Data Protection Impact Assessment (DPIA) – Stage 2

In this stage of the DPIA process you must provide full details about the lifecycle of the data and the risks associated with the proposal. The information you provide will supplement the information provided in Stage 1.

The aim of this process is to identify and mitigate risks. If any **residual risks** to individuals are **high** then the ICO must be consulted before processing commences.

Section 6 - Impact

Expanding upon the purpose outlined in Section 2.1, please detail the intended effect of the processing on: Derbyshire Constabulary; the data subjects; and society/the general public

Describe the benefits and disadvantages to each of the above.

Derbyshire Constabulary *(or another Police Force or Unit using the PCA – NTA)*

The effect on the Police is to allow this data to be used in the prevention and detection of crime and the apprehension and prosecution of offenders. The data will enhance the intelligence picture around the criminals involved in criminal activity online and provide a picture of the Organisations who have been or are subject to criminal activity. Minimal personal data of Derbyshire Constabulary employees will be processed to enable them to access the Police Cyber Alarm Data Lake.

Data Subjects

Minimal personal data will be obtained from Member Organisations and their representatives to carry out the analysis of their Suspicious Firewall Activity (SFA) and enable the Police to communicate with them.

Police Cyber Alarm 'acts as a CCTV camera recording information about traffic seen by an Organisation's firewall, known as 'Metadata', such as where it came from, where it is going and what it is trying to do.

Cyber Alarm collects the log messages produced by internet facing devices such as firewalls, web servers and IDS/IPS. These messages **do not contain any of an Organisation's content data**. They are simply logs about how data was sent/received through an internet gateway. The metadata collected is not limited to rejected traffic, but at the collector stage does include metadata pertaining to traffic which emanated within **S31** from the same IP address as traffic which is subsequently rejected. Traffic identified as suspicious is transferred to the servers whereas other data is deleted.

By an organisation contributing to Cyber Alarm **the Police will not have view of the data being sent/received by the organisation through the Internet**, only information about the data being processed such as IP Addresses for external connections, amount of data transferred, and the port used to process the data.

The data subjects that the Police are interested in are only those engaged in illegal activity. However, the Police Cyber Alarm algorithm needs to be 'supervised' to machine learn to more accurately sift the suspicious activity data from legitimate data. Initially the Data

Server is likely to acquire some personal data the Police are not interested in. As at launch, this was minimal (c.3% and is likely to reduce further in time). The IP addresses used by some law-abiding citizens and Organisations will be captured at the collector stage and even transferred to the PCA servers. This is a disadvantage for those concerned, which is to be considered against the benefit of being able to attack criminality and mitigate the threat and risk that it poses. Safeguards are in place to ensure that such data is identified and promptly deleted, and these are kept under review to ensure their effectiveness.

Criminals leave a trail of limited personal data online during the course of their criminal activity such as their IP addresses. The use of the Police Cyber Alarm system will allow for this personal data to be collected and used in the identification of criminals 'attacking' an organisation's firewall.

General Public

As the use of technology, the internet, cyber enabled and cyber dependent crime[1] grow, there is an expectation that the Police will use all available lawful tools and techniques to protect the public and apprehend offenders.

The impact on the general public will be a positive one in that it will reduce the number of victims of crime. For example, Organisations (not only Member Organisations, but all organisations through the intelligence gleaned which can be used to inform the wider public) will become better informed and able to mitigate risk and threats and suspects will be identified and investigated. This needs to be weighed against the collection of all traffic data at collector level to identify SFA, and the collection and transfer of any IP addresses associated with SFA which was actually legitimate business traffic. This could result in some legitimate customers' IP addresses being added to the Police CyberAlarm Data Servers for the Police to analyse and data match. This is expected to impact a very small number of the total, but will be monitored, and the businesses will be engaged and involved to minimise this. This is possible because the data collected and stored in the 'Pervade' Data Lake remains attributable to the source Force and Member Organisation who can be identified.

The legitimate traffic collected and transferred to the servers as at launch is estimated to form three percent[2] of the SFA collected, which is considered to be proportionate in the context. The benefits outweigh the costs of the collateral intrusion. Static rules will be updated as necessary to minimise the legitimate traffic erroneously transferred to the PCA servers. In due course, once operational the supervised algorithm will be constantly learning and improving which will be demonstrated by the percentage of false positives being further reduced. If necessary the reduction will also be achieved by Pervade and the Police providing feedback to Member Organisations about how their Firewall has been set up where this is causing legitimate traffic to become SFA.

[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,

[2] Following initial review and research by Pervade

The identification of any false positives occurs in two locations:
Within the Member organisation's data collector – this rule based filtering operates initially on 2 simple rules:

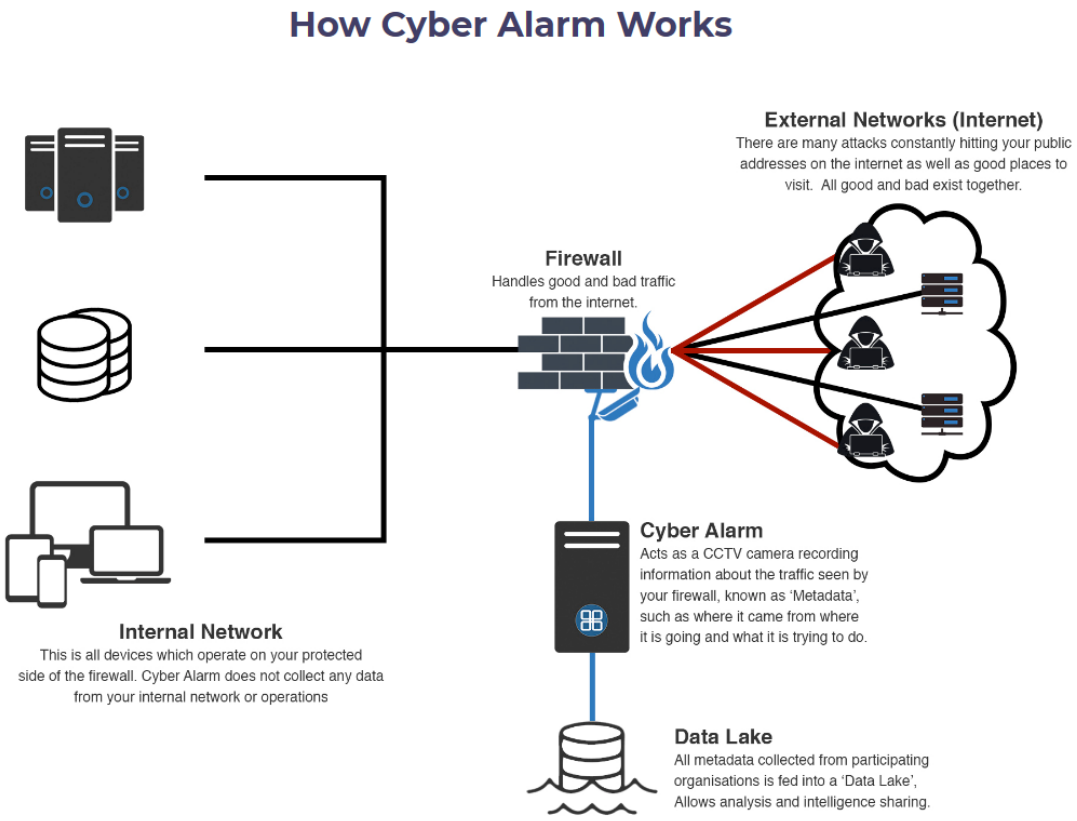
1. *If the traffic originates from inside the network, it is dropped;*
2. *If the traffic is allowed by the firewall, the system will check if the source IP address of the data has had any traffic denied* **S31** *if not then the traffic will be dropped.*

If the SFA is not filtered out, the data is sent to the central servers and reviewed against the correlation engine's static rules to determine if the SFA formed part of an attack and what type of attack occurred. If the traffic is deemed to not be attack traffic it is deleted in line with the Review, Retention and Disposal Policy, usually within a week if not sooner.
The rules used on the Member Organisation's data collectors can be reviewed and adjusted by the central server and then pushed down to all the Data Collectors at the Member Organisations, and the data is checked against the rules as frequently as every minute.

Section 7 - Information Lifecycle

7.1 Diagrams and Tables

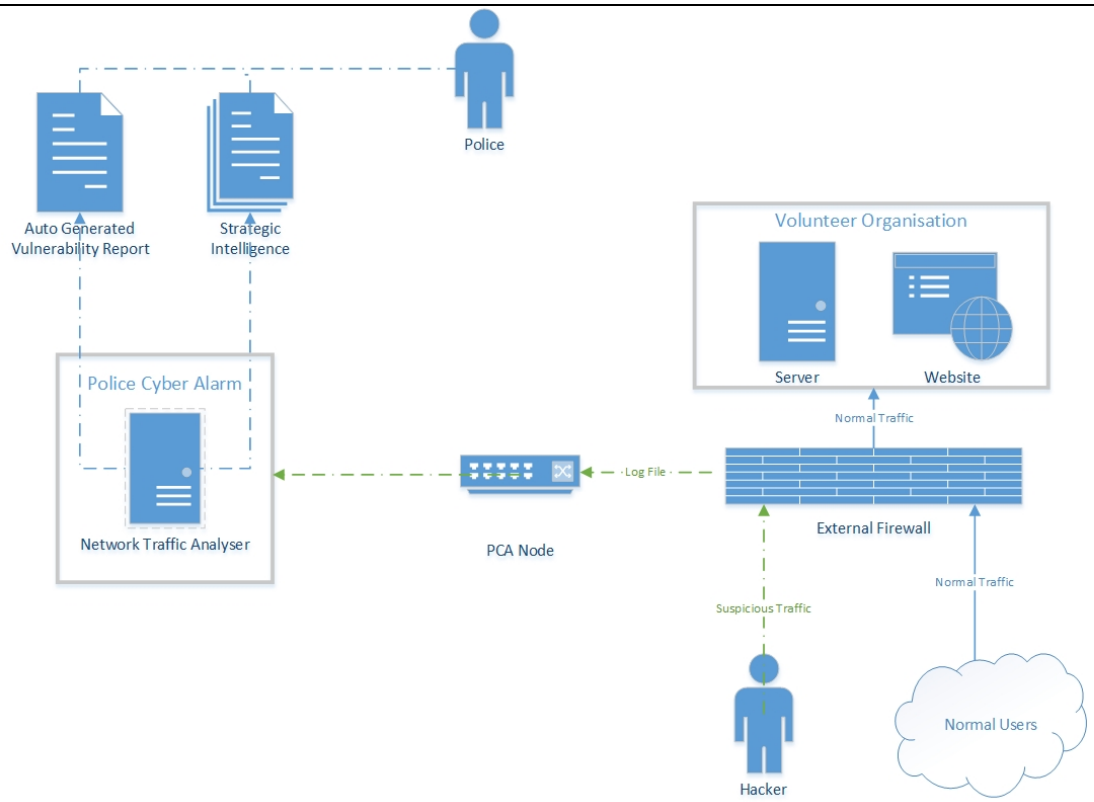
Please insert a diagram or table that demonstrates the flow of data within this proposal. You should reflect the information lifecycle.



S31 & S43

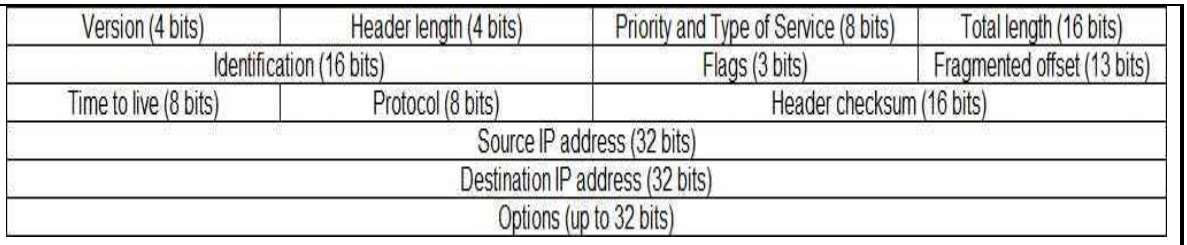
Phase 1 rollout infrastructure

Network Traffic Analyser



7.2 Provide a full description of the information lifecycle	
Stage of Processing	**Description**
Collection Where does the data originate from, who will you collect it, how will the data be obtained and how often?	There are two options available for the installation of Police Cyber Alarm by an organisation: • VMWare Virtual Appliance - simply copy and paste the provided URL into VMWare's management console. • As a software installation on a Linux device - requires CentOS 7 Minimal on either a physical or virtual device. Police CyberAlarm continuously (approximately every 30 seconds) collects the log messages produced by internet facing devices such as firewalls, web servers and Intrusion Detection Systems. These are simply logs about how data was sent/received through the organisation's internet gateway. By contributing to Police Cyber Alarm **the Police will not have view of the data being sent/received by the organisation through the Internet**, only information about the data being processed such as IP

	Addresses for external connections, amount of data transferred and the port used to process the data. The log messages from an organisation's internet facing devices are not natively encrypted. In order to ensure security, the Police Cyber Alarm system installs a small collector on the organisation's network. Typically this would be installed within the Demilitarised Zone (DMZ), and gathers the data that the Member Organisation would like to share with the Police, encrypts it and compresses it before securely transmitting the data to the central Police CyberAlarm processing servers. The data is continuously collected and processed in near real-time until the Member Organisation uninstalls the collector. *Definitions* • Member Organisation – Organisations that have agreed to have the PCA system installed on their network. This may be for one or all three of the capabilities. Each will have to agree to the terms and condition of installation before the systems is deployed and be responsible for the installation of the node. • Node - a small piece of software installed within the Member Organisation's network which is able to process the suspicious firewall logs and if appropriate encrypt and send to the central PCA system for further analysis via the uni-directional VPN tunnel. • Log file – a small file recording activity with the file wall, this can be benign and suspicious. Only suspicious activity will be captured by the Network Traffic Analyser. • Uni-directional VPN tunnel – an encrypted communication tunnel between the Member Organisation and PCA servers allowing two way communication. • Central processing server – the central PCA server • Suspicious activity – any activity highlighted by the NTA system as potentially being an attack or part of an attack. Any normal type traffic will be ignored by the system. • Packet header information – An IP header is a prefix to an IP packet that contains information about the IP version, length of the packet, source and destination IP addresses, etc. [1]An **IP header** is a prefix to an IP packet that contains information about the IP version, length of the packet, source and destination IP addresses, etc. It consists of the following fields:

	 Here is a description of each field: **Version** – the version of the IP protocol. For IPv4, this field has a value of 4. **Header length** – the length of the header in 32-bit words. The minimum value is 20 bytes, and the maximum value is 60 bytes. **Priority and Type of Service** – specifies how the datagram should be handled. The first 3 bits are the priority bits. **Total length** – the length of the entire packet (header + data). The minimum length is 20 bytes, and the maximum is 65,535 bytes. **Identification** – used to differentiate fragmented packets from different datagrams. **Flags** – used to control or identify fragments. **Fragmented offset** – used for fragmentation and reassembly if the packet is too large to put in a frame. **Time to live** (TTL) – limits a datagram's lifetime. If the packet doesn't get to its destination before the TTL expires, it is discarded. **Protocol** – defines the protocol used in the data portion of the IP datagram. For example, TCP is represented by the number 6 and UDP by 17. **Header checksum** – used for error-checking of the header. If a packet arrives at a router and the router calculates a different checksum than the one specified in this field, the packet will be discarded. **Source IP address** – the IP address of the host that sent the packet. **Destination IP address** – the IP address of the host that should receive the packet. **Options** – used for network testing, debugging, security, and more. This field is usually empty. **TCP** – Transmission Control Protocol a set of networking protocols allowing two or more computers to communicate **UDP** – User Datagram Protocol a set of networking protocols allowing two or more computers to communicate [1] https://study-ccna.com/ip-header/
Storage Describe where and how the data is to be stored.	See Processors below.

Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	The data collected by Police Cyber Alarm is viewable only to Police and their authorised partners. Partners include; • **S23** • National Cyber Security Centre (NCSC) • Pervade employees named in the Police Data Processing Contract In addition, when authorised/required to do so by law, partners may make some data available to selected third parties. The processing is being carried out for law enforcement purposes and is subject to the Data Protection Act 2018. This processing involves new technology and the Police will match the data collected against other open and closed source data sets, that is those in the public domain and / or held on Police systems. **S31** The new information / intelligence generated as a result of the data matching will belong to the Police as the Controller and not the Member Organisation who supplied the IP address that has been matched. **S31** Monitoring of the efficacy of the datasets will be undertaken to identify whether additional/alternate datasets would result in greater confidence in the data.
Access Describe who has access to the data throughout the life of the processing.	Access to the data will be via a **S31**. Each group of users (Force / ROCU / **S23**) will have their own silo within the system. All access and searches will be fully auditable by Law Enforcement supervisors with the ability to delete any Police created data from the system (both within Police systems and the server rented by Pervade) in line with current policies and procedures.
Recording Describe the processes for recording the data.	The data will be recorded by Pervade within the secure Pervade Police Cyber Alarm system. The data sent to the Pervade Police Cyber Alarm systems will be securely encrypted to 256-bit AES and compressed.
Processors Describe the use of Processors. If a third party is being used, is a contract in place to regulate the relationship? Will the data be	Pervade are Processors acting on behalf of the Police. Pervade in turn use **S31 & S43** as Sub-processors. All data will be processed within Pervade's dedicated secure servers housed by **S31 & S43** **S31 & S43**

processed outside of the UK or the EU?	This data centre has ISO27001 (BM TRADA), ISO9001 (BM TRADA) and PCI-DSS (PCISSC Pending) accreditation. The servers at **S31 & S43** **S31 & S43** have no access to the data. [Information provided by Pervade: **S31 & S43**
Sharing With which external organisation(s) is the data shared, what data is shared, and why? Describe any sharing that will occur within Derbyshire Constabulary. Outline any national and international sharing or processing.	Member Organisations will be made aware that they are being invited to share their data with UK Policing nationally, because it is the aggregated pooled data that will enable the identification of patterns of behaviour linked to IP addresses. The data collected by Police Cyber Alarm is viewable only to Police and their authorised partners. Partners include: • **S23** • National Cyber Security Centre (NCSC) • Pervade employees named in the Police Data Processing Contract In addition, when authorised/required to do so by law, partners may make some data available to select third parties. The Police will use the data collected to inform local, regional and national statistics about the cyber-attacks that UK Organisations are facing. In the event of a cyber-attack on an organisation the Police may also choose to use the data from Police Cyber Alarm as evidence in court.
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate.	All data retained by the Police will be retained in line with MoPI. The data being processed by Pervade is described in the retention schedule included in the DPIA Part 1.
Disposal	In line with Management of Police Information (MoPI). The Pervade Police

Describe the process for disposal of data, including when and how.	Cyber Alarm platform on the **S31 & S43** Pervade and its Sub-processors are subject to a Data Processing Contract, to ensure all the Police Personal Data is destroyed beyond being retrievable at the end of the contract.
7.3 Assets Describe the assets that you intend to use.	
Hardware	**S31 & S43** Pervade. Desktop / laptop with internet access.
Software	Pervade Police Cyber Alarm web portal via.
Networks	Web access. Collector Node installed on the Organisation's public facing network.
Hardcopy/paper	None.
Any other relevant assets	None, all assets will be maintained and controlled by Pervade with access to Police Cyber Alarm via a web portal.

Section 8 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you should consider consulting them or their representatives.

8.1 Do you intend to consult data subjects?

☐ **Yes**

If yes then outline your plan in **Section 8.2** below together with details of consultation with other stakeholders.

☒ **No** If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 8.2** below.	The Personal Data will come from collecting all the IP addresses sending traffic to Member Organisations, which is then filtered at the collector to identify SFA traffic. It would be impossible and impractical to consult with all the data subjects. There is also a wish to avoid compromising Police protected tactics and operational activity. Any access to the collected personal data will be used for the prevention and detection of crime. Safeguards have been put in place in relation to the processing: a legal opinion has been obtained, this DPIA has been conducted, the initiative will be subject to ongoing monitoring by the programme data protection adviser and the overarching governance process, the existence and operations of the system has been publicised through the Police CyberAlarm website where the tool's privacy policy/fair processing notice is posted, Member Organisations are required under the terms and conditions of use to include relevant information in their

	privacy policies directed to their users, and it is intended that as the project progresses further consultation will be carried out with third party stakeholders.

8.2 Consultation Action Log

Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- The general public
- Union representatives
- Information Security Officer
- The DPS
- Equality unit
- Derbyshire Constabulary' Legal Team
- Ethics Board
- Police and Crime Commissioner (PCC)
- Partner agencies
- Data Processors
- Information Commissioner's Office (ICO)

Who	When	How	Outcome
The DPS	19/11/2019, 17/12/2019, 07/01/2020 & 14/02/2020	Face to face meetings	This DPIA
Information Assurance Officer (**S40** NPIRMT)	21/11/2019	PASF assessment for Pervade**S31 & S43**	PASF assessment for Pervade. **S31 & S43**
Other Police DPOs	14/02/2020	Act as a 'critical friend' for this document	
Pervade		Development of NTA	
Member Organisations		Obtain feedback including any concerns	

Section 9 - Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. **The assessment criteria outlined in italics in section 9.1 applies to all categories** in Section 9 and 10, i.e. for 'likelihood' you must always assess whether it is 'rare, unlikely, possible, likely or almost certain'.

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Examples of **risks to individuals** include**:**	Examples of **corporate risks** include:
• Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights	• Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations

You should identify **solutions** such as:

- Deciding not to collect certain types of data
- Reducing the scope of processing
- Reducing retention periods
- Taking additional technical security measures
- Following approved codes of conduct
- Restricting access to data
- Training staff to understand the risks
- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third-party Processor

9.1 Data Protection Principles

1. Lawfulness, fairness and transparency
- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected, recorded and managed?

2. Purpose Limitation
- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Storage Limitation
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all Derbyshire Constabulary systems if required?
- Is the retention period necessary and proportionate?

6. Integrity and confidentiality
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights
- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to the DPS.

Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**
	1 - Rare *2 - Unlikely* *3 - Possible* *4 - Likely* *5 – Almost Certain*	*1 - Insignificant* *2 - Minor* *3 - Moderate* *4 - Major* *5 - Critical*	*High* *Medium* *Low*	*Describe the mitigation and whether it will be implemented*	*Is the risk:* *- Eliminated* *- Reduced* *- Accepted*	*High* *Medium* *Low*

ICO - Data controllers will need to be able to justify the risks which have been rated as low						
9.1.1 Reduce Reputational risk by demonstrating lawfulness, fairness and transparency.	4	3	Medium	The DPIA Co-ordinator to consider developing and actioning the Consultation Action Log including the creation of an Ethics Board. (See 8.2). This was approved by the Pascal Governance Board and is now in development.	Accepted	Low
9.1.1 There is a risk that the Police process more information than the Member Organisation (VO) has agreed for them to do.	4	3	Medium	The DPIA Co-ordinator to ensure that the Data Processing Contract between the VO and Police reflects the data being provided and the system configuration and any agreed terms are complied with. Governance and auditing of product.	Accepted	Low
9.1.1 The Member Organisations of Police Cyber Alarm may need to create or amend their Privacy Notice to state they will share information with the Police.	3	2	Medium	Advise Member Organisations to consider whether their Privacy Notice needs to be updated. The Police will offer a template additional notice to use. (see 5.8 & 5.14). PCA tool privacy policy posted on PCA website	Reduced	Low

				(https://cyberalarm.police.uk/cyber-alarm-tool-privacy-policy/). Consider including a Privacy Notice within the PCA – NTA system.		
9.1.1 It is intended the Member Organisations will be the Controller of Data which they transfer to the PCA for collection, analysis and transfer. The DPC will need to describe how it is terminated. Personal data that the Police receive and subsequently develop for law enforcement purposes will become Police personal data which will be retained in accordance with MoPI, even if the DPC has been terminated. This could be a Risk to Police Cyber UK reputation.	3	4	High	The IAO needs to ensure the terms of the DPC are complied with to avoid the Police using the personal data beyond what the Member Organisation authorised.	Reduced	Low
9.1.1 There is a risk that more people than necessary can process the Police personal data, including employees of sub processors.	2	2	Low	Contractual provisions limit access to data, and auditing provisions will enable compliance to be checked.	Reduced	Low

				Standard MOPI audits will monitor access to and use of data.		
9.1.1 The SFA will contain some legitimate traffic data particularly immediately after the PCA – NTA software node has been installed by a Member Organisation and on an ongoing basis through the collection of data pertaining to potential port scanning activities. There is a risk of processing innocent people's data which may not be proportionate.	5	2	Medium	Collateral intrusion is anticipated to be minimal in light of the criteria for identifying suspicious activity data, and ongoing monitoring and machine learning improvement to be in place. To be ascertained by determining the percentage of data identified as comprising potential port scanning activities as a proportion of the totality of data collected at collector level, and the percentage of false positives among the SFA at server level. (Pervade in an email dated 23/04/2020 estimates this to be 3%.) Pervade estimates that at initial implementation, SFA data will comprise 3% false positives, but that these will be reduced through amendments to the static rules and, ultimately, the	Accepted	Low

				use of algorithms. Non-suspicious activity data at collector level is deleted within approximately an hour of collection and is not transferred to the PCA servers. False positive data at server level shall be identified, usually within a week, and securely destroyed.		
9.1.1 The SFA will contain some legitimate messages particularly immediately after the PCA – NTA software node has been installed by a Member Organisation and at collector level when the data is initially filtered. There is a risk of processing 'innocent' people's data may not be proportionate.	5	2	Medium	The identification of any false positives occurs in two locations: Within the Member organisation's data collector – this rule based filtering initially on 2 simple rules: 1. If the traffic originates from inside the network, it is dropped. 2. If the traffic is allowed by the firewall, the system will check if the source IP address of the data has had any traffic denied in the	Accepted	Low

				last hour, if not then the traffic will be dropped. If the SFA is not filtered at this point the data is sent to the central servers and reviewed by the correlation engine to determine if the SFA formed part of an attack and what type of attack occurred. If the traffic is deemed to not be attack traffic it is deleted in line with the RRD Policy. The rules used on the Member Organisations' data collectors are reviewed and adjusted by the central server and then pushed down to all the Data Collectors at the VOs as frequently as every minute. The percentage of false positives will be monitored to identify what percentage of false positives remain following the assessment		

				at both node and server (as described above) and to monitor the progress in reducing the percentage of false positives.		
9.1.1 Invisible processing creating a lack of transparency. (see 5.8)	5	2	Medium	In an effort to be transparent the Police will offer to the businesses who take up Police Cyber Alarm a statement to use on their websites – see 5.8. The PCA tool privacy policy has also been posted on the PCA website, and the initiative has been publicised in the media.	Accepted	Low
9.1.1 When SFA contains legitimate message data, the Police will need to facilitate data subject's rights. (see 5.14 and 6)	5	2	Medium	Procedures implemented to destroy beyond being retrievable such personal data as soon as possible from both Police and Pervade's records. (As per the RRD policy at 4.1) Forces responsible for complying with DSARs and other rights requests, as data controllers.	Accepted	Low
9.1.3 There is a risk that the SFA will contain legitimate traffic, which	5	2	Medium	1. At collector level, non-SFA is dropped prior to being	Accepted	Low

will be subject to Police data matching.				transferred to the PCA servers and is therefore never subjected to data matching or other analysis. Data erroneously identified at collector level as potential SFA data is correlated at server level and if not correlated is deleted. Static rules can be revised to further reduce the incidence of legitimate traffic being erroneously identified. 2. In due course, it is intended that the data collected can be used to train an algorithm which will further reduce the risk of processing legitimate data. This will be done by the refinement of the algorithms and its		

				ability to identify the false positives. 3. Once implemented, procedures to be implemented to enable effective reviewing of the supervised machine learning to reduce the incidence of this occurring, including refinement of the algorithms following evaluation of the input and outputs. 4. The algorithm will be evaluated before being deployed.		
9.1.4 Inaccuracies and bias created by the algorithm.	5	2	Medium	Any bias will be minimal and not based on protected characteristics, but rather resulting from nature of Member organisations which sign up. Consideration of impact of Equality Act (Public Sector Equality Duty) has been undertaken. The majority of	Accepted	Low

				traffic we will be collecting will be denied firewall traffic and as such it is traffic that the VO firewall has blocked. We are using the term suspicious firewall activity as we are also collecting traffic that is linked to the DFT. **S31 & S43** 1. As described above the PII being collected is IP which can be classed as bias blind in that it does not link to any personal trait be that gender, ethnicity etc. **S31 & S43** The IAO to ensure constant attention and vigilance is given to the algorithm to ensure the predictive assistance provided is as accurate and unbiased as possible. To include regular		

				scrutinisation of the algorithm by an appropriately formed ethics board.3 Any intelligence from the system will be checked by Police before action is taken and if required any inaccuracy will be fed back into the system to assist in the algorithms learning and reducing false positives.		
9.1.4 ICO: …implement innovative techniques to develop **auditable machine learning algorithms**.	5	2	Medium	1. There is minimal expectation for errors with the SFA this is estimated at this time to be 3%. The majority of internet traffic is for a lawful purpose and is able to navigate the firewalls. Otherwise we would constantly be getting errors when using the internet. If the Member	Accepted	Low

				Organisations have configured their firewall correctly (if they haven't they would get access complaints) the error rate for collection of legitimate traffic which is transferred to the PCA servers will be minimal (approx. 3%). 2. The IAO to ensure internal and external audits will be undertaken with a view to explaining the rationale behind algorithmic decisions and checking for bias, discrimination and errors. This will be an ongoing process as part of the refinement of the system. It is expected as the system is refined the number of false positives is reduced.		

				This will continue to be monitored. But there is no guarantee of this and if the error rate remains at 3% then this is proportionate and acceptable because no action will be taken on the data without human review. Any learning from the audits will be used to refine the system.		
9.1.5 Police Cyber Alarm – Not knowing where each of the Processing Server, Regional Central Server and National Central Server are located? (Stage 1, 2.1 and Stage 2, 7.1)	5	2	Medium	The DPIA Co-Ordinator has confirmed **S31 & S43**	Eliminated	Low
9.1.5 Police Cyber Alarm – Network Traffic Analyser requires a Review, Retention and Disposal policy in keeping with Derbyshire Constabulary policies.	5	2	Medium	The IAO to ensure that a policy is written and implemented including registering the asset with the Derbyshire Force Records Manager **S40** (incorporated above).	Reduced	Low

9.1.5 Police Cyber Alarm – Network Traffic Analyser requires a Review, Retention and Disposal policy that includes 'innocent' personal data.	5	2	Medium	The IAO to ensure that a policy is written and implemented including the destruction of the false positives collected.	Eliminated	Low
9.1.5 'Storage Limitation' There is a risk the Police data will be left in the 'cloud' too long, including beyond the end of the processing or contract with the supplier, in breach of the Data Processing Contract.	5	2	Medium	Contractual provisions in place to prevent such incidents. The IAO to know which third party company is responsible for securely destroying the Police data and ensuring this is done at the time required.	Reduced	Low
9.1.6 There is a risk of not implementing appropriate technical and organisational measures to protect personal data if vetting is not carried out.	3	2	Medium	Contractual obligations require appropriate technical and organisational measures to be imposed by the Processor and any sub-processors. The IAO to ensure that all Pervade staff with access to the PCA system will be vetted to the relevant level. Contractual provisions create auditing rights which will be conducted.	Reduced	Low

9.1.6 There is a risk of not implementing appropriate technical and organisational measures to protect personal data if Confidentiality Agreements are not signed.	3	2	Medium	The DPIA Co-ordinator to ensure that Schedules B & C of the DPC name the Pervade staff with access to the PCA system and ensure they each have signed a Confidentiality Agreement.	Reduced	Low
9.1.6 There is a risk of not implementing appropriate technical and organisational measures to protect personal data if unaccountable 'Members' are used by the Police or Pervade.	3	2	Medium	The DPIA Co-ordinator made the decision that no Members would be used. Police employees are subject to a Misconduct Code. Pervade employees will be subject to the Data Processing Contract including signing a personal Confidentiality Agreement.	Eliminated	Low
9.1.6 *In terms of the web portal that Force users use to access the data, the DPIAs do not appear to touch on the security aspects of the system/web portal such as the list below. Consideration should be given to the development of an Information Risk Asset Register (IRAR) for the project.*	3	2	Medium	Penetration testing has been conducted by independent external specialist providers PRISM Infosec and Arcanum. An onoing programme of testing is underway. • The exact version of the system used by Police, installed in the same data centre	Reduced	Low

• *Penetration testing requirements/results* • *Anti-Virus/Anti – Malware scanning* • *Patching* • *Maintenance* • *Access requirements* • *Roles – view only, edit* • *Audit* • *Define the hosting of the web portal – cloud service provider or hosted by Pervade?*				but running services to a different client, was tested in a pen-test commissioned by NCSC by an approved tester in Q1 2020. In addition, external pen tests have been commissioned and have reported. Anti-Virus/Anti – Malware scanning • The systems are all scanned daily Patching • The systems are patched by the Pervade team, maintaining the most up-to-date stable build that allows the system to function as designed. Maintenance • The system is maintained by the Pervade team and actively monitored by Pervade's own		

				OpView software to audit both configuration and activity. Access requirements All user access **S31 & S43** Roles – view only, edit • All user access is controlled very strictly by Role-Based Access-Control that has very granular settings. Audit • Pervade is Cyber Essentials Plus and IASME Gold certified, both of which requiring on-site audits and both include the Data Centre including the police systems in scope. Define the hosting of the web portal – cloud service provider or hosted by Pervade		

				S31 & S43 everything from the Operating System up is managed by Pervade **S31 & S43** do not have access to it. All data on the servers is encrypted 256bit AES.		
9.1.6 Not having a Technical Risk Assessment.	3	3	Medium	Compliance with a Technical Risk Assessment – completed by an ISSO / ISO. This is being undertaken by NMC.	Reduced	Low
9.1.6 Not complying with our Business Requirements document.	4	2	Medium	The DPIA Co-ordinator to review the Business Requirements document and address any matters arising with Pervade.	Reduced	Low
9.1.6 Using a Cloud environment and not applying the NCSC 14 Cloud Security Principles https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles	3	3	Medium	Contractual provisions in place. The DPIA Co-ordinator to engage an Information Security officer to ensure the NCSC 14 Cloud Security Principles have been complied with. https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles	Reduced	Low

9.1.6 Using a Cloud environment and not applying the ICO cloud computing guidance.	3	3	Medium	Contractual provisions in place. The DPIA Co-ordinator to engage an Information Security officer to ensure the ICO cloud computing guidance have been complied with. **ICO Guidance on use of Cloud Computing – Embedded Doc**	Reduced	Low
9.1.6 Using a Cloud environment and not applying the ICO cloud computing guidance – Get a written contract.	3	3	Medium	Apply the ICO cloud computing guidance – A Data Processing Contract is being entered into to ensure this. **Extract - ICO Guidance on use of Cloud Computing – Embedded Doc**	Reduced	Low
9.1.6 Using a Cloud environment and not applying the ICO cloud computing guidance – Complete the checklist.	3	3	Medium	The DPIA Co-ordinator to ensure the ICO cloud computing guidance checklist has been completed. **ICO Guidance on use of Cloud Computing – Embedded Doc**	Reduced	Low
9.1.6 7.2 'Processors': **S31 & S43** makes the Police data susceptible to a catastrophic natural disaster, infrastructure fault, and internal or external human interference.	1	5	Low	The data at this time forms part of a trial of both PCA and also the intelligence benefit of Network Traffic data in policing. **S31 & S43** Any data being used as part of a criminal	Reduced	Low

				investigation will be extracted and placed on a Police system as per the RRD requirements.		
9.1.6 The DPIA Co-ordinator to consider whether a PASF is **S31 & S43** (See 2.1 & 8.2)	3	2	Low	Implement a PASF when Covid-19 restrictions are lifted or record rationale for not doing so. This is currently being undertaken by NMC.	Accepted	Low
9.1.6 The DPIA Co-ordinator to consider whether a PASF is required **S31 & S43** (See 2.1 & 8.2)	3	2	Low	Implement a PASF when Covid-19 restrictions are lifted or record rationale for not doing so.	Accepted	Low
9.1.6 The DPIA Co-ordinator to ascertain if **S31 & S43** has ISO 27001 Certification. (See 8.2)	3	2	Low	ISO27001 certification in place.	Eliminated	Low
9.1.7 5.14 'The right to access data' not being made available to the owners of the '3%' of personal data collected that was legitimate traffic.	5	2	Medium	This has been addressed in the Voluntary Organisation to Police and the Police to Pervade Data Processing Contracts. The intention is to make this right unnecessary due to the personal data being destroyed as soon as it is recognised to be legitimate	Reduced	Low

				traffic. There is no intention at this time to feedback to the VO the false positive list. They will have access to this type of data from their own firewall logs which will identify Denied Firewall Traffic. The VO organisation will get a summary of the attacks.		
Reputation harm or embarrassment if Pervade suffered a data breach within Police Cyber Alarm for the SIRO, Derbyshire Police and UK Law Enforcement	2	4	High	A Procurement Contract and a Data Processing Contract between Pervade and Police details data protection requirements. These contracts indirectly apply to the third-party server provider, **S31 & S43* Pervade, **S31 & S43** have been checked by an Police Information Assurance Officer, to minimise security risks. (i.e. Police-Approved Secure Facilities (UK) compliant). Their internal security policies and GDPR / DPA compliance will	Reduced	Low

				minimise the risk of a data breach. In addition, external penetration and other information security testing has been and will continue to be conducted by independent external specialist providers.		
Unlawful access to data by Police employee	2	2	Medium	All access to the systems will be **S31 & S43** The Police Cyber Alarm system is fully auditable by Police managers to ensure compliance by staff. All staff will receive appropriate training.	Reduced	Low
Wrongful arrest or prosecution	2	3	Medium	Police Cyber Alarm data will be treated as intelligence only and will require human review and enriching before being acted on or entered as evidence. All data once obtained by the Police will be subject to intelligence assessment and MoPI.	Reduced	Low

9.2 Data Sharing - including the involvement of other Controllers and Processors

- What contracts, MOUs etc are in place or may be required? - What measures have you taken to ensure third parties comply with Data Protection laws?	- What risks are involved with sharing data? - Is sharing necessary and proportionate? - Is the sharing of data being minimised?

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation / Solution	Result	Residual Risk
Not having a Commercial contract with Pervade and indirectly **S31 & S43**	Unlikely	2	Low	Commercial contract in place with suppliers (Procurement contract)	Eliminated	Low
Not having a Data Processing Contract (DPC) with Pervade and indirectly **S31 & S43**	Unlikely	2	Low	Data Processing contract between Pervade and **S31 & S43**and any other sub-contractor in place.	Reduced	Low
NPCC Cybercrime may want to confirm that Pervade have a DPC with **S31 & S43**that cascades all the Police requirements and the latter likewise **S31 & S43**	Unlikely	2	Low	The DPIA Coordinator to confirm that Pervade have a DPC with **S31 & S43**that cascades all the Police requirements and the latter **S31 & S43**	Reduced	Low
Indemnity A figure subject to the Procurement cost is suggested which is considerably less than the **S43(2)** usually stated in the Data Processing Contract.	Unlikely	2	Low	The DPIA Coordinator has decided that the Data Processing Contract (Police - Pervade) should state **S43(2)** **S43(2)**, the usual level of indemnity between Derbyshire Constabulary and a third party. It is recognised that this sum is providing cover for up to 46 Controllers, which is proportionate due to the	Reduced	Low

				low level of risk. The DPIA Coordinator will ensure that Pervade obtain the required level of insurance to provide this level of cover for data protection.		
Indemnity There is a risk of an ICO fine exceeding the indemnity level agreed.	Unlikely	2	Low	The IAO to consider the financial risk that each of the Controllers are exposed to, should a data breach lead to an ICO fine exceeding the level of the agreed indemnity. This is mitigated by the type of personal data being processed and the technical and organisational measures put in place. This risk has been reduced due to stating an indemnity figure of **S43(2)**.	Reduced	Low
Data sharing between UK law enforcement and partner agencies in an unlawful manner	Unlikely	2	Low	Any data shared between UK law enforcement and partners will be via recognised intel sharing procedures and subject to further DPIAs/lawfulness and proportionality assessments as required.	Reduced	Low

9.3 International Transfers						
- Will data be shared with a third party based outside the EU? - If you will be making transfers, how will you ensure that appropriate safeguards are put in place?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**
Data sharing between UK law enforcement and international partners including EUROPOL and member states in an unlawful manner	Unlikely	2	Low	Any data shared between UK law enforcement and international partners will be via recognised intel sharing procedures and subject to further DPIAs/lawfulness and proportionality assessments as required.	Reduced	Low
9.4 Additional Risk Factors Describe any further risks, ensuring that any risks not already identified are included.						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**
The use of new technologies including an algorithm (See 5.4)	5	2	Medium	Implement AlgoCare, ICO guidance (Guide ICO big-data-artificial intelligence machine learning-data-protection Sept 2017) and RUSI recommendations. (Machine Learning Algorithms and Police	Accepted	Low

				Decision-Making - Legal, Ethical and Regulatory Challenges - Whitehall Report 3-18) AlgoCare review completed by Pervade: **IMORCC Embedded Doc**		
Can the Machine Learning algorithm be retroactively deconstructed to determine how the prediction has been generated?	5	2	Medium	The data that feeds the algorithm and the data produced by the algorithm (the suggestions made) are owned by the Force and can be accessed easily. If requested the vendor (Pervade Software Ltd) is prepared to uncode and share the conditions produced by the algorithm that are used to evaluate the data in order to prove the functional success of the algorithm. This will be subject to the oversight of the Governance Board, and Ethical and Technical Advisory Groups.	Accepted	Medium

Describe in plain English the influence that each variable has on the systems overall prediction.	5	2	Medium	In the learning phase the algorithm receives an event (which could happen many hundreds of times per second) that is identified as an attack event, either by the static rules engine or manually whilst being taught though it is not informed why the event has been categorised as such. The algorithm attempts to identify similarities between all of the events passed to it in order to provide rules that might be used to auto-categorise. Each event has an equal chance to influence the resultant rule-set however any single event can easily be cancelled out by a contradicting event.	Accepted	Medium

Section 10 – Operational Data Risks - Additional Risks Relevant to Operational Data Only

This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then move to Section 11.**

10.1 Data Logging

Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.

If the data is processed electronically then will a log be retained of the following actions:

• **Collection** • **Alteration** • **Consultation** • **Disclosure** • **Combination** • **Erasure**	☒ Yes for all actions ☐ No* for any action ☐ Not applicable ***If you answered "no" then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**
No risks identified						

10.2 Data Categorisation

When processing data for law enforcement purposes, you must **provide where relevant and as far as possible** a clear distinction between categories of data subject.

Will there be a clear distinction between different categories of personal data suspects, for example subjects who are:

• Suspected of having committed, or are about to commit, a criminal offence • Convicted of a criminal offence, • Victims of a criminal offence, • Witnesses to a criminal offence.	☒ Yes The Police are only interested in suspicious activity. ☐ No* ☐ Not applicable If you answered "no" then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation / Solution	Result	Residual Risk
A data subject may initially be identified as a suspect if, as a result of being categorised with the SFA, when in fact they had sent a legitimate message.	4	Minor	Medium	All PCA - NTA data will be subject to grading and further development by UK law enforcement as part of an investigation strategy minimising the risk of a victim being wrongly identified. If a subject is mis-identified as a suspect then this should be corrected as soon as possible.	Reduced	Low

Section 11 – Outcome and Review			
11.1 Outcome			
Item	**Name**	**Date**	**Notes**
Residual risks approved by:	T/Detective Chief Superintendent Andrew Gould	19/05/2020	Comments and changes recorded in tracked changes for audit purposes. I am happy all reasonably foreseeable risks have been identified and mitigated appropriately.
The DPS/DPO advice provided by:	**S40**	21/05/2020	The actions to mitigate or provide a solution for the risks recorded in Section 9 and 10 are to be completed by being integrated back into the project plan. The IAO must be able to demonstrate 'accountability' by having appropriate measures and records in place to show compliance. Any deviation from the 'Nature, Scope, Context and Purposes' of the processing described in this DPIA needs to be subject to a new DPIA.
Summary of the DPS/DPO advice, including whether the ICO must be consulted:	**S40**	21/05/2020	As above. There is no need for the ICO to be consulted at this time.
11.2 Review			
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.			
Outline: • Who will be responsible for reviewing the processing • The frequency of review • The date of the next review			
It is recommended the Information Asset Owner review this DPIA and have it updated following the 'local trails' before the PCA – NTA tool is rolled out to the rest of the country.			