Home Office

Independent Review Summary of Lessons Learned Report

Critical Incident - data deletion on the Police National Computer

19 March 2021

Contents

1. Summary

1.1. The records and information held by the Police help to keep us safe, but they, like many other public bodies, have an obligation to ensure the information they hold is appropriately managed. The Police National Computer (PNC) is critical to meeting these responsibilities. The PNC is part of the UK's Critical National Infrastructure and is the primary repository for UK criminal records. Almost every police activity will involve a PNC check on a person or vehicle.

1.2. First built in 1974 it is now maintained by Home Office, Digital Data and Technology (DDaT) on behalf of the Police. It has continued to prove effective in its simple task of providing background detail on people's character wherever they are found in the UK. It is a 47 year old system which has provided a stable service for users (99.95% availability over the last 3 years) but is inflexible when changes are required, also relying heavily on a diminishing skills base.

1.3. In February 2019, the Home Office PNC team began work as part of a programme of change first approved in 2011. They were aiming to improve the way a set of records, relating to police cases where 'no further action' was the outcome, were recorded and deleting records that should not be retained by law. This related to a law change in 2003 and was formally requested in 2007. Although applied in February 2020 it was not run on the system until November 2020 with records then being scheduled for deletion in January 2021.

1.4. Deletion of data from PNC happened on Saturday 9 January 2021. During this time, 112,697 person records were deleted from the PNC that should not have been deleted. Two of the systems connected to the PNC are IDENT1 (the National Fingerprints Database) and NDNAD (the National DNA Database). 26,329 DNA records were wrongly deleted from NDNAD on the same day. 195 full sets of fingerprint records were also wrongly deleted from IDENT1.

1.5. A number of queries were raised regarding the deletions over the subsequent 48 hour period, however it was only on Monday 11 January that the PNC team fully realised what had occurred. In fact, had it not been for intervention from the IDENT1 and NDNAD teams, it is not clear when PNC services would have been aware of the erroneous deletions.

1.6. It has been established that all records erroneously deleted are capable of being restored. The full restoration of the data is taking 15 weeks and will complete by 30 April 2021. In the intervening period mitigation measures substantially reduce the risk of harm to individuals or inefficiency in the Criminal Justice processes have been removed. Importantly, it appears that no one has been harmed as a result of the deletions of records and biometric data. It also appears that no one has escaped justice because of the loss of data.

1.7. The cause of the erroneous deletions was the introduction of a single error in the code created by the PNC team. This was the result of human error. However, the underlying causes lay not with the individual but the processes and culture that allowed this error to affect this vital database in such a profound way. The underlying causes include:

- Established procedures, such as reviews, were only loosely followed or in some cases not followed at all, such as not having fully defined business requirements or not maintaining an accurate record of tests undertaken.
- A failure to design effective and complete tests, including for affected systems, and what appears to be a significant failure of the manager whose responsibility it was to thoroughly review the testing procedures prior to approval. It appears this was not done.
- Testing of the new code was inadequate and specific processes within the change were not tested at all. It is concerning that the supporting documentation for these recent actions cannot be found.
- A failure from the first alert to act quickly resulting in an uncoordinated; ineffective effort exacerbated by the department incorrectly giving the all clear on the first alert.
- The context in which the PNC operates must be considered. It is a 47-year old system for which the replacement programme, National Law Enforcement Data Programme (NLEDP), that enables the decommissioning of PNC is undergoing a fundamental reset.
- The problems of an old IT system go way beyond the hardware and software associated with it. The team who operate it have worked together over a long period of time. The expertise and closeness of the teams involved in running the PNC increased the risk that their work would be accepted rather than checked by a leadership that were in a poor position to challenge their decision making. The PNC services team has very limited police experience in the team and have limited understanding of how the police operate.

1.8. The response to this incident has been of a far higher quality than the events which led to the erroneous deletions. However, it still took from the 11 January 2021 until the 7 February 2021 to issue a list of the affected records to police forces. This included a delay in the Home Office approving the release of the affected records to the police service which took an extra 5 days, which should have been avoided.

1.9. In the final analysis, major improvements need to be made in the following areas to address the underlying factors that led to this serious incident:

1. The creation of a culture in the PNC operation that promotes checking, testing and independent assessment of daily operations and change, to address the complacency that the review identified in the PNC operation.

2. The embedding and involvement of the Police Service and other PNC users into the decision making around the PNC and its development.

3. A strategic plan for the future of PNC and its replacement.

4. The Home Office and Police response to PNC Critical Incidents should be reviewed and refreshed.

2. Lessons and recommendations

Summary of Lessons Learned

1	Police-led control of changes to PNC, including their prioritisation, is essential
2	Software development lifecycle quality and compliance processes must be fully fit for purpose
3	A single, joined-up DDaT incident management approach can make the response to incidents more efficient
4	Rehearsing Home Office Gold Command is essential to prepare for incidents of this nature and scale
5	Issuing accurate, clear and timely information to operational users enables them to more quickly assess risks and impacts
6	Don’t rely on a diminishing skills base
7	Investing in the sustainment of critical legacy IT services such as PNC is critical
8	Working together generates a commitment to improve and to put things right
9	Understanding and managing threats to public harm must be the priority for everyone working on PNC

Lesson 1 - Police-led control of changes to PNC, including their prioritisation, is essential

Recommendation 1 – P4G must control and approve all changes

- The Police PNC Policy and Prioritisation Group (P4G) must approve and prioritise changes before any work can commence. Changes must have impact assessments provided at this stage.
- All changes which haven't commenced within 6 months of approval must be reapproved by P4G to validate the business requirement, before development work can begin. P4G must have refreshed impact assessments at this stage.
- P4G must provide approval before the release of all changes to the live system.

Recommendation 2 – PNC user representatives must be involved at every stage of developing and running the PNC

- PNC's policing and non-policing users, sponsors or subject matter experts must be involved at every stage of the software development lifecycle and decision-making.

Recommendation 3 – A Protocol must be agreed for information ownership and escalation

- The needs of the data controller for PNC (the Police) and the data processor (the Home Office) can potentially come into conflict. This can happen where there are different priorities for handling communication and data sharing. It is for these very specific, but potentially critical events, that a clear Protocol must be provided by the Police and agreed between the parties.
- The Protocol must be explicit in determining what information is required for operational policing purposes. The Protocol must maintain the operational independence of the Policing Gold groups to ensure the public are kept as safe as possible whilst the investigation and detection of crime continues.
- The Protocol must separate operational information from other matters that have little impact on the delivery of policing services. The Police Gold would take precedence of information that is required for operational policing purposes.
- The Protocol must explain the relationship, levels of visibility, and associated authority from Policing into Home Office Gold, to bring consistency and awareness across key command structures and communications.

Lesson 2 - Software development lifecycle quality and compliance processes must be fully fit for purpose

Recommendation 4 – A Technical Architect must be responsible for the end to end technical design of the PNC

- Ownership of all PNC architecture must be undertaken by a specific person within the PNC services team. This person must be responsible for providing leadership, direction and accountability for the full technical design.
- This person must ensure the architecture is documented so people involved in developing and running the service understand the technical design, including different database processes and how the PNC interacts with other systems. This will reduce the risk of PNC changes bringing unwanted impact on other systems, such as NDNAD and IDENT1.

Recommendation 5 – Product management lifecycle techniques and principles must be applied to the PNC service

- Software for PNC must be developed using more formal product management principles. For example, designated product owner(s) with clear accountability for the team's delivery activities and working practices to ensure user requirements are met and product manager(s) with a strategy for PNC's short term and longer-term plans.
- Introducing new ways of working could include the potential for more frequent and smaller releases.

Recommendation 6 – Business analysts must describe the 'why' and not just the 'how'

- When making changes to the PNC the priority for business analysts must be on 'why' a change is required by users and not just 'how' it is to be done.
- This must be clearly documented within the business requirements and communicated to all those involved in developing or updating software. These business requirements must include an understanding of the impact on users of all affected systems from an operational user perspective.

Recommendation 7 – Effectiveness of PNC software engineering practices and leadership must be fully fit for purpose

- Leadership for the engineering function within PNC must be fully fit for purpose, bringing accountability for the quality of development work, whilst helping to make improvements to the engineering practices.

- A full evaluation of software development activities must be undertaken within 4 weeks, to ensure best practice is followed. For example, code reviews, pair programming and technical testing. Subsequent improvement actions must be planned and implemented at the earliest opportunity and within 4 weeks where practical.

Recommendation 8 – PNC testing practices and management must be fully fit for purpose and compliant with defined standards (Test Maturity Model integrated - TMMi)

- Management for the testing work within PNC must be fully fit for purpose with responsibility for the quality of testing to standards.
- Testing controls must be in place to ensure test planning, risk-based testing and end-to-end testing are effective. Improvements must be planned and implemented within 4 weeks.

Recommendation 9 – PNC change and release practices must ensure the integrity and effective management of the PNC technical environment

- PNC must implement tighter control mechanisms for managing the configuration of the full PNC technical environment. This includes version control and configuration management for all elements of the PNC service.
- Any approved changes where greater than 4 weeks have elapsed since an approval was last given, must be recycled for further approval to ensure a current risk and impact assessment is in place before deployment. Any changes introduced to PNC but not run immediately, such as future dated batch jobs, must be recycled for a further risk and impact assessment every 4 weeks.
- Release managers must be involved throughout the software lifecycle, including input to all risk and impact assessments for every change to the system.

Recommendation 10 – Assurance controls must be in place to manage quality and compliance to standards

- Assurance must be provided that the right quality controls are in place and that they are being consistently followed. This must include opportunities to provide challenge, reviews and governance on key outputs such as business cases, test plans and release plans, for example. As part of the assurance process, there must be clear definition and compliance with any relevant technical standards such as TMMi and ISO.
- Formal independent assurance reviews, covering the full development process, must be undertaken at least every 12 months in the form of an annual health check

Lesson 3 - A single, joined-up DDaT incident management approach can make the response to incidents more efficient

Recommendation 11 – Do it once, via a single, joined-up DDaT incident management function

- The process for responding to and managing incidents on the live PNC system must be converged to enable a single team approach, as is standard practice elsewhere within DDaT. This includes convergence onto the 'ServiceNow' IT service management tooling as the DDaT standard.
- Knowledge must be transferred and shared across nominated individuals across the local PNC and core DDaT Incident Management teams, to close any gaps and increase the depth of PNC knowledge held to enable rapid response, including early understanding of other systems that may be impacted.
- Record keeping and work notes must be clear and accurate, including precise timing of key events such as the start, communications, technical bridge calls, suspension or activation of key processes, identification of cause and effect.

Lesson 4 - Rehearsing Home Office Gold Command is essential to prepare for incidents of this nature and scale

Recommendation 12 – Home Office Gold Command procedures must be rehearsed

- Home Office Gold command procedures must be reviewed and updated to reflect the lessons learned from this incident, including bringing in Police experience to support best practice. This must be done at the earliest opportunity.
- The revised Gold Command procedures must include specific steps to ensure that the correct stakeholders form the response team with defined roles and responsibilities. For example, Home Office Policy, Legal and Communication personnel must be considered at the start of the response. Priority must be given to quickly address public harm threats and impacts.
- Gold Command procedures must be rehearsed regularly and include the bridge to Silver and Bronze commands. Training must be provided for key personnel.

Lesson 5 - Issuing accurate, clear and timely information to operational users enables them to more quickly assess risks and impacts

Recommendation 13 – The Home Office must create and maintain an accurate record of stakeholders

- An accurate record of all police and non-police stakeholders must be held by the Home Office. This stakeholder map must be accessible to everyone who needs it, it must be up to date, and it must contain accurate details for all primary contacts and deputies, including 24x7 contact points for the most critical services.
- All PNC teams must develop an improved understanding of the user base so they can understand how services are used and what types of information and data are important for those users.

Recommendation 14 – The Police must enhance their Communications Strategy for critical incidents

- The strategy for the Police to manage critical communications during a critical incident must be reviewed and updated. This work must be undertaken within 4 weeks.
- A review of the strategy must include how to direct communications through all the required points of contact (including deputies) and via different channels.
- The strategy must address how assurance is applied to ensure the content and guidance is clear and consistent, so the nature and impact of an incident can be quickly understood, and appropriate action can be taken by all required parties.
- The strategy must address the need for clear communication on direction and coordination from the National Police Chiefs' Council (NPCC) so a more consistent approach can be adopted by the forces.

Lesson 6 - Don't rely on a diminishing skills base

Recommendation 15 – The Home Office must manage critical PNC knowledge

- All essential documentation must be managed through formal review and sign-off processes and stored appropriately for easy reference. Modern tooling, like SharePoint for example, must be considered to enable teams to record, manage and share documentation, knowledge articles and guidance.
- This knowledge and supporting documentation and guidance must include how and why other systems, such as NDNA and IDENT1, connect to PNC.

Recommendation 16 – The Home Office must provide sufficient capacity for trained people to safely develop and support PNC

- A PNC Capability Development Plan must be developed and implemented in order to grow the number of people with specific PNC knowledge and skills.
- The Plan must address how to bring in Police representatives as part of the PNC team, further training for existing staff, and succession planning.
- The areas of poor performance identified during the review must be addressed via standard Home Office HR and Contract Management procedures.

Lesson 7 - Investment in the sustainment of critical legacy IT services such as PNC is critical

Recommendation 17 – There must be a plan, with investment, to sustain PNC for its full life

- Within 8 weeks, the Home Office must provide the Police with feasibility options, including estimated timescales, costs and risks for either replacing or sustaining the PNC.
- Options should consider whether the responsibility for running the PNC should remain with the Home Office.
- There must be direct links between the governance boards of PNC and the programme delivering its replacement (NLEDP). This must include relevant policing representatives in order to fully understand any changing plans or risks that may impact immediate and future PNC decisions.
- The Home Office must develop a controlled implementation plan to ensure recommendations from this review are acted upon and their effectiveness assessed. This implementation of this plan must be assured every 8 weeks.

Recommendation 18 – PNC technology must be made more resilient

- PNC must investigate methods, both short term and longer term, to introduce or improve technology resilience to the PNC service, such that problems can be prevented or intercepted.
- This investigation must include defensive measures such as system monitoring and alerting, automatic suspension of system processes based on set parameters like limiting the number of deletions.

Lesson 8 - Working together generates a commitment to improve and to put things right

The commitment shown in working together across the Home Office, policing and wider agencies to recover and help prevent reoccurrence of this incident was seen as a positive lesson.

Recommendation 19 – Keep working together, maintaining a strong commitment to improve and put things right

- This teamworking and open approach must be maintained and recognised.
- All parties involved must maintain support and care for the welfare of personnel involved in incidents of this scale and nature.

Lesson 9 - Understanding and managing threats to public harm must be the priority for everyone working on PNC

Recommendation 20 – Threats to public harm must be understood and managed by all those working on PNC

- Staff must acquire sufficient understanding of when and how the public may be impacted or harmed as a result of work being undertaken on the PNC.
- Within 6 weeks, each function within PNC, for example incident management, change and release, and testing, must consider and implement any process improvements to specifically manage public harm threats.
- All impact and risk assessments (including for changes already in progress) must specifically and clearly consider public harm.

Recommendation 21 – Understand the full public harm impact of this incident

Once data restoration is complete, and records retained in error have been removed:

- Policing must complete work to fully understand public harm impact.
- Non-policing must complete work to fully understand public harm impact.
- The Home Office must revisit the legal position and refresh legal advice.

Annex | About the review

Terms of Reference - Review Objectives

The purpose of the review was to establish where and how the error was introduced that led to wrongful deletion, why the Home Office's test and assurance processes did not find the error, and what action should be taken to reduce the risk of reoccurrence. The review also examined the speed and conduct of the incident response.

Timeline

The review started on 9 February 2021 with a final report produced on 19 March 2021.

Independent Panel

The Panel reported into the Home Office Permanent Secretary and was made up of:

- Lord Bernard Hogan Howe (Chair) – Home Office advisor on police engagement
- Simon McKinnon – DG DDaT, Department of Work and Pensions (DWP)
- John Paton – Home Office Non-Executive Director

Review Team

The supporting review team involved Home Office DDaT personnel plus two external policing experts representing the NPCC plus a DDaT expert from DWP. The review team undertook detailed investigation work, providing their findings and recommendations into the Panel for consideration.

[End of Report]