Information Risk Assessment Report

Police CyberAlarm

Author: **S40** (NMC Security Consultant)
Date: 26th April 2021
Version: 0.1

Document Information	
Author:	**S40**
Owners:	**S40**

Version History	Version Date	Requestor of Change	Summary of Change(s)
0.1	26/04/2021	**S40**	Initial draft
1.0	08/06/2021	**S40**	Updated after feedback from **S23**, **S40** and Pervade.

Distribution		
Version	**Date**	**Name/Role**
0.1	26/04/2021	**S23**- NPCC National Darkweb Coordinator
1.0	08/06/2021	**S23**- NPCC National Darkweb Coordinator **S40**– NPIRMT Lead Assurer

Contents

Executive Summary

The NPCC have launched Police CyberAlarm (PCA) to help small to medium size businesses (SMEs) protect themselves better from Cyber Crime and at the same time provide valuable intelligence to Cyber Policing.

The PCA service is promoted too Small to Medium Enterprises (SMEs) by local forces, who subsequently have access to the intelligence, along with Regional and National Cyber Policing Units.

It is proposed that forces themselves could and should consume the PCA services.

This document has been used to capture the details of the risk assessment that has been carried out on this service in order that it can be safely utilised by Forces, where they see a benefit.

The document provides the scope and governance of this risk assessment process, a more detailed overview of the service, including architectural principles and details of the risk assessment itself, including the supporting documentation.

The service has been through a robust risk assessment, including early engagement with NPIRMT, through the high-level risk review and process flow document, assessment via the Candidate Control Set for Security and a Data Protection Impact Assessment.

The service is provided by a third-party supplier, Pervade, who provide the technology to the voluntary organisations that consume the service, conduct the collection and scanning of firewall and vulnerability data and produce the reports. Pervade utilise UK based Data Centre services of another third-party, **S31 & S43**, who in turn provide Data Centre facilities from **S31 & S43** These premises were in the process of undergoing a PASF (Police Approved Secure Facilities) review but, have been held up by the current Covid pandemic. **S31 & S43**are ISO 27001 certified and the **S31 & S43**is in scope of this accreditation, by the British Assurance Bureua.

The assessment identifies three (3) risks, two low and one medium. Adequate mitigation is either in place or has been agreed to be put in place and it is recommended these two low risks are accepted. The medium risk relates to the service sending reports across standard email channels. It has been recommended that a secure method of sending the reports is agreed and used as the default for Forces consuming the services, once this is designed, documented and agreed, then the residual risk can be lowered to 'Low' and the risk would be at an acceptable level.

Once the outstanding medium level risk is reduced and NPIRMT are in agreement with this report, then it is recommended that this service is suitable for consumption by Police Forces across the UK.

1. Introduction

1.1. Purpose

The purpose of this risk assessment is to evaluate the adequacy of the security of the Police CyberAlarm system and supporting processes (referred to as the 'service'). This risk assessment provides a structured qualitative assessment of the operational environment. It addresses sensitivity, threats, vulnerabilities, risks and safeguards. The assessment recommends cost-effective safeguards to mitigate threats and associated exploitable vulnerabilities.

1.2. Background and context

The NPCC have launched Police CyberAlarm (PCA) to help small to medium size businesses (SMEs) protect themselves better from Cyber Crime and at the same time provide valuable intelligence to Cyber Policing.

The PCA service is promoted too Small to Medium Enterprises (SMEs) by local forces, who subsequently have access to the intelligence, along with Regional and National Cyber Policing Units.

It is proposed that forces themselves could and should consume the PCA services.

The benefits to the forces are:

- Will have visibility of external attacks on their own web facing infrastructure.
- Will have regular updates on any vulnerabilities on their external facings IPs, Websites and Web Applications.
- Avoiding embarrassment of having vulnerabilities on their own systems, that they are advising the public on.
- **S31**
- Which provides more contextual knowledge and intelligence to the NMC, which benefits the forces with accurate NMC response to attacks.
- Network Traffic Analysis can be used to monitor for and identify use of shadow IT Infrastructure.

The Police CyberAlarm service is made up of 3 components: Network Traffic Analysis, Vulnerability Scanning IP and Vulnerability Scanning Website and Web Application.

Network Traffic Analysis

- Suspicious firewall activity (SFA) is collected from volunteer organisations[1] firewalls and sent to Pervade central servers for analysis.
- Monthly reports are provided to volunteer organisations, with details of attacks on firewalls.
- Police Cyber Crime Units utilise the data for intelligence and investigations.

Vulnerability Scanning - IP

- Volunteer organisations provide target IP addresses they want scanned.
- IP addresses are scanned by OpenVAS (an open-source vulnerability scanner) hosted on the Pervade Central Servers.
- Identified vulnerabilities are reported to the volunteer organisation with recommended remediation.

[1] Volunteer Organisation would be an SME or a Force

Vulnerability Scanning – Website and Web Application

- Volunteer organisations provide target websites and web applications they want scanned.
- Websites and web applications are scanned by Nikto hosted on the Pervade Central Servers. This would include testing for SQL injection, Cross-Site Scripting (XSS) and Layer 7 denial of service attacks amongst other attacks.
- Identified vulnerabilities are reported to the volunteer organisation with recommended remediation.

1.3. Ownership

The NPCC Cybercrime programme is responsible for the delivery of the Police CyberAlarm Service.

Ownership of the contract with the supplier sits with the Police & Crime Commissioner for Derbyshire.

Firewall logs and vulnerability data collected are owned by the Forces who consume the PCA services.

IA Role	Person Responsible
National SIRO (NSIRO)	Commissioner Ian Dyson, Police Information Assurance Board
Information Asset Owner	Detective Chief Superintendent Andrew Gould
Programme Manager	**S23** - NPCC National Darkweb Coordinator
NMC Assurer	**S40**, NMC Security Consultant
Lead Assurer	**S40**, NPIRMT

Table 1 – IA Roles for the Police CyberAlarm Service

1.4. Scope

The scope of this risk assessment is to assess the system's use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threat sources, internal and external, to the Police CyberAlarm Service.

Listed below is the assurance scope for this Risk Assessment:

- Pervade – Solution Provider;
- **S31 & S43**– Data Centre Provider;
- Network Traffic Analysis Software deployed to Force environments;
- Data and report transmission.

The following solution components are **out of scope** of this risk assessment:

- **S31 & S43**– Solution Host(1);
- Police force networks, where the software is deployed(2).
- Vulnerability Scanning solutions – OpenVAS and Nikto(3).

Rationale for out of scope components:

(1) The Common Council of the City of London contract is with Pervade and **S31 & S43**are a downstream supplier, with a contract with Pervade. The risk

assessment relies on Pervade having suitable supplier assurance processes in place, which will be validated through the assurance of Pervade itself.

(2) PCA/Pervade provide an FAQ, which recommends deployment of the NTA collector in the Force DMZ to enable the secure collection of firewall traffic (metadata). It is incumbent upon the Force to follow this guidance for secure deployment or implement an alternate secure solution, if they do not operate a DMZ.

(3) OpenVAS and Nikto vulnerability scanning solutions are provided by Pervade as part of their solution. They are hosted, managed and accessed by Pervade only and so the Pervade data controls are already covered in this assessment.

This Risk Assessment Report evaluates:

- Confidentiality - protection from unauthorised disclosure of system information and data.
- Integrity - protection from improper modification of information.
- Availability - loss of access to the system
- Compliance - with national guidelines and legislation, and local policies and procedures.

2. Governance

2.1. Risk Appetite

The National Policing Risk Appetite Policy has been consulted to determine the overall risk appetite for this service. Risk appetite has been set to a level of 'Cautious'. The rationale being, the collection of vulnerability data and firewall log data should be managed safely, but the benefits of this service are also seen to reduce risk through the early identification of vulnerabilities and the gathering of intelligence to detect current and/or prevent future attacks.

Cautious is defined as - *preference for safe delivery options that have a low degree of residual risk*.

Consequently, it is intended that the design, implementation and operation of security controls will result in the reduction or elimination of any identified risks to an acceptable and low level.

2.2. Roles & Responsibilities

The roles and responsibilities identified to support and approve this Risk Assessment are as follows:

- **Police Information Assurance Board (PIAB)** – is responsible for acting as the information risk management governing body for all national policing systems and the accreditation process that governs the management, connection to them and sharing of their data;
- **National SIRO (NSIRO),** Commissioner Ian Dyson, Police Information Assurance Board - has responsibility for ensuring all national information systems are appropriately risk assessed and identified risks are managed in accordance with the National Policing Accreditation Policy;
- **Police CyberAlarm Information Asset Owner (IAO),** Detective Chief Superintendent Andrew Gould - responsible for understanding and addressing risks to the Police CyberAlarm;
- **NMC Security Consultant,** **S40**– has assisted in the assessment of information risks presented by the Police CyberAlarm service, identifying mitigating controls, working with the PCA Programme on implementation of the controls by the PCA Programme and/or its suppliers, and working with NPIRMT to ensure satisfactory risk levels are achieved;
- **Programme Manager (PM),** **S23** – is responsible for the implementation and management of the PCA service, including, but not limited to the implementation and maintenance of agreed security controls; and
- **National Police Information Risk Management Team (NPIRMT),** **S40**, Lead Assurer, NPIRMT - acting as an impartial assessor of the risks presented by the Police CyberAlarm service.

2.3. Review & Approvals

This document and all listed assurance artefacts are required to enable NPIRMT, the IAO and the NSIRO (if required) to understand the residual risks of the Police CyberAlarm.

Review and approval of the final Information Risk Assessment Report (IRAR) will support the overall NPIRMT/IAO/NSIRO assurance to operate the Police CyberAlarm for authorised use by police forces.

Note: NPIRMT, the IAO or NSIRO, may choose not to support the provision of the Police CyberAlarm, if they deem the residual risks to be too great.

3. Solution Overview

3.1. Information Assets

The Police CyberAlarm is intended to store and handle the following national police information asset groups:

Data	Description	Information Asset Type	Classification	Risk Ranking
Member Data (Force)	Data collected for contact and management purposes: Volunteer Organisation's Name | email addresses | Address | IP addresses | Website URLs (For Web App scanning)	Personal Data	Official	Medium
Force Data	For managing access to PCA: Username | email address | Name | Role | Unit | Force of the Police 'staff'	Personal Data	Official	Medium
Vulnerability Data	Vulnerabilities collected are public, as can be collected by anyone conducting a scan of the public facing IPs and web applications.	Police Corporate Information	Official (Sensitive)	Medium
Suspicious Firewall Activity Data	Header Data Collected: IP Version | Header Length | Priority | Length | Identification | Flags | Fragmented Offset | TTL | Protocol | Header Checksum | Source IP | Dest. IP | Options | TCP | UDP	Police Corporate Information	Official (Sensitive)	Medium

Table 2 - NPIRMT definition of National Policing Information Assets

Under the Government Security Classifications Policy, this data has been classified as OFFICIAL and OFFICIAL-SENSITIVE. Under national policing guidance for handling policing data within the OFFICIAL and OFFICIAL-SENSITIVE tiers for this type of data, the Police CyberAlarm attracts the MEDIUM gradation of the policing candidate control sets.

Note: The Police CyberAlarm is not expected to hold information assets pertaining to:

- Special categories of personal data and personal data related to criminal convictions (as defined by the Data Protection Act);
- Covert intelligence or other police operations; or
- Counter terrorism operations.

3.2. Architectural and Process Flow Overview

The Police CyberAlarm system has been designed to have a minimal footprint in the Volunteer Organisation environment and to move and store data gathered securely. This centralised server model has been utilised to maximise processing and storage capacity, with little impact on the Volunteer Organisations.

The diagram below provides a high level overview of the PCA solution. More detailed and technical design documentation is available in the supporting documents referenced in Section 4.3.

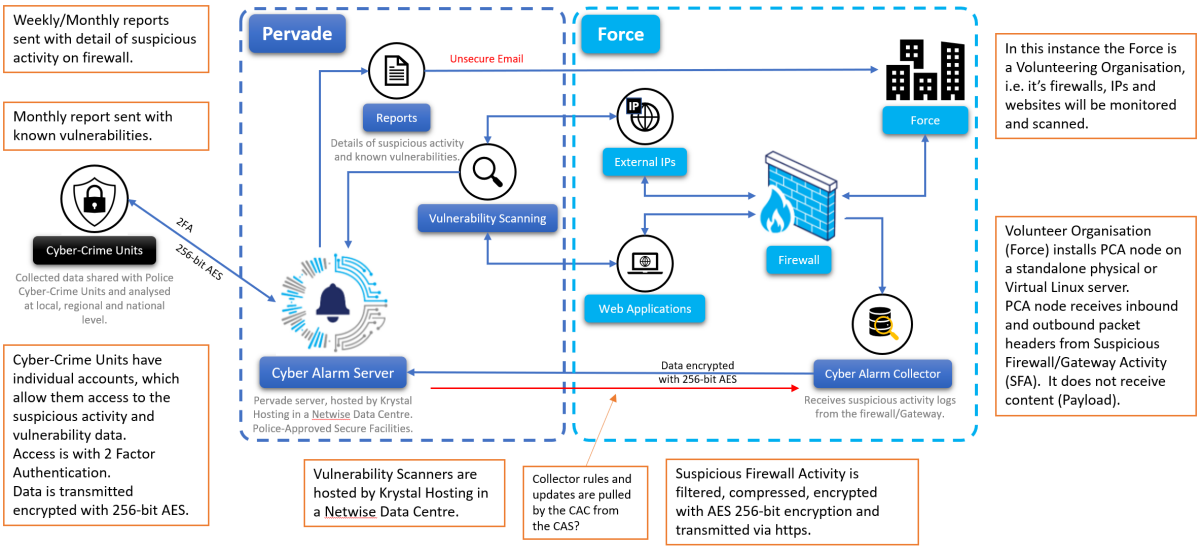


Figure 1 – Process Flow Diagram for the Police CyberAlarm

Key steps in the flow of data.

Network Traffic Analysis:

- Force deploys CyberAlarm Collector (software) to a stand-alone Linux physical or virtual server.
- CyberAlarm Collector (CAC) server is sited in the Force DMZ alongside the Firewall or on a dedicated VLAN.
- The service is registered, and the necessary keys exchanged to create secure communications tunnels.
- Firewall is configured by the Force to send inbound traffic header logs to the CAC. Assuming syslog (depends on firewall type).
- CAC receives the firewall header logs (metadata), identifies what it believes to be Suspicious Firewall Activity (SFA), e.g. dropped packets, specific packet types, etc and drops the valid traffic headers.
- The CAC compresses the SFA, encrypts the SFA (AES-256) and writes to disk on the CAC ready to send to the central CyberAlarm Server (CAS).
- The CAC instigates a secure channel with the CAS and sends the compressed and encrypted SFA across an encrypted tunnel.
- The CAS unpacks the data, takes a forensic hash and encrypts the data to an individual database related to the source Force.
- The CAS takes a copy of the unpacked data, extracts the relevant header data it requires, **S31 **, etc and stores encrypted.
- Periodically (Weekly/Monthly) the analysed data is collated, and a report produced detailing malevolent firewall activity at the Force perimeter.
- The data and reports can be accessed by Regional and National Police Cyber Crime Units to allow reporting and analysis at a Regional and National level.

Vulnerability Scanning – IP, Website and Web Application:

- Force registers for the PCA service.
- Check conducted to ensure validity of organisation registering.
- Email address for reporting is agreed.
- Force provides IP addresses, Website addresses and Web application details that they require scanning, via PCA portal.
- Monthly scans conducted either by OpenVAS (IP Addresses) and/or Nikto (Websites and Web Applications).
- Both scanning tools are hosted in the Pervade environment, based in the UK.
- Scan results are encrypted and stored separately for each Voluntary Organisation (Force).
- Scan results are used to produce a vulnerability report, which is emailed to a previously agreed email address, agreed at registration.

3.3. Architectural Notes

3.3.1. Force Environment

It is assumed Force Firewalls at the perimeter will be on a dedicated network, often referred to as the De-Militarised Zone (DMZ), which is segregated from internal networks by further firewalls and used to host external facing services, such as webservers, firewalls and load balancers. It is recommended that the physical or virtual Linux server used to host the CyberAlarm Collector (CAC) is hosted here.

This means the third-party supplier Pervade does not have access to the internal network of the Force and the traffic from the firewall remains in the same network zone, exposing it to no more risk that it would already be exposed to in this zone. Additionally, the use of vulnerable UDP protocols and ports, typically seen in the DMZ, do not need to be extended to the internal network.

Should a Force not be using a DMZ, then a dedicated Virtual Local Area Network (VLAN) should be utilised to host the virtual or physical Linux server running the CAC, with traffic restricted to the Firewall logs sent from the Firewalls.

3.3.2. Data Storage

Pervade utilise **S31 & S43**Data Centre based in London, UK, with hosting services acquired via **S31 & S43**

Pervade utilise industry best practice hashing algorithms to forensically protect the integrity of the data they collect.

Each data set is segregated, i.e. Suspicious Firewall Activity from a Force will have its own database, likewise a vulnerability scan will be segregated in its own database. These two data sources are not merged. Neither is multiple Forces data collated or merged. Only meta data is taken and used for Regional or National reporting, e.g. a common known bad source IP scanning multiple Forces.

Data is encrypted when written to disk using 256-bit AES algorithms.

Access to data by Forces, Regional Units or National Units is via the PCA Portal and requires 2 Factor Authentication, set-up at registration, i.e. password and one time access code sent via SMS to number registered at set-up.

3.3.3. Access Controls

A Force will have two roles within Police CyberAlarm if they install the system as a 'Member Organisation'

- As a 'Force' who is receiving the Member Organisations data.
- As Member Organisation who is sending data to their Force (themselves)

Each Force can receive requests from or invite SMEs (Voluntary Organisations) within its patch to participate in the PCA service.

As a Force they will have access via a web portal to the PCA central servers and analytical suite. This access is controlled via a Force Group which is controlled by a Local Admin who can create and delete group members.

To be a member of a group you have to have access to a .pnn.police or police.uk email address, along with other domains as required (for example the nca.gov.uk domain). The Local Admin is approved by the PCA Programme Team. The Admin is then able to authorise other members of the group.

It is the responsibility of the Local Admin to review and monitor access including conducting regular reviews of users, ensuring users remain valid, i.e. movers and leavers are removed.

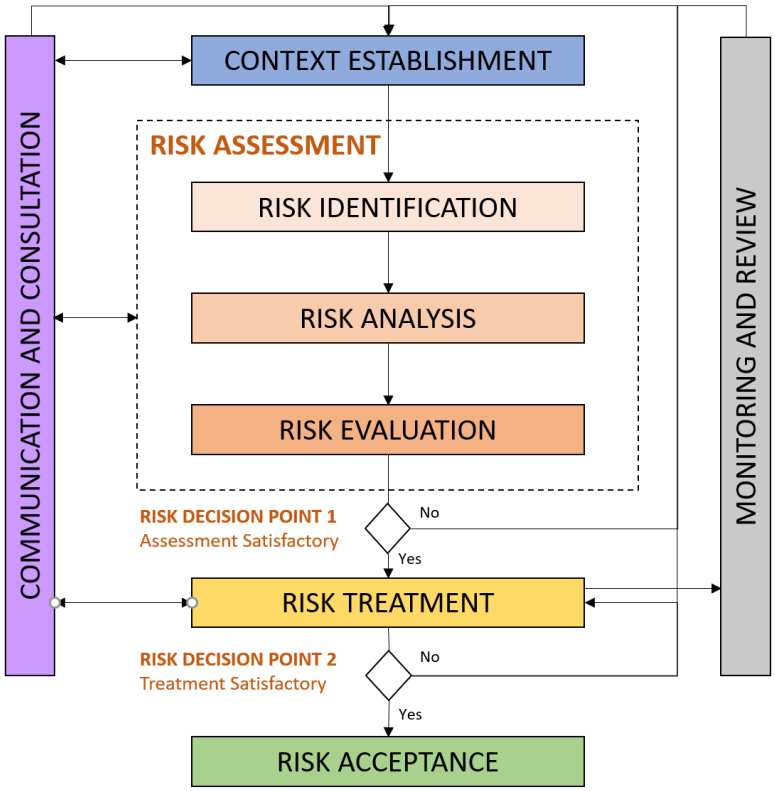
Regional Cyber Crime Teams and **S23**

As a Member Organisation the Force will have to agree to the standard terms and conditions and install a PCA data collector as per the guidelines (as outlined above) this will identify any domains and IP addresses which require scanning and the details of who the reports will be sent to.

4. Risk Assessment

4.1. Risk Assessment Methodology

This Risk Assessment follows an industry standard risk assessment methodology, which is aligned to 'ISO 27005 - Information technology - Security techniques - Information security risk management' and is illustrated in *Figure 2* below:



The assessment has conducted over a number of stages:

1. The NMC Security Consultant has worked with solution owners and designers to understand the data assets, system components and data flows.
2. The NMC Security Consultant hosted a high-level risk workshop (formal) and/or multiple conversations (informal), with the solution owners and designers to understand the threats, vulnerabilities, and existing controls. The output of this was a high-level data flows and risk overview document (see artefacts in Section 4.3) which was reviewed and validated by the solution owners and designers and presented to the Lead Assurer (NPIRMT), to allow NPIRMT input.
3. Based on the above the CCSS v2.0 (spreadsheet) was completed and this document has been produced (IRAR). These are again validated by the solution

owners/designers and subsequently passed to the Lead Assurer (NPIRMT) for review and approval.

4. Any residual risks and/or risk actions will be recorded by the PCA Programme, in an appropriate Risk Register and monitored and managed as appropriate during the life of the PCA service.

4.2. Minimum Control Assumptions

This risk assessment has been conducted with the assumption that a number of controls are in place and effective:

- The ISO accreditations published by the third parties engaged in the provision of the PCA service and on which we rely, have been carried out with due diligence, have a suitable scope and have been provided by reputable certification authorities;
- The third party suppliers are operating under ISO27001:2013 certification that remains aligned with the NPIRMT control requirements set out in the Candidate Control Set for Services (CCSS), and the NCSC Cloud Security Principles; and
- The Pervade support personnel with potential access to OFFICIAL-SENSITIVE materials have a valid need-to-know and hold levels of formal vetting in accordance with the specific contractual conditions.

4.3. Background Assessments

The following background assessments are employed by this Information Risk Assessment Report:

Document	Details
2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 1) **2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 2)**	**Data Protection Impact Assessments** – the need for the DPIAs was identified as personal data of Force Personnel will be handled by Pervade, i.e. User names and email addresses.
2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 3)	**Data Flows and Risk Overview** – Initial risk assessment document that considers the solution components, the data assets, the data flows and looks at risk from a data perspective.
2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 4)	**Candidate Control Set for Services** – Completed as part of the Risk Assessment.
Available on request	**Pervade and **S31 & S43****ISO Certificates** – Reviewed and validated by **S23**

Document	Details
2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 5) **2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 6)**	**Voluntary Organisation Implementation Guide and FAQ** – Guide provided to Forces for implementation of the solution, along with FAQ.
2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 7) **2021.04.26 PDS Information Risk Assessment Report v1.0 (PCA) (Embedded doc 8)**	**Pen Test Report & Resolution Tracker –** As an external facing service, the PCA service has been penetration tested, with findings reviewed and remediated. Both the PCA portal and the CAC were in scope.

4.4. Risks Identified

This assessment in combination with the original high-level assessment has identified three (3) risks, detailed below:

Risk Reference			PCA01
Vulnerability	Eavesdropping / line tapping / espionage		
Threat	Loss of data, loss of confidentiality and/or loss of reputation.		
Risk Description	Firewall log data could be intercepted on the hop from the Firewall to the CyberAlarm Collector (CAC), resulting in a risk to confidentiality, integrity and availability of the data.		
Existing Controls	Forces follow implementation guidance for the CAC to sit in the DMZ with the Firewall or alternately a secure solution based upon their own network design. See architectural guidance for more detail and guidance document in Section 4.3.		
Gross Ratings	**Likelihood**	**Impact**	**Risk Rating**
	Negligible	Moderate	Low
Mitigating Controls	No additional controls are deemed necessary over and above the existing controls.		
Residual Ratings	**Likelihood**	**Impact**	**Risk Rating**
	Negligible	Moderate	**Low**

<table>
<tr><td colspan="3">Risk Reference</td><td>PCA02</td></tr>
<tr><td>Vulnerability</td><td colspan="3">Eavesdropping / line tapping / espionage</td></tr>
<tr><td>Threat</td><td colspan="3">Loss of data, loss of confidentiality and/or loss of reputation.</td></tr>
<tr><td>Risk Description</td><td colspan="3">NTA and Vulnerability reports are intercepted when sent across unencrypted email platforms, resulting in a loss of confidentiality of the reports and causing reputational damage.</td></tr>
<tr><td>Existing Controls</td><td colspan="3">• Pre-agreed email addresses are used, which are populated through automated processes.
• Relies on optional TLS at the mail servers for encryption.</td></tr>
<tr><td rowspan="2">Gross Ratings</td><td>Likelihood</td><td>Impact</td><td>Risk Rating</td></tr>
<tr><td>Low</td><td>Major</td><td>Medium</td></tr>
<tr><td>Mitigating Controls</td><td colspan="3">Agreed with Pervade:

• New user type to be created for Force users, i.e. when consuming the PCA service.
• New user type will have access to the PCA portal (not normally available to SMEs).
• New user type will have access to their reports (for their Force) only.
• Force will receive an email letting them know a report is available on the portal.
• New Force User type will go through secure registration as per other Force, RCCU and NCSC user types and will follow same secure access protocols to the PCA portal.

The above will be implemented prior to use of this service by Forces.</td></tr>
<tr><td rowspan="2">Residual Ratings</td><td>Likelihood</td><td>Impact</td><td>Risk Rating</td></tr>
<tr><td>Negligible</td><td>Major</td><td>Low</td></tr>
</table>

Risk Reference			PCA03
Vulnerability	Poor control over access rights.		
Threat	Theft of data, unauthorised access and/or modification of data.		
Risk Description	Force, RCCU and NCCU users could retain access to PCA data, after they have moved from a Team requiring access or leave the Force, RCCU or NCCU, resulting in potential unauthorised access to Force Vulnerability data and/or NTA.		
Existing Controls	Additional Movers and Leavers controls are to be put in place for the RCCUs and NCCU.		
Gross Ratings	**Likelihood**	**Impact**	**Risk Rating**
	Negligible	Moderate	Low
Mitigating Controls	Forces will be advised to do the same.		
Residual Ratings	**Likelihood**	**Impact**	**Risk Rating**
	Negligible	Moderate	**Low**

4.5. Residual Risk Assessment

Following a number of risk assessment activities identified within this document, the overall risk findings for the Police CyberAlarm indicate that there will be three residual risks, that after mitigation will be rated as low and are therefore within appetite for this service.

4.6. Assurance Conditions

This assurance confirms that the Police CyberAlarm service may be operated on the understanding that the service and its supporting systems continue to be satisfactorily risk-managed.

This assurance should be reviewed and re-assured, if an event listed below occurs (subject to the Assurers discretion):

- The introduction of interconnections to other business domains;
- A change in requirements for storing and processing protectively-marked information;
- A change in the type of data processed and stored, i.e. other than firewall metadata and vulnerability data;
- A significant change in the system configuration or architecture;
- Changes in architecture or practices that are warranted following the review of repeated security incidents of a similar type;
- A major single security incident; or
- A significant alteration to working practices.

NPIRMT Lead Assurer Comments

5 Approvals

Name and Role	Signatures and Dates
S40 - NPIRMT Lead Assurer	
- **S23** NPCC National Darkweb Coordinator	

Appendix A: Risk Evaluation Detail

The Risk Matrix below is aligned to the Impact and Likelihood ratings defined in the NMC Information Risk Management Framework and noted below.

LIKELIHOOD						
	Severe	**Medium**	**High**	**High**	**Very High**	**Very High**
	Substantial	**Low**	**Medium**	**High**	**High**	**Very High**
	Moderate	**Low**	**Medium**	**Medium**	**High**	**High**
	Low	**Low**	**Low**	**Medium**	**Medium**	**High**
	Negligible	**Very Low**	**Low**	**Low**	**Low**	**Medium**
		Negligible	Minor	Moderate	Major	Critical / Catastrophic
		IMPACT				

Risk evaluation is the process of taking the potential impact and likelihood ratings and applying them to a predetermined evaluation criterion, which is defined in the Information Risk Assessment Process.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

Risk Rankings

The table below defines the nomenclature used for each ranking, taken from the 'National Policing Information Risk Appetite v2.2'.

Risk Ranking	Description
Very High	This is above the organisation's defined tolerance level. The consequences of the risk materialising would have a disastrous impact on the organisation's reputation and business continuity. Comprehensive action is required immediately to mitigate the risk.
High	The consequences of this risk materialising would be severe but not disastrous. Some immediate action is required to mitigate the risk, plus the development of a comprehensive action plan.
Medium	The consequences of this risk materialising would have a moderate impact on day-to-day delivery. Some immediate action might be required to address risk impact, plus the development of an action plan. Status of the risk should be monitored regularly.
Low	The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered. Status of the risk should be monitored periodically.
Very Low	The organisation accepts this risk / impact of risk would be insignificant. Status of the risk should be reviewed occasionally.

Likelihood Analysis

National Policing use an Information Threat Model which describes the likelihood of an event occurring and is used here for gauging the likelihood of an event occurring.

The National Policing Information Threat Model provides an overview of the potential sources of threat posed to National Police information systems, Force systems and networks, and collaboration systems.

The descriptions used are from the now discontinued HMG Information Security Standards No. 1 and 2, but still prove useful in quantifying risks to National Police Information Systems.

The following governing factors were considered when calculating the likelihood that a potential vulnerability might be exploited in the context of the associated threat environment:

- Threat source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

Likelihood Score	**1**	**2**	**3**	**4**	**5**
Descriptor	**Negligible**	**Low**	**Moderate**	**Substantial**	**Severe**
Threat Level: Established from Threat Actors capability combined with priority.	The threat is highly unlikely to materialise.	The threat is unlikely to materialise.	The threat is possible, but not likely.	The threat is likely to materialise.	The threat is highly likely to materialise.
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Frequency: How often might it/does it happen.	This will probably never happen or recur.	Do not expect it to happen/recur but it is possible it may do so.	Might happen or recur occasionally.	Will probably happen/recur but it is not a persisting issue.	Will undoubtedly happen/recur, possibly frequently.

Impact Analysis

Currently NPIRMT Policy, Home Office Policy and PICT Co Policy provide an 'Impact Scale' of 1 to 5 (Negligible to Critical/Catastrophic) and this is used in combination with the Likelihood scale to assess risk.

The table below provides the descriptors for the different types of Risk Impact used by the NMC and Police ICT.

Impact Score	1	2	3	4	5
Descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Critical / Catastrophic**
Strategic Objectives: PICT Co, Supplier(s), Forces strategic objectives are impacted.	Negligibleimpact on strategic objectives.	Small variance from overall strategic objectives.	Notable variance from overall strategic objectives.	Significant variance from overall strategic objectives.	Failure to meet strategic objective(s) threatens independent functioning or stability of PICT Co, Supplier(s) and/or Forces.
People: Impact on the safety of the staff, contractor or public.	Minimal injury requiring no/minimal intervention or treatment. No time off work.	Minor injury or illness, requiring minor intervention. Increase in length of time off work by 1–3 days.	Moderate injury requiring professional intervention Increase in length of time off work by 4–15 days. RIDDOR/agency reportable incident. An event which impacts on a small number of staff.	Incident resulting in serious injury or permanent disability/incapacity. Increase in length of time off work by >15 days. Mismanagement of staff with long- term effects.	Incident resulting in fatality or multiple fatalities. An event which impacts a large number of staff.
Reputation: PICT Co, Supplier(s), Forces suffer reputational damage.	No noticeable or measurable effect on brand value or perception. No mention of incident in the media.	Minor damage to brand image / perception among a small number of forces and/or members of the public. Minor coverage of incident in local media.	Brand fails to meet force or public needs in some areas, but force preference and public confidence remains largely unchanged. Some coverage in regional media (but controlled).	Brand perception badly damaged. Brand not 1st or 2nd choice for forces and/or public confidence is negatively impacted. Wide coverage in national media.	Widespread and irreversible perception that brand fails to meet most force needs and/or public confidence is adversely impacted. Significant coverage in national (and international media).
Compliance: The organisation breaches legal or regulatory requirements e.g. Data Protection Act 2018.	Breach of voluntary code / guidance; no regulatory action / no investigation / no civil action.	Minor / limited breach unlikely to prompt an investigation, fine or censure. Informal recommendation from regulator.	Serious breach of single requirement, possibly prompting regulatory oversight / investigation and civil sanctions.	Systemic breach, possibly prompting investigation / enforcement / substantial investigations and large civil sanctions.	Serious systemic breach likely to prompt restrictions / enforcement / criminal prosecution or conviction.
Financial: PICT Co, supplier(s), Forces suffer a financial loss.	Negligible loss	<£10k	>£10k ≤£100k	>£100k ≤£500k	>£1M
Data: PICT Co, Supplier(s), Forces suffer a financial loss.	One Force impacted and non-personal data items lost /stolen, classified at Official or less. Minor breach of confidentiality. Single individual affected.	More than one Force is impacted and non-personal data items are lost / stolen, classified at Official or less. Breach with potential for theft / loss of personal information, with between 20 – 50 people affected.	More than ten (10) Forces are impacted, and non-personal data items are lost / stolen, classified at Official or less. Breach with potential for theft / loss of personal information, with between 50 – 100 people affected. Loss or misuse of sensitive personal information, relating to 2-5 persons.	More than twenty (20) Forces are impacted, and non-personal data items are lost / stolen at Official or less and / or any data classified as Official Sensitive (non-personal) or above is lost. Serious breach with potential for theft / loss of personal information, with between 100 - 500 people affected. Loss or misuse of very sensitive personal information, relating to 5-20 persons.	The majority or all Forces are impacted, and non-personal data items are lost at Official and / or any data classified as Official Sensitive or above is lost. Major breach with potential for theft / loss of personal information, with over 500 people affected. Loss or misuse of sensitive personal information, relating to over 20 people.
Operational: Operational activities of PICT Co, Supplier(s) or Forces are impacted.	Negligible, very short-term or nominal interruption in operations. Loss/Interruption >1 hour.	Partial short-term interruption of operations. Loss / interruption of >8 hours.	Partial interruption of operations. Loss / interruption of >1 day.	Widespread short-term interruption of operations. Loss / interruption of >1 week.	Widespread, long-term operational shut-down. Permanent loss of service or facility.

Appendix B: Glossary

Name	Meaning
App	Application
BPSS	Baseline Personnel Security Standard
CCSS	Candidate Control Set for Services
CIA	Confidentiality, Integrity, and/or Availability
DPA	Data Protection Act
EUD	End User Device
GDPR	General Data Protection Regulation
GDS	Government Digital Service
GIRR	National Police Governance & Information Risk Return
GSC	Government Security Classifications
IA	Information Assurance
IRAR	Information Risk Management Report
ITHC	IT Health Check (CESG CHECK scheme penetration testing)
Member Organisation	An organisation, such as a Police Force, a Regional Cyber Crime Unit or a National Cyber Crime Unit, who manage the accounts of the Voluntary Organisations and have access to the Voluntary Organisation data of their Voluntary Organisations.
NAPS	National Accreditors for the Police Service
NCSC	National Cyber Security Centre
NPCC	The National Police Chiefs Council
NPIRMT	Nation Policing Information Risk Management Team
NPPV	Non-Police Personnel vetting
NTA	Network Traffic Analysis
PASF	Police Approved Secure Facility
PED	Personal Electronic Device e.g. Laptops, USB drives etc.
PIAB	Police Information Assurance Board
PNN	Police National Network (synonymous to PSN4P)
PSN	Public Services Network
PSN4P	Public Services Network for Policing (synonymous to PNN)

Name	Meaning
SC	Security Clearance – one of the National Security Vetting clearance levels
SFA	Suspicious Firewall Activity
SFTP	Secure File Transfer Protocol
SIRO	Senior Information Risk Owner
SME	Small to Medium Enterprise.
Voluntary Organisation	An organisation, either an SME or a Force, that has volunteered to install a PCA agent in their network and provides IP addresses for scanning.