INFORMATION SECURITY AND GOVERNANCE

Independent Review

Systems, Policy, Processes, Practice, Culture & Behaviours - in response to the Data Breach Incident of 8th August 2023

TERMS OF REFERENCE

1. Introduction

This Review has been *jointly* commissioned by the Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI) into the circumstances surrounding an information security data breach incident on 8th August 2023 that led to disclosure of personnel records to '*Whatdotheyknow.com'* public website in response to a routine Freedom of Information (FOI) request.

This Review will be led independently of the NIPB and the PSNI and is designed to:

(1) Investigate (a) the processes and actions that led to the breach occurring and, (b) any organisational, management or governance factors that allowed that breach to occur;

(2) Identify any action required to prevent further data leaks, to build more robust future risk mitigation systems and to make recommendations for any necessary improvements to information governance systems, policy, organisational practices, cultures and behaviours; and

(3) Restore confidence in the organisation's approach to information security.

Note: C*onsequence management* relating to the immediate information security actions, incident investigation and personnel security and welfare matters following the specific incident continue to be governed separately via Gold Command critical incident response under Operation Sanukite.

2. Background

On 8th August 2023, the Police Service of Northern Ireland (PSNI) suffered a critical information security data breach following a routine Freedom of Information (FOI) request. Data contained within a spreadsheet was published on a legitimate website called www.whatdotheyknow.com.

The detail was formatted into thirty-two (32) columns including the surname, initials, rank/grade, role, service number, department, location, duty type and gender of all serving officers and staff.

Due to the sensitivity of the information, as well as the ongoing SEVERE threat level, a Critical Incident was declared on the 9th August 2023, with reporting into (PSNI) Platinum and Gold Command structures.

This loss of information has caused unquantifiable damage to the confidence of officers and staff in the PSNI, as well as in the eyes of the public and the PSNI's policing partners, as to the capability to safely and securely handle personal and sensitive data. As result, this Independent Review has been commissioned.

The Senior Responsible Officer (SRO) undertaking this Independent Review will report directly to the Chair of the Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI).

A summary of the governance structure for the Independent Review is attached at **Appendix I** for reference.

3. Scope of the Independent Review

The **objectives** of the Independent Review fall under the following key themes:

Processes and Protocols

1. To review the workflow processes in place at the time of the breach, establish compliance against any documented Standard Operating Procedures and/ or agreed processes or policies.
2. To identify the root cause(s) of the information security breach and record any learning.
3. To review the current process for handling FOI requests against compliance with the 'NPCC FOI Manual of Guidance' and the 'ICO Guide to FOI' and make recommendations
4. To identify business areas that handle large volumes of sensitive personnel data that are routinely requested under FOI and the IT systems that support those processes.
5. To review current information security and data handling steps (including accountability, quality assurance, system limitations, access permissions and information security standards) for those processes and systems identified in point 4.
6. To inform options for mitigating risk of future information security incidents for those processes and systems identified in point 4.

Policy and Systems:

For those systems identified under point 4 above:

7. To review Standing Operating Processes and any other internal policy, guidelines, service instruction(s) or standard(s) particularly where there are instructions for the extraction of data, attaching of documents and the application of controls to data released to third parties.
8. To review the assurance documentation, identifying any gaps in assurance or residual risks that are relevant to the breach.
9. To review the development of standards for these systems, comparing to required.
10. To review existing auditing and monitoring capabilities.
11. To review controls/ alerts and presence of any technical failsafe mechanisms in place relating to the transfer of information and options for further development.
12. To examine and provide advice on any changes to information security requirements/access permissions and controls.
13. To provide advice on updated Security Assurance for Policing (SyAP) scores where appropriate.

People - Culture, Practice and Behaviours:

14. To review the skills sets required and/or training needs and status for personnel involved in data sharing functions.
15. To assess attitudes and behaviours surrounding the robustness of organisational information management practices including evidence of proportionality of data sharing.
16. To examine lines of accountability, governance and oversight in information management roles.
17. To review adherence to legal obligations.

4. Governance

In order to ensure that the Review has the appropriate powers to complete a thorough investigation, a partnership has been agreed between the Northern Ireland Policing Board (NIPB) (as the accountability body) and the Chief Constable of the Police Service of Northern Ireland (PSNI) (as the body with operational responsibility).

The Senior Responsible Officer (SRO) for the Independent Review is **Assistant Commissioner Pete O'Doherty**, NPCC Lead for Information Assurance. The SRO will be supported by a Review Team that includes a number of specialists that work for both Police Digital Services and the National Chief's Police Council. The members of the team provide extensive skills and experience in freedom of information requests, information and cyber security, data protection and compliance.

The Chief Constable, the NIPB and the Review Team will develop procedures to protect personal information of individuals (including officers and staff) and ensure that confidentiality of information is maintained during the Review period and in the Report.

5. Leadership of the Review

The Review will be led by the SRO as outlined at Section 4 above. Designated Single Points of Contact (SPOC) for all matters of logistics and support to the Review Team are as follows:

- **Aldrina Magwood, ACO Strategic Planning & Transformation - PSNI**
- **Sinead Simpson, Chief Executive - NIPB**

A PSNI corporate support team will be established to facilitate and enable the work of the Independent Reviewers.

In addition, the Department of Justice (DOJ) will provide critical peer support as required.

The NIPB and the PSNI will provide access to the following as are relevant to the scope of the Review:

a. Policies and systems.
b. Related training material.
c. External and internal risk, assurance and audit reports.
d. Briefings from key staff in relation to the above.
e. Other requests or access to staff to be agreed.

6. Methodology & Timescales

The Review Methodology will assess against relevant sections of established professional and expert standards, including police standards, and best practice.

Standards will include, but not be limited to, College of Policing Information Management APP, NPCC published standards and Manuals of Guidance, and policing security standards. The review may also have regard to broader relevant standards such as ICO and government Digital Data and Technology (DDaT).

'Best practice' is what has been established as such by the NPCC DDaT Coordination Committee and sub portfolios, the expert National Police FOI and Data Protection Unit, and the Police Digital Service (PDS) Cyber and Data Units. The Review will also simultaneously be working closely with the NPCC National Police Data Board to identify any further good practice of relevance.

It is expected it will be necessary to conduct a phased Review to deliver the full scope of the objectives commissioned.

- **Phase 1** – will commence 29th August 2023 and will deliver the objectives relating to the specific data breach incident of the 8th August 2023. This Phase will be completed on the 8th September 2023 and will include Stages 1 and 2.

The outcomes of Phase 1 will further inform the Review Plan proposed to deliver fully the objectives agreed as part of Phase 2.

- **Phase 2** – will run sequential to Phase 1 and will involve Stages 3, 4 and 5. Phase 2 is estimated to be completed by the 30th November 2023

The Review will be conducted in five (5) stages:

Phase One – Discovery

Stage 1 – (21st August 2023 to 28th August 2023):

- Logistics
- Documentation
- Interview and observation schedule
- Commencement of online research

Stage 2 – (29th August 2023 to 8th September 2023)

- Request of any further documentation considered relevant by the Review Team.
- Undertake interviews[1] and observations as agreed, and as may become necessary throughout the Review.
- Continued online research.
- Any high risk finding requiring immediate action will be notified as soon as possible and where possible, be reported to PSNI Gold Command.
- 'Hot debrief' and sharing of high level findings with the NIPB and the PSNI. This will include an overview of any high risk findings notified through the PSNI Gold Command structure.

By the end of Phase One and to ensure procedural fairness the Independent Review Team will establish and provide the facts required to enable the appropriate authority within the PSNI to make a determination if any disciplinary procedures should be initiated.

Phase Two - Report Preparation & Reporting

Stage 3 – (September to October 2023 plus 2-weeks for slippage)

- Review Team review and write-up of findings.
- Research into current best practice amongst Home Office Police Forces will be conducted to further inform recommendations.
- In writing the Report, the principles of FOI with be applied to the Main Report intended for future publication. Any findings not suitable for public disclosure will be prepared for sharing with the NIPB and PSNI in closed session.
- Follow-up of any significant action taken in the period since the review and high risk, immediate findings reported as part of the site visit.

[1] The Review Team will undertake all interviewing in a sensitive manner and in-line with the wellbeing and welfare objectives of the PSNI. Noting that establishing the full facts of the data breach is dependent upon the cooperation of the organisation's employees.

Stage 4 – (Estimated Mid November 2023)

- Review of factual accuracy with relevant parties
- Consultation with relevant parties in relation to establishing any harm to inform the decision making for inclusion in the 'closed' report in line with FOI obligations
- Finalisation of the publication date
- Final draft of the Report by the Review Team

Stage 5 – (estimated End November 2023)

- Final version of the Report presented and released to the NIPB and the PSNI.
- Consideration of requirement for any follow up.

Delivery against the timeline will be subject to availability and access to all relevant information.

7. Deliverables

The key deliverables of the Review to the Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI) include the following:

- Regular feedback on findings as the Review progresses.
- A Draft Report, enabling both parties to provide comment.
- A Final Report.

In conducting the Review, the Reviewer will comply with all applicable laws, including in relation to personal information

8. Publication

The Final Report will be published.

The Northern Ireland Policing Board (NIPB) and the Chief Constable of the Police Service of Northern Ireland (PSNI) will be provided with an un-redacted copy of the closed findings subject exempt from disclosure under FOIA if applicable.

The details of the report will be kept confidential until both parties decide on the publication arrangements. The Permanent Secretary or Minister for Justice (subject to any return to the NI Assembly) will be advised of publication arrangements and provided with a copy of the Report.