`

Forensics Net – Supplier Market Briefing Note

1. Purpose of This Briefing

Forensic Services (MO4) deliver the majority of forensics for the MPS, encompassing both digital and traditional disciplines. At present, all data and applications utilised by MO4's digital forensic teams are hosted on a central IT platform known as Labnet, while other M04 teams rely on various platforms and standalone systems for their respective data and applications. Labnet is well established but was implemented several years ago only for use in digital forensics, Labnet and now requires an upgrade to accommodate advances in digital forensics, and consolidating forensic data onto a single platform is now recognised as advantageous.

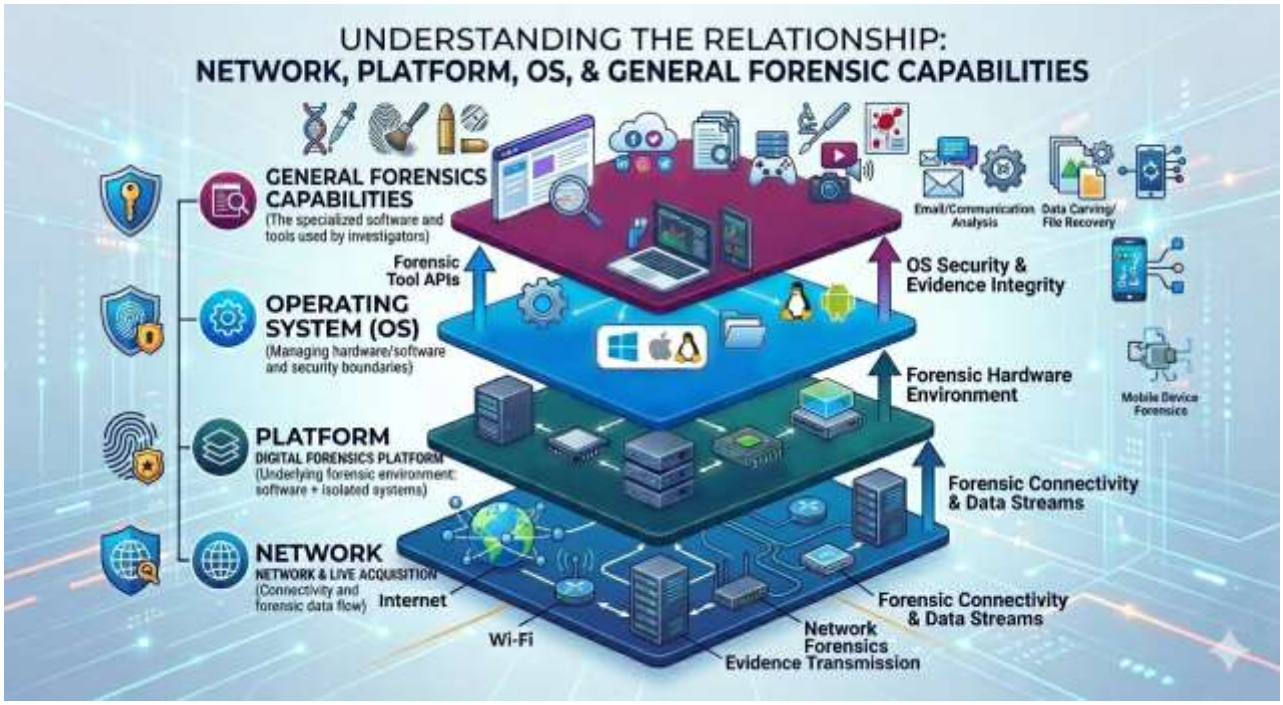
The MPS is exploring market options for a next-generation forensic platform, Forensics Net. This briefing aims to:

- Share the emerging vision, operating context, and high-level requirements
- Invite suppliers to provide insight, methodologies, and solution concepts
- Support early market engagement prior to procurement activity

The MPS is not seeking specific investigative tools, case management solutions, or analysis software. The focus is on a platform enabling secure, scalable, and modern delivery of forensic services, including digital and traditional disciplines.

1.1 Terminology Glossary

To clarify our objectives for this procurement, the diagram below outlines our definitions of "network," "platform," "operating system," and "applications." Our primary focus is on the development and ongoing maintenance of the platform; while there may be some overlap with requirements pertaining to the network and operating system, the principal request concerns the platform itself.



Programme overview: Forensics Net

2. Strategic vision

To deliver a secure, resilient, and integrated forensic platform that connects all areas of forensic services, enabling timely access to forensic evidence, supporting collaboration and contribution across disciplines, and maintaining compliance with retention and regulatory standards.

Forensics Net will serve as a one-stop platform for investigators to access and review their forensic evidence and will play a vital role in supporting staff through easy access to the right tools, systems, and information enhancing both operational effectiveness and service quality.

3. Drivers for change

Forensics Net adheres to our commitments in A New Met for London

Fixing our foundation	Improved security and compliance	End to end data integrity
		Controlled access
		Auditability and transparency
	Enhanced user experience and workforce capability	Simplified access
		Modern user interface and search
	Governance, accountability and strategic control	Local governance with central oversight
		Real- time dashboards

		Policy automation
	Cost Efficiency and sustainability	Consolidated platforms
		Hardware lifecycle management
		Cloud hybrid flexibility
Putting Crime-fighting First	Operational efficiency and productivity	Reduces fragmentation, duplication and delays
		Enables Automation
		Scalable infrastructure
		Remote access
	Future Readiness	AI readiness and innovation sandbox
		Future-proof infrastructure
Working in Partnership	Improve collaboration and case visibility	Inter- departmental connectivity
		Secure external access
		Centralised evidence handling (DAMS/DEMS

4. Departments to be connected

Forensics Net will support all MO4 units, including

- **Digital forensic -**includes hubs located at police station around London
- **Frontline Policing -** includes the crime scene investigation and forensic collision investigation team located in multiple sites
- **Biomatrices** – includes DNA, fingerprints and secure ops
- **Physical forensic** - Includes drugs and firearms
- **Continues improvement team**- includes quality assurance

5. Future high-level functional and non-functional requirements for Forensics Net

High-level requirements from all forensic departments have been identified and are presented in the following summary, categorised onto broad requirement areas- Accessibility, Capability, Governance, Infrastructure, Security, User Experience

MO4 currently employs over 1,200 staff members and police officers, reflecting a 26% increase since 2024, despite ongoing organisational reductions. Forecasting future growth remains complex, as it is contingent upon government funding, police reform, and the continued development of our operational capabilities.

Estimating future storage requirements is challenging; however, the platform must support data storage exceeding 20PB, with anticipated annual growth of 2–3PB.

Accessibility

Title	Description
Unified Secure Connectivity and Access	Remote and cross-site connectivity for authorised staff, officers, contractors, and partners. Provides seamless, secure, and auditable access across all forensic sites and systems, supporting remote work and external collaboration without compromising security.
System Interoperability and Integration	Interoperability between MPS Foundation network, Forensic Case Management System, Quill, Evidence.com, CONNECT, and other core systems to ensure seamless data flow and eliminate re-entry.
Unified Single Sign-On (SSO) and Simplified Access	Single, secure sign-on across all platforms and devices; consistent credentials reduce multiple logins.
Secure Network-Based Data Sharing and Air-Gap Mitigation	Enables secure, monitored digital data transfer between systems and partners, replacing physical media while maintaining chain of custody. Option to use existing MPS network, with logical segregation
External and Time-Bound Partner Access	Provides controlled, auditable, and time-limited access for CPS and contractors with full activity logging.
Resilient Network and Site Connectivity	Maintains high-availability, redundant network connectivity across all forensic hubs, ensuring continuity during outages.
Digital Licence and Accessibility Compliance Management	Online licence activation and compliance with accessibility standards
Controlled and validated access	Support for MFA *(supports controlled and validated access, though often grouped under Security)*

Capability

Title	Description
Centralised Digital Asset and Evidence Management	Single DAMS/DEMS for ingestion, storage, review, and collaboration on digital evidence.
Automated Retention and Archiving Workflows	Automated data retention, archiving, and deletion linked to FCMS and CONNECT with alerts
Scalable Storage and High-Performance Processing	Expandable storage with GPU/VM compute capacity and distributed processing for large datasets.
Integrated AI and Analytics Capabilities	AI-driven analysis, reporting, SOP management, and decision support to reduce manual effort.

Controlled Software Repository and Deployment	Central software repository with version control, gold builds, and controlled deployment management.
Forensic Integrity and Audit Compliance	System-level hashing, deduplication, and audit logging to maintain forensic integrity and legal defensibility.
Local Workflow Control and Customisation	Allow forensic teams to customise workflows and administer local processes within governance standards.
Continuous Technology Refresh and Testing Environment	Regular hardware/software updates with a dedicated sandpit for validation and training.
All-in-One Investigation and Case Management Platform	Unified platform to manage investigations from ingestion to court submission, including digital casefiles.
Patch and Upgrade Testing Environment	Ability to test patches / upgrades on transient replica environment (capability for lifecycle & quality assurance)
Storage	Must support data storage exceeding 20PB… (capacity & scale capability)
Environments	Isolated workstations / VDI for specialist forensic handling capability

Governance

Title	Description
Local Ownership and Change Control	Empowers forensic teams to manage software installs, updates, and workflow changes locally within defined controls.
Central Governance with Local Application	Hybrid model of central policies and local execution for automated retention, archiving, and deletion.
Tracking, Monitoring and Accountability	Ticketing systems and real-time dashboards for monitoring operational status, data flows, and user activity.
Training and Guidance for Governance	Structured training on policies and processes for governance, change control, and audit readiness.
Retention and Deletion Policy Compliance	Automated and auditable retention and deletion policies aligned to regulatory standards.
Compliance with Forensic Codes and Legal Standards	Ensures adherence to Forensic Regulator Codes, GDPR, ISO and evidence-handling accreditations
Cross-Department Visibility and Evidence Coordination	Improves case visibility across departments to avoid duplication and enhance coordination.
Naming Convention and Data Hygiene Policies	Defines consistent naming, storage, and classification standards for all digital files and reports.

Audit logs	Centralised audit logging for all activities, with ability to transfer these logs to central audit service (Splunk)

Infrastructure

Title	Description
High-Speed, Resilient, and Future-Proof Network	High-speed LAN/WAN with redundancy, low latency, and capacity for future growth and AI processing. Option to use existing MPS network, with logical segregation
Business Continuity and Disaster Recovery	Multi-site redundancy, regular backups, and tested recovery plans to ensure continuity of forensic operations.
Hybrid Cloud and On-Premises Architecture	Balanced cloud and on-prem model for storage, archiving, and processing to optimise performance and cost.
Dedicated Forensic Data Centre Capacity	Sufficient data centre space and hardware for specialist forensic requirements
Compatibility with Multimedia and Label Printing	Supports ingest of photos, videos, voice, and on-site label printing for evidence bags.
Secure DMZ Integration and Patch Management	DMZ for secured connection to external sources & services
	Patching (O/S, app) via DMZ ingestion
	Ability to test patches / upgrades on transient replica environment

Security

Title	Description
Role-Based and Granular Access Control	Enforces RBAC with fine-grained permissions and secure casework sections for sensitive investigations
Air-Gapped and Isolated Environments	Secure, air-locked network zones for classified work and national-security data handling
Audit Logging and Monitoring	Comprehensive audit trails for all user and system activities with monitoring dashboards. This could include the export of audit logs to central audit and review systems
Account and Identity Management	Streamlined account creation, deactivation, and secure handling of leavers' data with multi-factor authorisation support.
Anti-Virus and Tool Exception Capability	Controlled temporary disabling or exception handling of security software for forensic tools.

Data Validation and Integrity on Ingest	Automated validation of media uploads (SD cards, discs, portable drives) to prevent corruption or tampering.
Accreditations	CEP - Cyber Essentials Plus
	ISO 27001
	NCSC 14 Cloud Security Principles (Mapping)
	National Institute Standards Technology Cyber Security Framework
	Separate domain for environment, capable of trust relationships with MPS domains
	Support for MFA
	Intrusion Protection System/Intrusion Detection System

User experience

Title	Description
User-Friendly Search and Interface Design	Intuitive search, navigation, and UI that supports technical and non-technical users.
Training and Continuous Learning Support	Embedded guides, virtual training sessions, and scheduled onboarding resources.
Consistent and Familiar Environment	Uniform look and feel across test and live environments with familiar file paths (e.g., H: drive)
Data Hygiene and Storage Organisation	Structured folders, naming standards, and clear case status notifications for efficient retrieval.
Rapid Build and Deployment Experience	Accelerated gold build deployment and consistent user setup across sites.
User Feedback and Improvement Mechanisms	Integrated feedback loops and surveys to capture user issues and drive continuous UX improvement.
Device Compatibility and Ergonomic Design	Standardised cabling, workstation ergonomics, and mobile device access.

What we are seeking from the market

The MPS welcomes supplier engagement on:

- Architectural proposals for a unified forensic network
- Approaches to hybrid cloud deployment
- Methods for supporting secure multi-disciplinary forensic work
- Opportunities to optimise workflows through automation
- Approaches to enhance evidence access for frontline staff
- Models for scalable storage and compute (GPU, high-performance nodes)
- Best practice for integrating biometrics, wet forensics, and digital forensics
- Approaches to user and role-based access control in complex environments
- Options for futureproofing and incorporating AI safely
- Service provision and service model for support of the platform, the hardware it sits on and the network that it runs across.

<u>Suppliers should not propose:</u>

- Specific investigative tools (e.g., phone extraction tools, analysis suites)

- Replacement case management systems

This engagement is focused on the platform, not the specialist tooling or applications that operate on the platform.

7. Next steps

The MPS intends to use supplier feedback to refine:

- Commercial model and procurement approach
- Technical specification
- Architecture and hosting strategy
- Deployment plan and timelines