Use of the Police National Computer by non-police organisations

An inspection of the Environment Agency

May 2016

ISBN: 978-1-78655-097-2

www.justiceinspectorates.gov.uk/hmic

Contents

Introduction 3

Background and context 3

Terms of reference 4

About the Environment Agency 4

Methodology 5

Findings 6

Scale of PNC use 6

The level of access and authorised purposes for PNC use 6

Does the organisation comply with its Security Operating Procedures? 8

Conclusions 11

Level of access 11

Compliance 11

Efficiency and effectiveness 11

Introduction

Background and context

The Police National Computer (PNC) is a national database of information available to all police forces throughout the United Kingdom.[1] In addition, certain other organisations, referred to as “non-police organisations”, have access to information held on the PNC in order to help them fulfil their statutory functions.

In such instances, access is granted by a body called the Police Information Access Panel ("the Panel").[2] In order to obtain access, each organisation must submit a detailed business case that satisfies the Panel that a valid and lawful requirement for access exists.

If this is the case, two documents are produced that specify the level of access permitted and the manner in which the non-police body may use the PNC: the *Supply Agreement*, which describes the permitted access and how it will be provided, and the *Security Operating Procedures*, which are a requirement of the *Supply Agreement* but which are produced by the non-police organisation for the attention of their staff.

Some non-police organisations access the PNC through discrete computer terminals installed in their premises. This is known as “direct access”. Other non-police organisations obtain PNC information through a third party, usually a police force. This is known as “indirect access”.

In either arrangement, the public needs to have confidence that access is properly regulated and that effective auditing arrangements are in place. This is important because much of the information held on the PNC is sensitive and personal.

Her Majesty's Inspectorate of Constabulary (HMIC) is recognised as having strong expertise in this area and the Government’s Independent Advisor on Criminality Information Management recommended that HMIC’s audit role is extended to cover all PNC users.[3]

---

[1] *Police National Computer (PNC) Guidance version 5*, Home Office, January 2014, page 5. The PNC holds information concerning people and property, including convictions, wanted and missing people, stolen vehicles and other types of stolen property.

[2] The Police Information Access Panel is a sub-group of the PNC governing body – the Police PNC Policy and Prioritisation Group (known within policing as "P4G"). The Panel is chaired by a chief officer and comprises a cross-section of senior Home Office and police leaders who are concerned with the management of the PNC. The Panel meets on a quarterly basis to consider applications for access to the PNC. Her Majesty's Inspectorate of Constabulary is represented on the Panel.

[3] *A Common Sense Approach: a review of the criminal records regime in England and Wales*, Sunita Mason (Independent Advisor for Criminality Information Management), November 2011, pages 34-35.

Consequently, as part of our regular programme of inspections,[4] we examine the circumstances under which non-police organisations are granted access to the PNC; the ways in which they use PNC information; the safeguards that are required in order to protect the information and whether those safeguards are being properly applied.

Non-police organisations are also subject to a separate Home Office audit, which examines in detail whether PNC data is held and used in an approved and secure way.[5]

While HMIC's inspections can be prioritised on the basis of the findings of these Home Office audits, HMIC's inspections do not examine all of the same issues. However, there can be certain areas of overlap. Where our inspections reveal concerns in areas that are also subject to Home Office audit, we highlight this.

Terms of reference

HMIC's inspections of non-police organisations that have access to the PNC aim to answer three questions:

1. Is the level of access specified in the *Supply Agreement* appropriate for the needs of the non-police organisation?

2. Does the non-police organisation comply with the *Security Operating Procedures*? In particular, are the arrangements for training, physical security, and internal audit compliant with the *Security Operating Procedures*?

3. Is the non-police organisation making efficient and effective use of the PNC?

About the Environment Agency

The Environment Agency, which we also refer to in this report as "the Agency", has direct access to the PNC. It also has indirect access to the PNC through an arrangement with Her Majesty's Revenue and Customs.

The Environment Agency is a non-departmental public body reporting to the Department for Environment Food and Rural Affairs. The Agency has approximately 10,600 staff.

---

[4] *HMIC's 2015/16 Inspection Programme: An inspection framework prepared under Schedule 4A to the Police Act 1996*, HMIC, March 2015, page 11. Available from: www.justiceinspectorates.gov.uk/hmic/publications/hmic-inspection-programme-2015-16/

[5] The Home Office National Police Information Risk Management Team conducts audits to assure the Police Information Access Panel that PNC data is being held and used in an approved and secure manner in accordance with the supply agreement and relevant legislation, including but not limited to the Data Protection Act 1998, the Computer Misuse Act 1990 and the Official Secrets Act 1989.

The Environment Agency's functions include pollution control, waste regulation including the monitoring and management of international waste shipments, the management of water resources, flood and coastal risk management, fisheries, conservation and navigation. The Environment Agency holds formal enforcement powers and will, under certain circumstances, apply sanctions or initiate prosecutions.[6]

The Agency is also responsible for issuing various forms of 'environmental permits'. Businesses that manage or produce waste or emissions that pollute the air, water or land may be required to hold such permits.[7]

The Agency investigates environmental crime, predominantly in relation to waste. Illegal waste sites form a significant part of this work. These sites are created when criminals rent land or hire warehouses and fill them with (often toxic) rubbish, which they have been paid to dispose of responsibly. Criminals then abandon the sites and the cost of cleaning them up has to be met from public funds.

Methodology

This inspection took place in February 2015. Before the fieldwork stage, we reviewed documents (including the *Supply Agreement* and the *Security Operating Procedures)* in order to assist us in preparing questions for the interviews.

We invited the Environment Agency to provide us with documentary evidence of their adherence to the *Supply Agreement* and *Security Operating Procedures*. This was followed by a visit to the Agency's 'intelligence hub' in the Midlands (where the Agency's PNC terminal is housed). Over a day, we assessed the physical security arrangements and interviewed a cross-section of Environment Agency staff who use the PNC, including the manager, supervisors and PNC operators. We asked interviewees to show us how they used the PNC.

We examined the Environment Agency's internal audit process for the PNC. Through our interviews we tested interviewees' understanding of the internal audit processes and escalation procedures.[8]

We also reviewed data relating to the Environment Agency's use of the PNC. These data were provided to us by the Environment Agency, the Home Office and NDI Tech (the Agency's information technology supplier).

---

[6] *Enforcement and sanctions statement*, Policy 1429_10 (previously EAS/8001/1/1) version 3, Environment Agency, 2014.

[7] www.gov.uk/environmental-permit-check-if-you-need-one/overview, downloaded 5 October 2015.

[8] In this context, escalation procedures are the procedures that personnel are expected to adopt when an internal audit reveals that a PNC check has been conducted for an inappropriate purpose. Generally, the procedure involves referring the matter to a manager.

Findings

Scale of PNC use

The Home Office provided us with statistics on the number of PNC checks carried out by the Environment Agency for the twelve months to February 2015. We found that 1,729 checks in relation to people were carried out by the Environment Agency, either directly or through its arrangements with HMRC,[9] in the twelve months to February 2015. A further 3,994 vehicle checks were carried out over the same period. [10]

The level of access and authorised purposes for PNC use

We found that the Environment Agency was using the PNC in accordance with the terms of the *Supply Agreement*. Overall the level of access was sufficient to enable basic checks against people and vehicles, but we considered there were unnecessary limitations concerning the information displayed on the computer screen and the information that could be printed. There was also a lack of clarity in the *Supply Agreement* about whether PNC checks could be carried out as part of the process for issuing certain categories of environmental permit.

Level of access

We were provided with a copy of the *Supply Agreement*, which was agreed between the Environment Agency and the National Policing Improvement Agency on 4 October 2012 and was to continue in force for three years. The National Policing Improvement Agency was abolished in 2013 and as a result, responsibility for the PNC was transferred to the Home Office. Paragraph 6 of Schedule 8 to the Crime and Courts Act 2013 provides for the *Supply Agreement* to continue to have effect once responsibility for the PNC had been transferred to the Home Office, without the need for adoption of a new *Supply Agreement*.

The *Supply Agreement* specified that the Environment Agency was authorised to conduct 18 different kinds of PNC transactions. The most important of these transactions were:[11]

[9] Between 31 October 2014 and 23 January 2015, the Environment Agency's computer link to PNC was not working, so all the checks that were required in this period were undertaken by Her Majesty's Revenue and Customs.

[10] NDI Tech reported 789 direct checks on people and 120 vehicle checks in this twelve month period; the Agency reported 940 checks on people and 3,874 vehicle checks undertaken indirectly through HMRC over the same period.

[11] *Supply Agreement for PNC access Version 1.0,* Environment Agency, October 2012, Part 2 Schedule 1, paragraph 1.3.

1. Name (restricted): this type of check allowed an operator to type in the name of a person in order to determine whether the PNC holds a record of someone with that name. If such a record existed, the Environment Agency level of access allowed it to view certain information from that record, such as criminal convictions, arrest details and cautions. For this kind of check, the Agency's access was restricted to particular parts of the record.

2. Vehicle registration mark (basic): this type of check allowed an operator to type in a complete vehicle registration mark in order to determine if the vehicle was stolen or of interest to the police for some other reason. This type of check also revealed the name and address of the vehicle's registered keeper.

3. Vehicle registration mark (part): this type of check allowed an operator to type in a part of a vehicle registration mark in order to identify all vehicles with a registration mark that included the part of the registration mark that was used to make the search.

4. Postcode: this type of check allowed an operator to type in a postcode (or a combination of postcodes up to a maximum of six) in order to identify vehicles registered to an address within the area covered by the postcode that was used to make the search.

5. Transaction log: this type of check allowed an operator to type in a code in order to generate a list of previous checks carried out on the PNC. Generally this list was used for audit purposes.

Authorised purposes

The Environment Agency *Supply Agreement* states that the Agency will only access the PNC for the following purposes:[12]

- "To confirm the identity of persons who are the subject of investigation by the Environment Agency and who may also be of interest to the Police.

- To provide previous conviction history that may be recorded against persons that the Environment Agency is prosecuting or is relying upon as a witness in a prosecution.

- To conduct vehicle registered keeper searches in order to deal effectively with offenders, such as operations involving numerous vehicles and/or vehicles identified by the witness. Examples include fly tipping, poaching illegal fish movements and the transfrontier shipment of waste.

[12] *Ibid.,* Part 2, Schedule 1, section 2.

- To raise awareness of Warning Markers that are placed against violent persons and illustrate where an alias has been provided that can be connected to other names with a previous history of convictions or violence.

- For the purpose of producing an intelligence assessment."

We found that the *Supply Agreement* was not sufficiently clear to the staff we interviewed. We were told that carbon emission permits may only be issued to applicants without previous convictions, and we found that the staff we interviewed were unclear as to whether the *Supply Agreement* allowed them to use the PNC as part of the process for dealing with applications for these permits.

Our interviews revealed other areas of concern in relation to the Agency's level of access to the PNC. These were:

- the level of access allowed PNC operators to see only a partial names record;

- the terminal did not display any known associates of the subject;

- in instances where the person who was the subject of a PNC check had a conviction, the operator could see certain facts about the conviction such as offence type and court disposal, but not detailed information on how the offence had been committed; and

- the organisation's level of access did not enable them to print paper copies of complete PNC records (known as full printouts); instead they could only print information intended for disclosure in court (known as disclosure printouts).

Does the organisation comply with its Security Operating Procedures?

We found that the Environment Agency was compliant with most, but not all, of the requirements set out in the *Security Operating Procedures*. However, we found that audits had not be carried out as frequently as required, and the *Security Operating Procedures* document was overdue for review.

We were provided with a copy of the Agency's *Security Operating Procedures* and found that it had been created as a draft document in May 2010, with no evidence that the draft had subsequently been approved.[13] The previous version (version 1.0) dated from July 2004. This brings a risk that the procedures may no longer be appropriate, given changes in legislation and the Agency's policies and practices over time; we consider that organisations should review their *Security Operating Procedures* regularly, and ideally annually.

[13] *PNC Security Operating Procedures version 1.1*, Environment Agency, May 2010.

Training

One of the requirements of the *Security Operating Procedures* is that all PNC users must receive accredited training.[14] While at the intelligence hub we asked the Environment Agency to show us the relevant training records. These were extensive and satisfied us that all the Environment Agency's PNC users had received accredited training.[15]

Physical security

A further requirement of the *Security Operating Procedures* is that the PNC terminal must be located in a secure building.[16]

We found that the Environment Agency's PNC terminal was kept in a secure building. Access to the premises is through a foyer with a 24-hour staffed reception desk at which visitors are required to sign in before being issued with a visitor badge. Access to the building beyond the reception is by elevator and doors, both of which requiring swipe cards for access. Visitors must always be escorted into and out of the building, accompanied whilst they remain on the premises and on leaving the premises, they are required to sign out and return their badge. Physical security of the terminal itself was satisfactory.

Internal audit

The *Security Operating Procedures* and other related documents set out various requirements that are subject of internal audit. These include:

- PNC personnel are required to sign a document to confirm they have read the *Security Operating Procedures* and undertake to comply with them;[17] and
- use of the PNC will be subject to audit fortnightly.[18]

In relation to the first requirement, we examined the documentation and were satisfied that all PNC personnel had signed the appropriate document.

In relation to the second requirement, the only evidence of auditing we found was in June 2014, when 25 records had been audited.[19] At the time of our inspection, the

[14] *Security Operating Procedures Version 1.1*, Environment Agency, May 2010, paragraph 4.1.

[15] The College of Policing is responsible for the accreditation of PNC training providers.

[16] *Security Operating Procedures Version 1.1*, Environment Agency, May 2010, section 3.

[17] *Ibid.*, paragraph 3.17.

[18] *Ibid.*, paragraph 10.1.

[19] Data supplied by Home Office PNC Services.

Environment Agency had not audited any records for eight months. This is unacceptable, especially given the volume of PNC checks undertaken.

We were informed that, for the general management of its use of PNC and the associated auditing requirements, the Environment Agency had been reliant on one staff member. We understand that this staff member left the Agency at short notice and that it had not been possible to immediately recruit and train a successor to conduct audits.

Conclusions

Level of access

Taking into account the purposes for which the Environment Agency needs PNC access and the confusion over whether PNC checks may be carried out for carbon emission permit applications, we conclude that the Environment Agency needs direct access to the PNC but that the level of access specified in the *Supply Agreement* does not fully meet the Agency's needs.

The Environment Agency should provide the Police Information Access Panel with an amended business case that would set out its requirement for full access to PNC Names records and full printing capabilities in relation to the issuing of carbon emission permits.If agreed, this would allow the creation of more comprehensive printed records in addition to the disclosure printouts to which the Environment Agency already has access.

Compliance

We found that the Environment Agency has not been complying with all the requirements of the *Security Operating Procedures.*

The comprehensive training records, the physical security arrangements and the signed undertakings by all staff with PNC access were all reassuring, but the near absence of audit was not. The Environment Agency must remedy this. As the lack of auditing was partly a result of dependence upon a single member of staff who left the organisation at short notice, we recommend that the Agency increases its audit resilience, whether through training of additional staff or planning to obtain audit services from another organisation should its own auditor be unavilable.

We also advise the Agency to review its *Security Operating Procedures* and to ensure reviews occur more regularly in future, ideally annually.

Efficiency and effectiveness

We conclude that, by addressing the areas for improvement described above, the Environment Agency could make more efficient and effective use of the PNC.