventing or detecting serious crime[4]; (c) the purpose of safeguarding the economic well-being of Jersey; and (d) the purpose of giving effect to an international mutual assistance agreement (in circumstances equivalent to those covered by the provision relating to the prevention or detection of serious crime). A factor which must be taken into account when considering whether these requirements are satisfied is whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

16. RIPL makes detailed provision for the content of warrants, their duration, cancellation and renewal, their modification, and their implementation. Articles 19 and 20 of RIPL contain general safeguards in relation to the dissemination, retention and disposal of intercepted material. In particular, Article 19(1) imposes a duty on the Attorney General to ensure that such arrangements are in force as he considers necessary for securing that the dissemination of intercepted material is limited to the minimum necessary for the authorised purposes and that any copy of intercepted material is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.

17. Disclosure of the issue or existence of a warrant, the interception of a communication or the content of an intercepted communication (identifiable as such) is generally prohibited and may, in certain circumstances, amount to the commission of a criminal offence. As in the United Kingdom and Guernsey, intercepted material is inadmissible in criminal trials. The purpose of the warranted intercept regime is accordingly, broadly, to gather intelligence to prevent or detect serious crime, and not to gather evidence for use in legal proceedings. The scheme is intended, among other things, to preserve the secrecy of the practical operation of the interception regime and to protect to the maximum extent possible the privacy of those whose communications are intercepted without their consent.

Acquisition and disclosure of communications data

18. Chapter 2 of Part 2 of RIPL contains a legislative scheme which regulates access to and handling of communications data – that is data about the use made of a telecommunication or postal service but excluding the contents of

[4] For these purposes as defined in Article 1 of RIPL, "serious crime" means conduct which constitutes one or more offences (a) which involve the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; and (b) for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for three years or more.

communications. Communications data are sometimes described as the "who, how and where" of a communication. They include subscriber information and call data held by a communication service provider.

19. The acquisition or disclosure of communications data is lawful if it is properly authorised under RIPL and is in accordance with that authorisation. RIPL gives power to certain designated persons to grant an authorisation to engage in conduct to which Chapter 2 of Part 2 of RIPL applies or to require a postal or telecommunications operator to disclose communications data. The designated persons are (depending on the public authority which seeks to exercise the powers under Chapter 2) the Chief Officer of the States of Jersey Police Force, the Agent of the Impots, the Chief Immigration Officer and the Attorney General.

20. The powers under Chapter 2 of Part 2 of RIPL apply only where a designated person believes that it is necessary on one of the grounds specified in Article 26(2) of RIPL to obtain any communications data. The grounds in question are wider than those which apply to interception warrants. They include the purpose of preventing or detecting crime (not only serious crime) or of preventing disorder, the purpose of protecting public health, the purpose of assessing or collecting taxes, the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health or of mitigating any injury to a person's physical or mental health, as well as the interests of national security and the economic well-being of Jersey.

21. Chapter 2 of Part 2 of RIPL permits communications to be obtained by one or other of two routes. The first is by giving a notice to the postal or telecommunications operator requiring the operator to obtain and disclose the relevant data to the public authority which served the notice. The second is by an authorisation which allows the public authority to collect or retrieve the data itself (where this is possible). The legislation provides for the form and duration of authorisations and notices. Although not specifically provided for in RIPL, communications data must be handled and stored securely and in accordance with data protection principles.

22. Communications data, unlike intercept product, are admissible in evidence in legal proceedings in Jersey. They are frequently used in the prosecution of serious criminal offences.

Surveillance and the use of covert human intelligence sources

23. Part 3 of RIPL applies to three kinds of covert activity: directed surveillance, intrusive surveillance and the conduct and use of covert human intelligence sources ("CHIS").

24. "Surveillance" is defined in Article 31 of RIPL to include "(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; (b) recording anything monitored, observed or listened to in the course of surveillance; and (c) surveillance by or with the

assistance of a surveillance device". Certain matters are specifically excluded from the definition.

Directed Surveillance

25. In order to be "directed surveillance" for the purposes of Part 3 of RIPL, the surveillance must be covert but not intrusive, and undertaken –
    (a) for the purposes of a specific investigation or operation;
    (b) in such a manner as is likely to result in the obtaining of private information about a person; and
    (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for authorisation to be sought.

    This would, for example, cover static, foot or mobile surveillance in the street, whereby a surveillance team follows targets covertly in order to obtain information about what they are doing.

26. Article 34 of RIPL identifies designated persons who have power to grant authorisations for the carrying out of directed surveillance. These include the Chief Officer of the States of Jersey Police Force (where the surveillance is to be undertaken by that Force), the Agent of the Impots (where the surveillance is to be undertaken by officers of Customs and Excise), the Chief Immigration Officer (where the surveillance is to be undertaken by the Immigration and Nationality Department) and the Attorney General (where the surveillance is to be undertaken by other public authorities which are empowered under RIPL to use directed surveillance).

27. A designated person may not grant an authorisation for the carrying out of directed surveillance unless that person. Believes: (a) that the authorisation is necessary on one of a number of specified grounds; and (b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out. The specified grounds are effectively the same as those set out in Article 26(2) of RIPL which may justify the disclosure of communications data (with the exception of the purpose, in an emergency, of preventing death or injury or any danger to a person's physical or mental health).

28. The legislation sets out general rules for the grant, renewal and duration of directed surveillance authorisations. As a general rule a written authorisation will cease to have effect (unless renewed) at the end of a period of three months beginning on the day on which it took effect.

Intrusive Surveillance

29. In order to be "intrusive surveillance" for the purposes of Part 3 of RIPL the surveillance must be covert surveillance that: (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and (b) involves the presence of an individual on the premises or in the vehicle or is

carried out by means of a surveillance device[5]. Thus, whilst intrusive surveillance may involve the present of an individual, in its classic form it involves the use of a listening device placed in a private vehicle or a dwelling.

30. Authorisations for intrusive surveillance may only be granted by the Attorney General. Only certain public authorities may seek authorisation; most relevantly, for present purposes, these include the Chief Officer of the States of Jersey Police Force, the Agent of the Impots and the Chief Immigration Officer. The Attorney General may not grant an authorisation unless the Attorney General believes: (a) that the authorisation is necessary on one of the specified grounds; and (b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out. The only available grounds are: (a) the interests of national security; (b) the purpose of preventing or detecting serious crime; and (c) the interests of the economic well-being of Jersey. The Attorney General is required to take into account whether the information which it is thought necessary to obtain could reasonably be obtained by other means.

31. The legislation sets out general rules for the grant, renewal and duration of intrusive surveillance authorisations. As a general rule a written authorisation will cease to have effect (unless renewed) at the end of a period of three months beginning on the day on which it took effect.

Covert human intelligence sources

32. A covert human intelligence source ("CHIS") is a person who:
    (a) establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the obtaining of information or provision of access to information;
    (b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or
    (c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

    An essential feature of the definition is that the person (who may be a law enforcement officer or a civilian) acts covertly. The legislation does not apply to a situation where a member of the public comes forward with information about a crime, but it does include an informant (or police officer) who cultivates a relationship with another person for the purposes of supplying (or obtaining) information about that person to the police or other law enforcement authorities.

33. The public authorities entitled to use a CHIS are the same as those permitted to seek authority to use directed surveillance. The system for authorisation and the grounds for which a CHIS may be authorised are also the same. However the legislation specifies certain additional requirements, in particular:
    (a) an officer (known as the handler) must have day-to-day responsibility for contact with the CHIS and for his or her welfare;

[5] Article 32 of RIPL contains certain qualifications to this definition.

(b) a different officer (known as the controller) must oversee the use of the CHIS;
(c) records must be kept of the use made of the CHIS (and other specified matters); and
(d) the CHIS' identity must be protected.

34. The legislation provides for the grant, duration and renewal of authorisations. As a general rule, a written authorisation will, unless renewed, cease to have effect at the end of a period of twelve months beginning with the day on which it took effect.

Interference with Property

35. Entry on or interference with property or with wireless telegraphy is governed by provisions contained in Part 11 of PPCEL. In many cases, a covert surveillance operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. This can be achieved by way of a combined authorisation, although the criteria for the authorisation of each activity must be considered separately.

36. PPCEL provide that no entry on or interference with property or with wireless telegraphy will be unlawful if it is authorised under Part 11. Article 101 provides that the Attorney General may authorise interference with property or the taking of action in respect of wireless telegraphy where he believes this to be: (a) necessary for the purpose of preventing or detecting serious crime or in the interests of the security of the island; and (b) proportionate to what the action seeks to achieve.

37. The legislation contains provisions which govern the form and duration of authorisations. Written authorisations generally cease to have effect at the end of a period of three months beginning with the day on which they took effect.

Investigation of data protected by encryption

38. Part 3A of RIPL, inserted by the Cybercrime (Jersey) Law 2019, allows for the issue of notices requiring the disclosure of the key to encrypted information that is lawfully within the possession of the authorities. This power may be used for example to obtain a password so as to obtain access to an electronic device such as a mobile telephone or a computer. The provisions contain powers to issue a disclosure notice, where the person issuing the notice believes on reasonable grounds that it is necessary in the interests of national security or for the purpose of preventing or detecting crim e or in the interests of the economic well-being of Jersey or where it is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty. Failure to comply with a notice is a criminal offence.

CODES OF PRACTICE AND GUIDANCE

39. Article 51 of RIPL empowers the Minister to issue Codes of Practice relating to the exercise and performance of powers and duties conferred or imposed by RIPL and by the PPCEL. Whilst failure to comply with the Codes of Practice does not of itself render any person liability to criminal or civil proceedings, persons exercising or performing powers or duties under the legislation are obliged to have regard to the provisions of any relevant Code of Practice. The Codes of Practice are admissible in evidence and, where relevant, must be taken into account by a court or tribunal.

40. There are five Codes of Practice which were brought into force by the Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006. These address:
    (a) the interception of communications;
    (b) the interception of communications (postal);
    (c) accessing communications data;
    (d) covert surveillance (including interference with property or with wireless telegraphy); and
    (e) covert human intelligence sources.

41. The Codes of Practice provide general guidance, in plain language, on the procedures to be followed before the relevant investigation techniques can be used. They are primarily intended for use by the various public officials who apply for, authorise or use the measure in question, although they will also be useful to anyone interested in the operation of the statutory scheme.

GENERAL OBSERVATIONS ON THE STATUTORY SCHEME

42. The provisions of RIPL and the PPCEL, supplemented by the Codes of Practice, are intended to provide a comprehensive legal framework for the regulation of the investigative techniques to which they apply. The legal framework serves the important public interest of ensuring that the use of these techniques, which are necessary in a modern democratic society, are regulated by law. The provisions establish procedures and prescribe rules which seek to ensure that the use of these techniques, which are capable of interfering with individual rights, will in every case be properly considered and justified, be appropriately authorised, and be subject to appropriate safeguards.

43. The statutory provisions and the Codes of Practice draw heavily on the United Kingdom Regulation of Investigatory Powers Act 2000 and associated Codes of Practice. The 2000 Act (along with the Regulation of Investigatory Powers (Scotland) Act 2000) remains the governing statute in the UK for directed and intrusive surveillance and the use and conduct of CHIS. There have been developments in the UK legislative regime which are not reflected in the Jersey legislation. Notably, in relation to interception of communications and the acquisition and disclosure of communications of data, the 2000 Act has been replaced by the Investigatory Powers Act 2016 and new Codes of Practice produced on the exercise of those powers. The Investigatory Powers Act 2016

responded to the legitimate needs of law enforcement in the context of a changing technological environment. The 2000 Act has itself been amended by the Covert Human Intelligence Sources (Criminal Conduct) Act 2021, to provide for criminal conduct authorisations (in recognition that sometimes the effective and legitimate use of a CHIS may involve activity which would otherwise be criminal). The relevant authorities may wish to consider whether a review of the Jersey legislative regime would be appropriate in light of developments elsewhere.

CONDUCT OF THE REVIEW

44. As was the practice of my predecessors, Lord Anderson of Ipswich KBE and David Perry KC, I undertook an inspection visit, which took place between 15 and 18 April 2024. I was greatly assisted by two specialist inspectors from the UK Investigatory Powers Commissioner's Office ("IPCO"), Mr Stephen Matthews and Mr Paul Gration. **In accordance with a practice first introduced by Lord Anderson, and continued during Mr Perry's tenure**, the UK Investigatory Powers Commissioner, the Rt Hon Sir Brian Leveson, agreed to make the services of these two inspectors available to me. Mr Matthews has expertise in, among other things, the interception of communications and the acquisition and disclosure of communications data. Mr Gration has expertise in, among other things, all areas of surveillance and the conduct and use of covert human intelligence sources. Both of them have substantial experience both of using and of inspecting the use of similar powers in the UK; and both of them have participated in previous inspection visits to Jersey.

45. I am glad to record publicly my gratitude to Sir Brian Leveson and to all those at IPCO who provided support and assistance to the inspection process this year. Mr Matthews and Mr Gration brought to the inspection knowledge, practical experience and understanding which no Commissioner, however senior or experienced, could be expected to possess. I benefited greatly, particularly on this my first inspection visit, from their insight and assistance. They have brought to bear their knowledge of current best practice in the UK (as well as the understanding of the system in Jersey which they have gained from previous visits), in oral briefings with relevant personnel in Jersey and in confidential reports which I submit to the Bailiff along with this public report. It is plain to me that their participation in the inspection process has provided and continues to provide significant benefit to the supervision and management of investigatory powers in Jersey and therefore to the work of Jersey law enforcement agencies.

46. In the course of the inspection, I received classified written briefing on the use of each of the relevant powers by Jersey law enforcement authorities. This was supplemented by oral briefings with a number of the personnel involved in the authorisation, management and oversight of covert operations. The inspection team was given full access to the records relating to the use of those powers during 2023. I was able to discuss the operation of the legislation with the Chief Officer of the States of Jersey Police and Jersey Customs and Immigration Service, as well as with the Law Officers. I can confirm that the IPCO Inspectors

and I were given access to all of the information and provided with every facility which we required in order to undertake a full and proper inspection. I am grateful to all those who **assisted in the inspection process**.

47. In addition to the statutory inspection, the IPCO Inspectors and I visited HMP Moye, which is not subject to RIPL and PPCEL, at the request of and with the support of the Governor. This followed a similar visit which was undertaken by my predecessor, on the same basis, last year. The IPCO Inspectors and I were left with a favourable impression of the commitment of the key staff within HMP Moye to learning from best practice. The relevant authorities may wish to consider whether HMP Moye should, like prisons in the UK, be brought within the statutory regime.

SCOPE OF THIS REPORT

48. Like my predecessors, I recognise the tension between the public interest in transparency and the need to maintain the confidentiality which necessarily attends the use of covert surveillance powers. In particular, I recognise the need to avoid any risk of undermining the effectiveness of those powers in ongoing and future operations. In balancing these competing interests, I have generally followed the approach adopted by my predecessors in previous reports.

49. My inspection focused on the use of surveillance powers by the Jersey law enforcement authorities (the States of Jersey Police and Jersey Customs and Immigration Service), and on the authorisation of the use of such powers by the Law Officers. Without disclosing the details of specific operations, I can confirm that the overwhelming majority of the authorisations requested and granted were in support of law enforcement activities conducted for the purpose of preventing or detecting serious crime, largely, though not solely, arising from drug trafficking.

50. The focus of my report is on compliance with the statutory requirements and the Codes of Practice. As in previous years, the inspection identified opportunities for further improvements in practice and procedure and these were communicated during the inspection visit. Further detail is contained in confidential reports prepared by the IPCO inspectors under my supervision, which I have provided to the Bailiff as appendices to this public report. I recommend that these confidential annexes be provided to the relevant agencies to assist with training and the ongoing pursuit of best practice.

INTERCEPTION WARRANTS

50. During 2023 eight interception warrants were approved and one application was refused. All of the warrants approved were for the statutory purpose of preventing or detecting serious crime. In one case, the Attorney General declined to authorise an application on the basis that the statutory purpose upon which the application was presented was not made out.

51. During the inspection visit, the documentation relating to the grant, modification, cancellation and refusal of applications was inspected. This disclosed a good standard of compliance with the legislation and the Codes of Practice. The applications identified the justification for the interception and an explanation of why the proposed activity was considered necessary and proportionate. Modifications were made were necessary and all cancellations were timely. The law enforcement officials involved demonstrated an appropriate awareness of their responsibilities; and the approach taken by the Attorney General was consistent with the care with which he performs all of his statutory functions under RIPL and PPCEL.

52. Article 19(2) of RIPL imposes a duty on the Attorney General to ensure that arrangements are in place for securing that the disclosure and distribution of intercepted material is kept to the minimum necessary for the authorised purposes. The inspection team was able to confirm that appropriate safeguards are in place and that the requirements of Article 19 are satisfied.

COMMUNICATIONS DATA

53. In 2023 215 applications for the acquisition of communications data were approved. During the inspection visit 65 applications were examined. These were all submitted for a proper statutory purpose and were prepared to a good standard. The inspection team was satisfied that the applications complied with the requirements of the law and the Codes of Practice and that the use being made of the technique by law enforcement agencies is fully justified.

PROPERTY INTERFERENCE AND INTRUSIVE SURVEILLANCE

54. In 2023 there were six authorisations for intrusive surveillance and seven authorisations for property interference, across seven operations. All but one of these operations (which resulted in a conviction for terrorism offences) was concerned with the investigation of drug trafficking. These powers were used lawfully and for proper statutory purposes. No reportable errors were identified during the inspection process.

DIRECTED SURVEILLANCE

55. In 2023 there were 23 directed surveillance operations. The majority of these were concerned with drug trafficking. No reportable errors were identified during the inspection process and the applications and authorisations were generally compliant with the legislation and Codes of Practice. The practice in relation to the formal cancellation of authorisations requires to be tightened up, and this has been communicated to the agencies involved.

COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

56. During the period under review Jersey law enforcement has used the services of registered CHIS. Mr Paul Gration has made a number of recommendations in relation to the management of CHIS in the confidential report provided to the Bailiff which is annexed to this public report. I recommend that this be passed to the relevant agencies with a view to continuing improvement in the management of CHIS; and I intend to review progress in that regard during my next inspection visit. It suffices for the purposes of this report to confirm that there were no reportable errors and that the relevant requirements of RIPL have been complied with.

CONCLUSION

57. In the course of my inspection, I was provided with all the assistance which I required in order to undertake (with the assistance of the IPCO inspectors) a full review of the use of the relevant investigatory powers during 2023. All of the public officials whom we met were well-informed, generous with their time, and demonstrably committed to the effective and proper use of these powers. They provided all of the information which the inspection team required to see and were receptive to suggestions and recommendations for improvements in practice.

58. The inspection process confirmed that the powers in RIPL and PPCEL are being used lawfully and proportionately, in pursuit of legitimate objectives. It is a reflection of the professionalism of the States of Jersey Police Force and the Jersey Customs & Immigration Service that there were no reportable errors during the review period. Whilst areas for improvement, in pursuit of best practice, were identified and communicated to those concerned, the documentation generally demonstrated the consideration being applied to the use of these investigatory powers.

59. The overall conclusion of this, my first report as Commissioner, is that the statutory investigatory powers are being used lawfully, for legitimate purposes in the public interest.

Rt Hon James Wolffe KC FRSE August 2024

INVESTIGATION OF DATA PROTECTED BY ENCRYPTION

In 2023 ten notices were issued under Article 42B of RIPL, requiring the disclosure of the key to protected information. Four of these led to the disclosure of the PIN which enabled a device to be unlocked. In four cases charges have been preferred or a prosecution is pending. All of the notices complied with the statutory requirements.