Home Office

Minister of State for Crime and Policing, Home Office
2 Marsham Street
London SW1P 4DF
www.gov.uk/home-office

Rt Hon Yvette Cooper MP
Chair, Home Affairs Select Committee
House of Commons
London
SW1A 0AA

27/01/21

Dear Yvette,

Thank you for your letter of 15th January regarding the deletion of PNC records in error. This is a very serious matter and I share your concerns. I would like to update the Committee on what we are doing to resolve the matter, and most importantly to make clear what is being done to protect the public and ensure similar incidents are not repeated.

During what should have been a routine exercise to remove data as an update to the PNC, and as a result of human error, the software which triggers automatic deletions contained defective coding. This inadvertently resulted in the deletion of records which were not to be deleted. It also meant that it had not deleted some records which should have been deleted.

A response team consisting of Home Office civil servant technology experts was immediately established to take command of the incident and to alert the police and other operational colleagues. We established a Bronze, Silver and Gold command to manage the incident and coordinate a rapid response, issuing specific guidance for police forces and other partners to ensure they were kept abreast of the situation.

Working closely with the NPCC, police, and other partners, we immediately initiated, through the GOLD command, an assessment of the full scale and impact of the incident. This included undertaking a robust and detailed assessment and verification of all affected records, followed by developing and implementing a plan to recover as much of the data and records as possible, and developing plans to mitigate the impacts of any data loss. This remains our focus.

Please be assured that decisions around individuals are not solely based on PNC data and therefore the risk to the public is minimal; police forces are able to work with other data sources to inform their decision making and reduce operational impact, and are actively doing so.

As you would expect, the Home Secretary has commissioned a full “lessons learned” review to establish exactly what happened, and to address the operational and technical failures that led to this unacceptable situation to ensure it cannot be repeated. We are appointing an independent team to lead this work.

You have asked a number of specific questions relating to this issue.

1. Exactly when did the error occur?
The data was deleted in a routine scheduled system update that ran overnight on 9/10 January. Home Office engineers identified that there was a problem with the routine on 10 January 2021 and an immediate investigation began.

2. Given the initial figure of 150,000 lost records was later reported as 400,000 records, can you please quantify the precise number of records that have been lost? Is there any further possibility that this number could be revised?
Estimated numbers of records potentially deleted in error from the PNC are:

- 213,000 offence records,
- 175,000 arrest records and,
- 15,000 person records.

In addition, a total of 26,000 DNA records and 30,000 fingerprint records in related databases are also being investigated as potentially deleted in error.

3. Why was the Home Office not able to ascertain an accurate figure straight away?
As soon as the error was identified all necessary resources were prioritised to understand the extent of the loss. It took a short amount of time to confirm due to the complexity of the systems involved and how they link together. It is worth noting that at least some of the deleted records will be valid deletions.

4. How did the deletion occur during what, according to reports, is a routine process carried out regularly?
This is a regular housekeeping task. However, a software defect introduced during a recent update to this task in November 2020 has resulted in this issue.

5. What was done differently, or not done, that could have allowed this to occur?
A software defect introduced during a recent update to this task has resulted in this issue.

6. What safeguards does the PNC have built into it, which seek to minimise the risk of accidental data loss or contamination? Were these safeguards operating fully at the time of the deletion?
The Home Office has robust procedures in place to ensure all software changes are thoroughly tested before they are deployed into the live environment. In this case these procedures were either incorrectly implemented or were not adequate to identify this particular software issue. We will be undertaking a detailed lessons learned review to identify exactly what went wrong and what corrective action is required.

7. What arrangements (if any) are in place routinely to back up and restore data erroneously deleted from the PNC and associated databases? To what extent have these arrangements proved effective in this incident?
Backups are held for all systems. Due to the scale, complexity and dynamic nature of how the affected systems interact, restoring from backups needs to be undertaken in a controlled manner and our technical teams are now working at pace to do this safely.

8. Why was it not possible to restore the estimated 150,000 records referred to in today's reports?
Our technical teams are currently working on this, but you will appreciate the restoration of data is a complex task that needs to be done in a careful manner.

9. Is it possible to reconstruct or replace any of the lost data from other sources? If so how, and how quickly, can this be done?
Yes, our technical teams are assessing how this can be done.

10. Could you explain the process behind 'weekly weeding' of the PNC, as referred to in coverage of the error?
PNC runs a weekly deletion process to update the PNC, extracting PNC reports based on their dates and so ensuring PNC complies with different legislative requirements for different UK jurisdictions.

10a. Does the estimated 150,000 figure for deleted records include records that were removed at the end of 2020 when the UK stopped accessing SIS II?
No, this number is related to this process only and not to any other deletion process.

10b. Was the same weekly weeding process used to remove SIS II alerts from the PNC at the end of 2020? If not, why was a different process preferred in that instance?
No. A different process was used for deletion of SIS II data because that data was held in a different way.

11. Could you please provide more detail and statistics about the records that have been lost, to include categories and quantities of data? I understand that some elements of this information might
need to be sent to the Committee privately.
We will provide an update on data and records once we have completed restorative data work.

12. Please could you explain how this loss of data interacts with records lost as a result of the UK losing access to the SIS II database? In particular, given the c.40,000 alerts on arrest and missing persons removed from the PNC as a result of leaving SIS II, how may persons of interest in total have been lost from the PNC since December?
There is no relationship between this incident and the SIS II deletion of records.

13. What is the Home Office doing to make sure it is certain about exactly what data has been lost?
The technical process is ongoing and I will update the House accordingly.

14. What is your initial assessment of the effect of losing the data on:
• Policing operations
• Policing intelligence
• Possible future prosecutions
• The reputation of UK law enforcement with its international partners
We are working with the police to prioritise recovery of high impact cases. We are engaging with international partners and reassuring them on our work to correct what has happened, in the context of the small percentage of records affected that PNC has with international partners.

15. What impact has the error had on the visa application system? Specifically, could you provide -

15a. The number of applications paused or delayed as a result of the lost information:
Given the relatively low volumes of cases at the moment and the short period over which we suspended activity we believe only a small number of applications were affected.

15b. The average time by which applications were delayed:
The maximum duration that any application has been delayed is less than 24 hours.

15c. What proportion of visa applications that had been paused are now able to proceed:
All visa applications have been able to proceed since Wednesday 13 January.

15d. What action the department has taken to inform affected individuals about possible delay:
Only those who chose to pay the additional fee for the Priority Visa Service or Super Priority Visa are affected. If the service standard was not met, they will be contacted and informed of the delay and offered a refund of the fee for that service.

15e. Where the loss of information materially affects the ability of the Home Office to grant a visa:
The loss of the information has not affected UKVI's ability to issue a visa.

15f. How it will provide equivalent information to substantiate its visa decision:
The loss of the information has not affected UKVI's ability to decide a visa application.

16. What action does the Home Office intend to undertake to ensure that lessons are learned from this error and to review processes that might have led to it?
There will be a full and independently led lessons learned exercise.

16b. By when do you expect the Home Office to have completed an internal review? Will you share the main conclusions of that review with the Committee?
This is being organised and we will share the details with the Committee.

16c. Will you consider inviting HMICFRS or the National Audit Office to conduct their own review of the processes involved that might have led to this error?
We are exploring different options.

17.The Police National Computer is due to be replaced by the National Law Enforcement Data Programme, as is the Police National Database. In its report on Major Projects 2019-20 the Infrastructure and Projects Authority (IPA) rated the NLEDP project as Amber/Red. Urgent action is needed to address these problems and/or assess whether resolution is feasible". In light of this, can you tell us:

17a. What major risks were identified during the IPA's review?
In November 2019 the Infrastructure and Projects Authority (IPA) gave NLEDP a delivery confidence rating of Amber.
The major risks identified were in the following areas:

- Finance (in quantum and in profile through major law enforcement portfolio prioritisation)
- Access to and the ability to retain suitably qualified and experienced IT development and programme and project personnel
- The expectation of stakeholders and users for rapid development of NLEDS capability after its foundation delivery
- The ability to 'nudge and lead' users to key change dates through influence alone without the lever of direct financial control

17b. What urgent action has been taken to address these risks?
Several actions have been taken to mitigate these risks since the IPA report in 2019 which are listed below. The programme entered a re-set in November 2020 and we are working with police stakeholders to deliver a refreshed plan and business case for the programme. This work supersedes the previous IPA report actions

17c. Is successful delivery of the project still in doubt?
We took the decision to initiate a reset of the programme in November 2020 because costs and timelines were extending outside the extant business case boundary. We are working with police stakeholders to deliver a refreshed plan and business case for the programme.

18. How has the maintenance of the PNC been sustained to the required standard while NLEDP is in development?
We continue to invest in maintaining PNC. For example, in 20/21 we have allocated £15m to carry out technical refresh of PNC and the Police National Database.

19. The contract to deliver the NLEDP was awarded to IBM UK in October 2016, was expected to start in February 2017, and to run for two years at a cost between £10 million and £12 million.

19a. What is the current expected delivery date?
The programme plan is undergoing a re-set. The business case and plans will be presented to Cabinet Office and Treasury later in the year.

19b. What is the cost to date and estimated cost to complete the project?
Costs to date to financial year end 19/20 are £150m. Work is underway for the 2021 business case and costs to complete will be baselined in this case. It is worth noting that the IBM costs quoted above are not (and were never) intended to be the full cost of delivering NLEDS.

19c. What is the impact of the late delivery of this programme on the support provided to law enforcement and other Agencies?
There will be no significant capability gap as law enforcement and agencies support continues through PNC and PND.

20. In October 2020 a Data Protection Impact Assessment of the Law Enforcement Data Service element of the new NLEDP found that there was "currently no process in place for reviewing and deleting court convictions on PNC. Agreement for LEDS processing of convictions needed between Home Office, MoJ, Court Services & Probation Service." This was one of 17 risks identified in the assessment of the new service.

20a. Have recommended mitigations been put in place for this and the other 16 risks identified?
Plans for risk mitigation are as follows:

- New ways of working will be needed to ensure efficient disclosure of information to data subjects. Better and more joined up processes are needed across the criminal justice sector. Initial conversations about these processes are underway.
- Improved data quality will feature more significantly within LEDS and dedicated resources have been directed towards this outcome.
- Two are dealt with through transformations to existing business mitigations.
- Two require reviews will be conducted into the retention and subsequent use of information.

21. Please provide a timetable and outline plan for the implementation of mitigations and monitoring of risks across the LEDS.
We are working with the operational community to further develop the framework through more detailed operational guidance. Detailed performance metrics will provide the detail against which the mitigations can be implemented and monitored.

22. Did this Impact Assessment lead to any changes in the management of PNC data that could have led to the erroneous deletion of records?
No.

23. What checks and controls are included in NLEDP to prevent the errors like those discussed in this letter happening in future?
LEDS will be governed by a set of processes closely aligned with ISO 27001. It will have many layers of security and operate in line with a cautious approach to risk management. This is complemented by a Data Quality approach which will maximise the data integrity protections. Importantly where manual data processing is required enhanced review and management processes will be implemented.

We are working with the Information Commissioner's Office to agree what the safeguards and processes for LEDS should be and will include lessons learned.

Yours sincerely,

Kit Malthouse MP
Minister of State for Crime and Policing