Data Protection Impact Assessment (DPIA) – Stage 1

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to refer to the guidance material available here [link to be created] before completing the form.

Data Protection Impact Assessment (DPIA)	
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.	
Section 1 - Governance	
Project Proposal Name:	*Police Cyber Alarm – Network Traffic Analyser*
Information Asset Owner:	T/DCS Andrew Gould (Metropolitan Police)
DPIA Coordinator: (Someone from the business area, a middle manager with a hands-on role with the project, heavily involved in its delivery.)	**S23** (Derbyshire Constabulary)
Date on which processing will commence:	01/09/2020
Date submitted to the DPS: (Data Protection Section)	15/05/2020
Date of latest update	01/03/2021
Note: The DPS will give an **initial response** within 10 working days of receiving the completed form.	

DPS Assessment		
DPS Use Only (Ensure the Asset and IAO are added to the Records Manager's IAO Register where appropriate.)		
A. DPIA is not mandatory.	☐	
B. A DPIA Stage 2 is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA Stage 2 will be required.	☐	
C. A full DPIA is mandatory.	☒	

Section 2 – Nature, Scope, Context and Purposes

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

Introduction

This document has been created for the National Police Chiefs' Council (NPCC) National Cybercrime Programme. The Lead for Cybercrime is Chief Constable Peter Goodman (Derbyshire). The NPCC Information Asset Owner and DPIA Co-ordinator are stated at Section 1 above. The latter is also the NPCC Project Manager for Police Cyber Alarm. The same team were responsible for procuring and rolling out Cybercrime tools for national use during 2019. At that time, due to time constraints and the NPCC not having their own Procurement and Data Protection Teams the work was undertaken by Derbyshire Constabulary on behalf of the NPCC Lead and Project Manager. Following that precedent, the same route has been followed for the procurement of Police Cyber Alarm, while the NPCC have paid for some Derbyshire Data Protection Team members to carry out this work on behalf of the NPCC Cybercrime Programme. Derbyshire Constabulary's Records Manager will provide advice and support. Otherwise, the Force does not have any more direct involvement in this project than any other Force invited to promote and make use of the Police Cyber Alarm tools.

Background

Policing recognises that it needs to address the changing pattern of criminal behaviour and offences. Much crime is now committed on the internet. When compared with the physical world, the Police currently have limited knowledge and intelligence about the criminal activity that is taking place. As crime is increasingly committed in the cyber environment, both businesses and individuals are becoming more vulnerable to attack. This is particularly so at the level of local Policing. In a move to address this risk and threat, Policing is to offer to deploy technical measures that represent a new kind of Police patrol and invite citizen engagement to create 'cyber neighbourhood patrols' which will enable a Police vision to protect the cyber neighbourhood in partnership with local businesses.

Those responsible for leading the Policing response (to cyber enabled crime[1]) recognised the need for the Police to identify its 'Requirements for the Analysis of Internet Data' (RAID) and undertook a project with that name. The RAID Project Board chaired by Chief Constable Goodman defined a 'single statement of user needs' to be adopted across the country to avoid (within Policing) duplication and disparity of direction, resources and effort. This statement states that national Policing needs:
"a capability to provide timely collection and processing of computer network traffic data to be able to analyse the data to produce information, intelligence and evidence in a legally compliant and ethical manner in order to Pursue, Prevent, Protect and Prepare."

Pervade's Police Cyber Alarm
Following a trial of three 'products' an open procurement process resulted in Police Cyber Alarm (PCA) being purchased from Pervade.

Two elements of the functionality of Police Cyber Alarm are its ability to:

1. Vulnerability scan IP addresses and
2. Vulnerability scan websites and web applications.

The processing associated with the above will be carried out by law enforcement agencies for the purpose of reducing the incidence of Cybercrime by providing crime prevention advice to businesses and organisations across the country. The PCA product has not been procured for Police Forces to use on their own IP addresses, websites or web applications, but this does not preclude them from doing so.

The intention is that the Police will provide crime prevention advice to organisations in relation to the vulnerability of their:

a) public IP addresses and
b) websites and web applications.

While providing the crime prevention advice the Police will offer the organisation the option to take up free of charge, the use of either or both of the Police Cyber Alarm Vulnerability Scanner elements. The organisations who choose to take up use of PCA are referred to as 'Member Organisations'.

The above two elements of PCA have been subject to another DPIA Stage 1. In their case, the assessment resulted in the decision that a Stage 2 or 'full' DPIA was not required.

[1] Cyber Enabled Crime is defended as "offences that can only be committed using information communications technology, where the devices are both the tool for committing the crime and the target of the crime " National Cyber Security Strategy 2016-2021, Her Majesty's Government,

Police Cyber Alarm Network Traffic Analyser, the subject of this DPIA, is a third element of the PCA product. This element will also be marketed to organisations and can be taken up with or without use of the PCA Vulnerability Scanner.

The Police Cyber Alarm Network Traffic Analyser offers the ability to collect and analyse Suspicious Firewall Activity (SFA). **S31** and allow for a better understanding of the threats the UK infrastructure faces on a daily basis. The potential benefits will only be realised if Member Organisations are willing to take part for the 'greater good' of all although they may benefit too.

The Police can only provide the Police Cyber Alarm Network Traffic Analyser service if the Member Organisation installs a node, which they can uninstall at any time and as a result opt out of the service.

Therefore, the Member Organisations are able to take up whichever of the three PCA elements they wish to use. All three elements are offered by the Police, without cost, to the Member Organisations. The Police have procured and paid Pervade Software Limited for the use of Police Cyber Alarm.

Network Traffic Analyser (NTA) – The collection of the SFA will work by the Member Organisations installing a software node onto their internet facing firewall device. The node continuously collects and shares the log files that are denied access and/or could be 'suspicious activity data', i.e. traffic emanating from an IP address which is subsequently denied access within a specific period of time (not data from known internal traffic) via a secure uni-directional VPN tunnel with the central processing server. 'Suspicious activity data' is any activity highlighted by the Pervade Police Cyber Alarm - Network Traffic Analyser system as potentially being an attack or part of an attack. The rules currently established to determine this are (1) the traffic is external; and either (2a) the traffic was itself rejected by the Member Organisation's firewall; or, (2b) the source IP address of permitted traffic has been the source of rejected traffic in the last hour. No packet (message) content is captured or shared with the central processing server. Only the IP header of the 'Suspicious activity data' is captured or shared with the Police via the central processing server. SFA is analysed and any false positive data will be identified and destroyed, usually in under a week (see attached retention schedule). Confirmed SFA data will be retained for 9 months and then destroyed, unless it is identified as being correlated to further suspicious activity in which case it will be retained until 9 months after the last correlating event. The central processing server has been procured by the Police from Pervade.

The Data will be encrypted by Pervade Police Cyber Alarm to 256-bit AES before being transmitted from the collector to the servers.

The combined crowd sourced data collected from all the Member Organisations making use of the PCA NTA tool will then be analysed in real time to highlight any useful intelligence from either a single or multiple organisations, identifying cyber-attacks and cybercrime trends. The Member Organisation can be sent automatically generated reports from PCA alerting them to attacks they have had should they wish.

The PCA - NTA has a number of built in analytical functions to enable exploitation of the data received from Member Organisations either at a Force, Regional or National level. Although useful on its own, the Police need the capability to enrich this data with other closed and open source data sets to allow for its full value to be gained. **S31**

PCA - NTA is scalable with full access controls allowing each Force/Region to control its own data supplied by the Member Organisations they have signed up. In the right circumstances all the collected data stored in the national server can be searched. Any data captured will be able to provide its provenance and chain of custody.

Management of the system once set up will be via the Regional and Force Cybercrime Units utilising their PROTECT and PURSUE teams.

As the number of Member Organisations using Police Cyber Alarm - Network Traffic Analyser (PCA – NTA) increases, the clearer the potential UK cyber risk and threat will become. The aggregated collected data when data matched will allow Policing to proactively target and investigate and identify potential suspects. As actors and methods are discovered, they can be responded to, to mitigate the threat and risk, for the benefit of the PCA users and the wider public.

Personal data will be collected by the Police and used for law enforcement purposes in keeping with the Data Protection Act 2018. Both a DPIA Stage 1 and 2 have been completed for the PCA – NTA element.

The purpose of the processing is to reduce the incidence of cybercrime to protect the public from harm. This proactive approach will also reduce demand for reactive Policing to investigate crimes that have already been committed. This will be accomplished by the PCA - NTA crime prevention tool capturing log files that are deemed to be suspicious by the Member Organisations' Firewall. This data can then be aggregated and data matched against other data sets, to verify and investigate 'suspect' cyber activity, so the risk and

threat to the Member Organisations and the wider public can be ascertained and mitigated. This will be done by identifying and apprehending suspects, reducing crime and advising organisations on the latest threats and how to protect themselves reducing the incidence of crime.

The Police employee and Member Organisations' personal data that the Police will process for this purpose is minimal and considered to be necessary and proportionate to the purpose. In the main the data processed will concern the Member Organisations' contact details (see 2.2), without which the vulnerability scanning and the provision of their vulnerability reports could not be provided to them. In addition, the PCA – NTA covered in this DPIA, will collect the 'IP address of the originating sender' and the 'Packet Header Information' of the SFA traffic, but not its content.

PCA was initially piloted in 4 regions (EMSOU, S/Wales, N/West, N/East and BTP). This was expanded in August 2020 to cover all forces in England and Wales along with Police Scotland and PSNI. Diagram 1 details the initial server set up per region.

Pervade will sub-contract the hosting solution to Police-Approved Secure Facilities (PASF) assessed / ISO 27001 providers, that is **S31 &S43**.
All of the Servers shown in Diagram 1 **S31 &S43** site. Confirmation of PASF & 27001 accreditation for **S31 &S43** was delayed due to COVID but is now hoped to be completed by the end of April 2021.

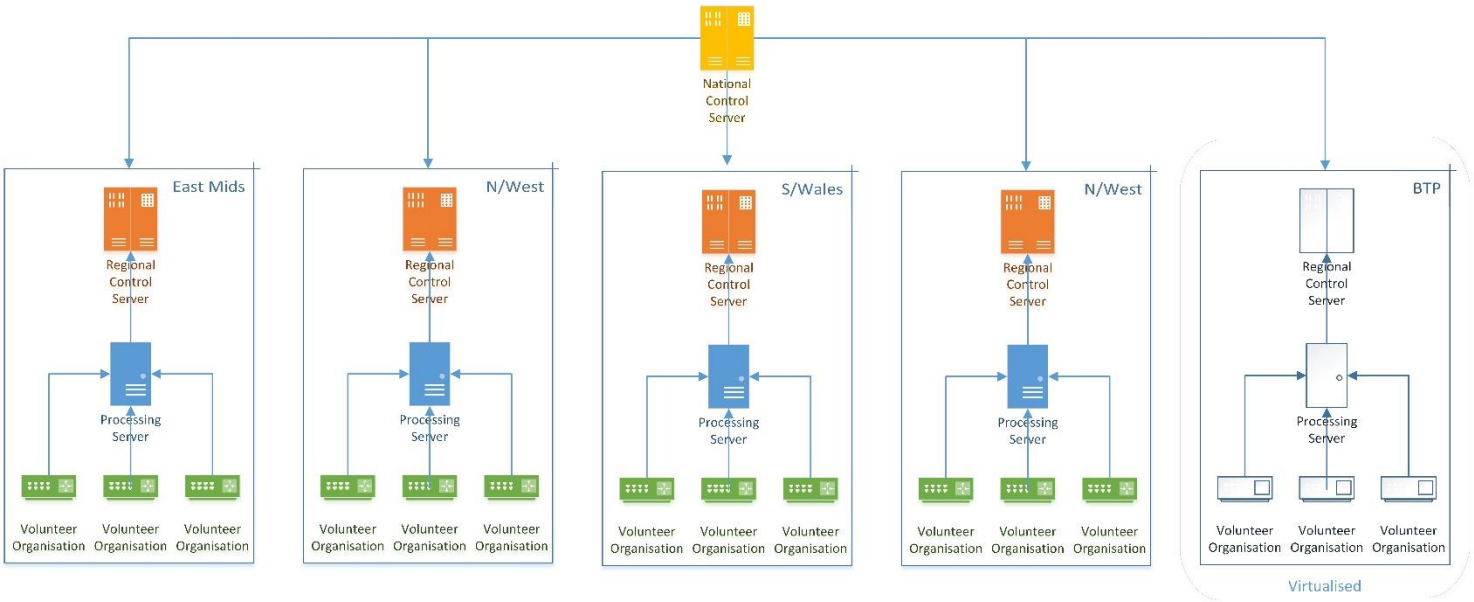

Diagram 1. Initial server set up per Region

2.2 What categories of personal data will be processed? Provide an overview of the

categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, Usernames, e-mail addresses.

Member Organisation's personal data (Node)

The Member Organisations' nodes will be sending network traffic data back to the central server. This will include packet information *but not content.* The following data has been identified as being collected as part of the Network Traffic Analyser:

- Member Organisation's Name
- Member Organisation's email addresses
- Member Organisation's Address
- Member Organisation's IP addresses

'Suspicious activity data' personal data collected from the Member Organisation's (Node)

- IP address of the originating sender
- Packet Header Information

Not all 'Suspicious activity data' personal data will be sent by/relate to people later found to be suspects. The PCA – NTA uses an algorithm of the 'supervised' machine learning type to verify the 'suspicious activity data' personal data that may have been sent by a suspect. Human corrections are learnt by the algorithm and used for future processing. There is human involvement in this decision making. This allows irrelevant data to be promptly destroyed and the accuracy of the system to be continuously improved.

Police employee personal data

Police access to PCA will be ****S31 & S43****. The name, role, unit and Force of the Police employee will also be processed and recorded for security, audit and logging purposes.

2.3 Will special category data be used in the proposal? (Select all that apply)

☐ Race	☐ Trade union membership
☐ Ethnic origin	☐ Genetic Data
☐ Political opinions	☐ Biometric Data
☐ Sex life	☐ Sexual orientation
☐ Religion	☐ Health
☐ Philosophical beliefs	☒ None

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in Derbyshire Constabulary's possession, from a partner agency.

To use the PCA – NTA, the Controller Member Organisation will ask the Police (Processor) to enter into a Data Sharing Agreement, which will cover the provision of the Member Organisation's personal data listed at 2.2 and limit the Police use of that data to the purpose for which it has been provided. In the case of the 'IP address of the originating sender' and

the 'Packet Header Information', once received by the Police that data will become Police personal data and be used for law enforcement purposes.

Network Traffic Analyser - The collection of the SFA will work by the Member Organisations installing a software node onto their internet facing firewall device (the public side). The node will collect and share the SFA log files via a secure uni-directional VPN tunnel with the central processing server. No packet (message) content is captured or shared with the central processing server.

The Member Organisation's personal data requiring processing is:

- Member Organisation's Name
- Member Organisation's email addresses
- Member Organisation's Address
- Member Organisation's IP addresses
- IP address of the originating sender
- Packet Header Information

Of the items being processed, the last two are those distinct to the PCA-NTA and additional to the PCA Vulnerability Scanner processing. These two items will be collected by the Police from the Member Organisations and not the data subjects.

Police employees will supply sufficient personal data so their use of Police Cyber Alarm can be appropriately managed (see above).

2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

The data will be stored on **S31 &S43**.
This will be done in near real time to highlight any useful intelligence from either single or multiple organisations, both in respect of Member Organisations and 'suspects', to identify cyber-attacks and crime trends. This will provide a strategic overview of current attack trends at a National, Regional and Local Level.

The data may be shared across UK Policing and with other law enforcement agencies through existing sharing protocols, where it is lawful, fair, necessary and proportionate to do so.

The Police employees' personal data will be used to manage their use of Police Cyber Alarm.

The data will be stored by Pervade using sub-processors, namely **S31 &S43**.(See 2.9.4 below.)

2.6 How many individuals will the processing affect? (Please specify one answer below)

☐ Fewer than 100 data subjects
☐ 100 to 1000 data subjects
☐ 1000 to 5000 data subjects
☒ More than 5000 data subjects (this includes Police employees, the Member Organisations using PCA - NTA and the IP address of the Senders of SFA)

2.7 What categories of data subject are involved? (Please select all applicable categories below)

☒ Persons suspected of having committed or being about to commit a criminal offence
☐ Persons convicted of a criminal offence
☒ Persons who are or may be victims of a criminal offence
☐ Witnesses or other persons with information about offences
☐ Children or vulnerable individuals
☒ Derbyshire Constabulary staff (current and former)
☒ Other

If other then please provide further details below:
UK Police Forces and Regional Organised Crime Units as part of the NPCC Cybercrime Programme.

2.8 Will it involve the collection of new information about individuals? Will Derbyshire Constabulary collect data that it has not previously collected or had access to?

☒ Yes The Member Organisation's Node Data listed at 2.2 including the IP address of the Senders of SFA.
☐ No

2.9 Data Sharing Does the processing involve:		**Select one option**
2.9.1	Data being shared with third parties external to Derbyshire Constabulary or recipients that have not previously had routine access to the information?	☒ Yes – The data sets will be pooled to form a national data set which other Forces and Regions will be able to access. ☐ No
2.9.2	Transferring data outside the UK but within the EU?	☐ Yes ☒ No
2.9.3	Transferring data outside the EU?	☐ Yes ☒ No
2.9.4	Storing data using a cloud service provider?	☒ Yes **S31 &S43**. The data is backed up on **S31 &S43**.

		This data centre has ISO27001 (BM TRADA), ISO9001 (BM TRADA) and PCI-DSS (PCISSC Pending) accreditation. The servers **S31 &S43**are provided and managed by **S31 &S43** have no access to the data. ☐ No
2.9.5	Is there an MoU, contract, or other sharing agreement in place with all parties with whom data will be shared?	☒ Yes – agreements in place Between the Police and Pervade within **S31 &S43** physical infrastructure, and between the Police and Member Organisations ☐ No – none required

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?
For example, can the aim be achieved by using less data or different types of data? Are all categories of data necessary to achieve the aim?

The Member Organisations' personal data (i.e. data relating to their representatives) will allow for their identification, should they be subject to criminal activity or be assessed as vulnerable and the Police need to contact them. Either the individual or the organisation will have consented to the processing of this data, and as a consequence of the agreement in place between LE and the VO's, will be required to be 'visible' processing through the use by the VO of appropriate fair processing/transparency notices.

In the case of the Senders of SFA, who may be engaged in criminal activity, it is not appropriate to advise them directly of Police tactics or interest. Their personal data is to be collected for law enforcement purposes with the intention of disrupting any criminal activity. Again, this processing of personal data is required to be reflected by Member Organisation's in their fair processing/transparency notices. It would not be possible or appropriate to collect data with the consent of data subjects and therefore the lawful basis for processing is that the collection and amalgamation of communications data is necessary for law enforcement purposes, and in particular to identify both attempted and successful cyber-attacks, not only against individual member organisations but also at a regional and national level to identify prolific offenders and systemic threats. This legitimate objective could not be achieved by alternate means.

The Police employee's personal data will allow for Officers to securely access the system in an auditable way.

2.11 Explain how the use of personal data is proportionate to the aim of the proposal. Weigh the advantages of achieving your purpose against disadvantages to data subjects.

The Member Organisations need to be identifiable, to allow identification of those who are

vulnerable or susceptible to any criminal activity.
The use of Police employee personal data is proportionate as there is no other practical way of providing them secure auditable access of the PCA – NTA.

The disadvantages are minimal to the Voluntary Organisations and the Police employees due to the type of personal data being stored by the Police.

Senders of SFA, who may be engaged in criminal activity, are at risk of investigation and prosecution, which is proportionate where evidence indicates that offences may be being or have been committed. The communications data collected by member organisations is, as detailed above, required to be notified to users of the relevant member organisation's system together with notification that the data will be transferred to law enforcement entities. The Police CyberAlarm system has itself been publicised by law enforcement, with a media launch and a system website providing further details of its operation, with appropriate information as to its use being made publicly available to those who might be affected by its operation (see: https://cyberalarm.police.uk/cyber-alarm-tool-privacy-policy/). This is more proportionate than the alternative option of seeking to impose a requirement to disclose data against those organisations or against ISPs, which would result in a wider collection of data and would be less visible to data subjects. The transfer of personal data from the member organisation to the relevant law enforcement entity in the first instance is governed by a data sharing agreement. A data processing agreement which meets the requirements of Article 28 GDPR, and provides for Pervade to comply with data protection legislation, ISO 27001 and the Information Community Security Policy for policing, inter alia, as well as allowing for audits of its processing activities by or on behalf of the data controllers has been entered into.
The collation of high volumes of data, gathered in real time (high velocity) and from a range of member organisations (high variety) render Project Pascal a 'big data' project. As at February 2021, the indicative volume of data gathered from just one member is 800k suspicious events per month from over 180 different countries and 45k unique source IP address[2].
The Police CyberAlarm Network Traffic Analyser software involves the deployment of supervised algorithms (i) identifying what constitutes suspicious activity data from the rejected traffic data supplied by member organisations and, (ii) analysing the suspicious activity data to identify correlations and priority incidents for investigation according to their potential harm and the available data.
As detailed above, the identification of suspicious activity data at the collector level is set to determine that (1) the traffic is external; and, either (2a) the traffic was itself rejected by the Member Organisation's firewall, or (2b) the source IP address of permitted traffic has been the source of rejected traffic in the last hour. Log data is collected every 30 seconds. Data can be collected, transmitted and analysed within 90 seconds of the event happening if there are no comms issues. Other data from traffic logs is deleted and not transferred from the collector to the PCA servers. The collector level filters can be modified on a per-member basis if required.
When data is transferred to the PCA servers, it is then subject to correlation. ****S31**.**

[2] Taken from a Typical Members Threat Report Feb 2021

If the rejected traffic data does not correlate with a known attack or meet the relevant traffic volume thresholds, the data will be deleted from the processing servers.
Having verified that the data constitutes suspicious activity, the data is further analysed initially ****S31**.**

Having done so, the data is assessed to identify a harm score, in relation to the potential impact of the attack, and the resolvability of the potential criminal activity. The harm score is set between 1 and 5 with 5 being the most severe according to the nature of the attack. The resolvability score is determined by reference to a series of criteria,

****S31**.**

This assists the relevant law enforcement entity to identify attacks for further investigation, but no action automatically arises as a consequence of this analysis.
While the latter has the potential to result in an adverse impact to individuals as a consequence of the prospect of enforcement action being taken against them, human intervention is always deployed prior to any action being taken in relation to an individual and therefore this does not involve purely automated individual decision making. The risk of bias being introduced as a consequence of data only being obtained from certain types/sizes/locations etc of organisation, and the validity of predictions in relation to the identification of priority incidents for investigation will be the subject of ongoing analysis and review throughout the trial period and at it conclusion to ensure algorithmic accountability. It is not anticipated that any bias may exist or will be introduced based on protected characteristics, but this will similarly be kept under review.
While there is a lack of a universal, audited evidence base in relation to the scale and cost of cyber crime in the UK, in 2018 the insurer Hiscox estimated that small businesses in the UK are the target of an estimated 65,000 attempted cyber attacks every day, with over 4,500 of those being successful and resulting in a cyber breach. Data breaches cost UK enterprises an average of $3.88 million per breach, according to IBM and Ponemon's Cost of a Data Breach study, with the average cost of remediation alone to UK enterprises amounting to $840,000. The National Cyber Security Strategy sets out the importance for the national security of the UK of understanding and effectively responding to the scale and nature of the cyber threat. If and to the extent that the gathering of data, and its subsequent analysis and possible retention, constitutes an interference with the Article 8 rights of individuals, the importance of the objective of the protection of UK cyber security, and its consequent impact on protecting the Article 8 and data protection rights of the public, is considered to be of sufficient importance to justify any such interference. When balanced against the actual and anticipated benefits to the community of the deployment of the technology, the limited interference with privacy is clearly justified for law enforcement purposes, and is necessary in order to achieve those legitimate aims since the objective could not be achieved by alternate means. The potential intrusion on the privacy of individuals is, in the majority of cases, plainly proportionate where suspicious activity data is collected relating to those individuals for the purpose of law enforcement.

Section 3 – Lawful Basis[3]
3.1 Lawful Basis To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.
Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes by Police): Necessary for a law enforcement purpose Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes: Necessary for the performance of a task carried out in the public interest or in the exercise of official authority
3.2 Further Special Category Lawful Basis If processing special category data (section 2.3) you must have identified a further lawful condition – Not applicable
Operational Data: The processing is strictly necessary (please tick to confirm) ☐ **AND** One of the following conditions applies (select from the list):
Administrative Data It is necessary for one of the following conditions (select from the list): **OR** It is in the substantial public interest (tick to confirm) ☒ **AND** for the following purpose:
Section 4 – Review, Retention and Disposal
4.1 Does the proposal have a review, retention and disposal process that complies with Derbyshire Constabulary Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within Derbyshire Constabulary's Review, Retention and Disposal Policy.
☒ Yes ☐ No

[3] See Annex for further information

Network Traffic Data

Information Activity / Task	Description / Example of Record	Retention (Minimum Period)	Rationale	Scope Notes	Comments
Volunteer Organisation/representative's personal data (Node)	Volunteer Organisation's Name, email addresses, Address, IP addresses and Website URL (For Web App scanning only)	For the life of the processing	The PCA vulnerability scanner will be scanning the external IP addresses of the Volunteer Organisation. To do this the system needs to know the IP range and details of the Volunteer Organisation	NPCC Cybercrime Programme	
Police employee personal data	Username, a .pnn email address. The name, role, Unit and Force of the Police 'staff'	For the period required for audit purposes around appropriate use of the system.	Police access to PCA will be via a web portal accessed using a Username, a .pnn email address. The name, role, Unit and Force of the Police 'staff' will also be processed and recorded for security, audit and logging purposes.	NPCC Cybercrime Programme	
Police Cyber Alarm – Volunteer Organisation log files	Suspicious Firewall Activity at collector level – following review deemed not to be suspicious	Until identified as not suspicious – typically around one hour	If traffic is rejected from an IP address which has previously had traffic permitted within the previous hour, all the traffic will be identified as suspicious activity data and transferred to the PCA servers. All logs which are not identified as	NPCC Cybercrime Programme	

			suspicious activity data after an hour are deleted.		
Police Cyber Alarm – Volunteer Organisation log files	Suspicious Firewall Activity which is transferred to server – following review deemed not to be suspicious	Until identified as not suspicious – *typically under a week.*	Within the system there is a small chance (under3%) of activity being reported as suspicious which following review is deemed not to be suspicious. Once identified there is no lawful reason to retain this activity.	NPCC Cybercrime Programme	
Police Cyber Alarm – Volunteer Organisation log file	Suspicious Firewall Activity – retained within Police CyberAlarm	9 months	If the log file although deemed as suspicious does not have any further activity within a 9 month period the relevance of the data will be reduced to the point where its retention is no longer considered to be necessary or proportionate.	NPCC Cybercrime Programme	Although initially set at 9 months this time frame will be reviewed to see if this can reduced or needed to be extended
Police Cyber Alarm – Volunteer Organisation log file	Suspicious Firewall Activity – extracted to other Police system	Minimum of 6 years / review as per nominal file	MoPI Groups 1- 4 Any data that is extracted from the PCA system for further work will be imported into other Police systems and as such will fall under MoPI	NPCC Cybercrime Programme	The majority of crime under investigation will be Computer Misuse Act offences which fall under MoPI Group 3

Section 5 – ICO: Additional Factors			
The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.			
Does the processing involve:		**Please check either Yes or No**	**If 'Yes' then please provide further details**
5.1	**Systematic, extensive and large scale profiling and automated decision-making about people?** *"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"* Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an individual, including the analysis or prediction of an individual's performance. Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.	☐ Yes ☒ No	Machine learning is not currently used to categorise, make decisions concerning or otherwise profile individuals or conduct. However, data collected is intended to be used to train a machine learning algorithm to enable it to identify patterns in data and to enable it to develop and apply dynamic rules in future. This is owned by Policing. The algorithm being used is of the 'supervised' machine learning type, where human corrections are learnt by the algorithm and used for future processing. Any positive action or legal process will only be taken following review and enhancement by normal policing involving human review and interaction with the data. Over time as the algorithm becomes more accurate there will be less human involvement. However, if any 'suspicious activity data' was to be investigated further this would be by human involvement.

			When the algorithm identifies false positives the Police, Pervade and the Member Organisation will work together to remove causes of false positives. As the machine learns these will drop.
5.2	**Large scale use of special category data or criminal offence data?** *"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"*	☒ Yes ☐ No	**S31**
5.3	**Public monitoring?** *"Systematic monitoring of a publicly accessible area on a large scale"*	☒ Yes ☐ No	The PCA - NTA will collect details of SFA access requests via the Member Organisations' external IP address range. This is the public facing part of their network. The SFA data collected will include details but will not include any content of any packet (message). The 'Suspicious activity data' access request log files may contain some legitimate traffic, as access to the Member Organisation will depend on how they have set up their firewall. Over time human corrections to the algorithm should improve the identification of 'Suspicious activity data' and reduce the quantity of legitimate data being collected. This log data will be processed by the PCA server to identify cyber-attacks.

5.4	**New technologies or techniques?** *"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"* [For the use of Algorithms, Machine Learning or Artificial Intelligence use the 'AlgoCare - 33 questions' document]	☒ Yes ☐ No	This involves the collection of Member Organisations' SFA in order to identify attacks and enable the analysis of those attacks. This has not been done before by law enforcement on a large scale but is routinely done by the cyber security industry.
5.5	**Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?** *"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"*	☐ Yes ☒ No	Click here to enter text.
5.6	**Biometrics/genetic data?** *"Any processing of biometric data"* ***and/or*** *"any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject"* Biometric data can include Facial Recognition technology, fingerprints and is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.	☐ Yes ☒ No	Click here to enter text.
5.7	**Data matching?** *"Combining, comparing or matching personal data obtained from multiple sources"*	☒ Yes ☐ No	Any third party personal data acquired as a result of 'Suspicious activity' (SFA) would be treated as Police personal data and there will be

			data matching for law enforcement purposes. **S31**
5.8	**Invisible processing?** *"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"* For example, when gathering data, without the knowledge of the data subject, in the course of a Derbyshire Constabulary investigation.	☒ Yes ☐ No	The processing is being carried out for a law enforcement purpose where 'Suspicious activity data' is identified or a crime has already been committed. In these circumstances third party personal data will be processed by the Police without the data subject's knowledge, although steps will be taken to publicise the initiative. The Member Organisations will be able to put a disclaimer on their website publicising the use of PCA via a Privacy Notice. Due to the way that the internet works the majority of subjects accessing the Member Organisations' networks will be unaware of this and it would be impossible to implement a system to make everybody aware of the use of PCA. In an effort to be transparent the Police will offer to the businesses who take up Police Cyber Alarm the following statement to use on their websites - *As part of our cyber security monitoring we share the Metadata of all traffic deemed to be suspicious accessing our*

			network with the Police. As this data is deemed suspicious, it is sent to a software company (Pervade) where the network traffic is collated and analysed. Any data deemed non-suspicious will be removed as soon as it is identified, and will no longer be processed. *This Metadata relating to the network traffic does not contain any information relating to the contents of the traffic, merely the destination, originating IP address and the 'packet header' of the request. As you may be aware, under the General Data Protection Regulation and Data Protection Act 2018, an IP address is considered to be personal data.* *In order to comply with a subject access request and be able to advise you as to whether your data has been shared and with whom, we will need you to share with us the IP address used to access our network and the date time including time zone of the access. If you have a dynamically allocated IP address, as is likely for home users, we would need to know the IP address(es) allocated to you for the period you are enquiring about. This information may be obtained*

			from your Internet Service Provider.
5.9	**Tracking?** *"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"*	☒ Yes ☐ No	Any suspect identified will be via their IP address.
5.10	**Targeting of children or other vulnerable individuals?** *"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children* For example, the use of personal data relating to children for the purposes of marketing their online safety products.	☐ Yes ☒ No	Children and other vulnerable individuals, such as neurodiverse individuals, will not be targeted but it is unavoidable that they may be the sender of SFA, which will not be known without further investigation after the SFA is collected. The risk is low.
5.11	**Risk of physical harm?** *"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals".* For example, if data relating to Child Sexual Abuse or Exploitation, Covert Human Intelligence Sources or protected persons data was compromised then it could jeopardise the safety of individuals.	☐ Yes ☒ No	Click here to enter text.
5.12	**Evaluation or scoring?** *"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of Derbyshire Constabulary's recruitment process.*	☐ Yes ☒ No	The processing will not be used to evaluate or score a Police employee's performance at work. Nor to score individuals who are senders of SFA.

5.13	**Data processed on a large scale.** *Considerations include:* • *The number of data subjects concerned* • *Volume of data and/or range of data items* • *Duration, or permanence, of the data processing* • *Geographical extent of data processing*	☒ Yes ☐ No	The intention is to roll out the offer of the use of the PCA - NTA crime prevention tool across the country, which could be taken up by a large number of Member Organisations. This will allow the large-scale collection of SFA Senders' IP addresses. In February 2021, the data from one member organisation resulted in the reporting of over 811,000 events emanating from 185 different countries and 44,886 unique source IP addresses.
5.14	**Preventing data subjects from exercising a right?** *The rights are:* • *The right to be informed* • *The right to access data* • *The right to rectification* • *The right to erasure* • *The right to restrict processing* • *The right to object* • *The right to portability* • *Rights relating to automated processing*	☐ Yes ☒ No	The Member Organisations and Police employees using the PCA – NTA crime prevention tool will be made aware of how their data will be used and retained. Any SFA will require further manual investigation to identify a suspect. If they are involved in this type of activity they will already be aware that their activity will be captured by any firewall and logged. Data subjects who become suspects may be prevented from exercising some of these rights. The initiative will be publicised by law enforcement entities and in addition, the Member Organisations will be required to ensure that their own privacy policies/fair processing notices make clear that they may transfer data to law enforcement entities and

			are to be offered to the businesses who take up Police Cyber Alarm to use on their websites - *As part of our cyber security monitoring we share the Metadata of all traffic deemed to be suspicious accessing our network with the Police. As this data is deemed suspicious, it is sent to a software company (Pervade) where the network traffic is collated and analysed. Any data deemed non-suspicious will be removed as soon as it is identified, and will no longer be processed.* *This Metadata relating to the network traffic does not contain any information relating to the contents of the traffic, merely the destination, originating IP address and the 'packet header' of the request. As you may be aware, under the General Data Protection Regulation and Data Protection Act 2018, an IP address is considered to be personal data.* *In order to comply with a subject access request and be able to advise you as to whether your data has been shared and with whom, we will need you to share with us the IP address used to access our network and the date time including time zone of the*

			access. If you have a dynamically allocated IP address, as is likely for home users, we would need to know the IP address(es) allocated to you for the period you are enquiring about. This information may be obtained from your Internet Service Provider. Arrangements need to be made for all parties to engage with each other if any of them receive a Subject Access Request, before responding to the Data Subject. For any requests received by the Voluntary Organisation or Pervade they should immediately inform the Police who will liaise with the other party before returning to the recipient of the request to agree any response to the Data Subject. For ease of data subjects, the NPCC may tale a co-ordinating role. This is to ensure a Police investigation is not jeopardised and Data Subject Access requests are dealt with appropriately.

Please forward the completed form to Data Protection,
DPROT@Derbyshire.PNN.Police.UK

ANNEX
SECTION 3 – Lawful basis

S42