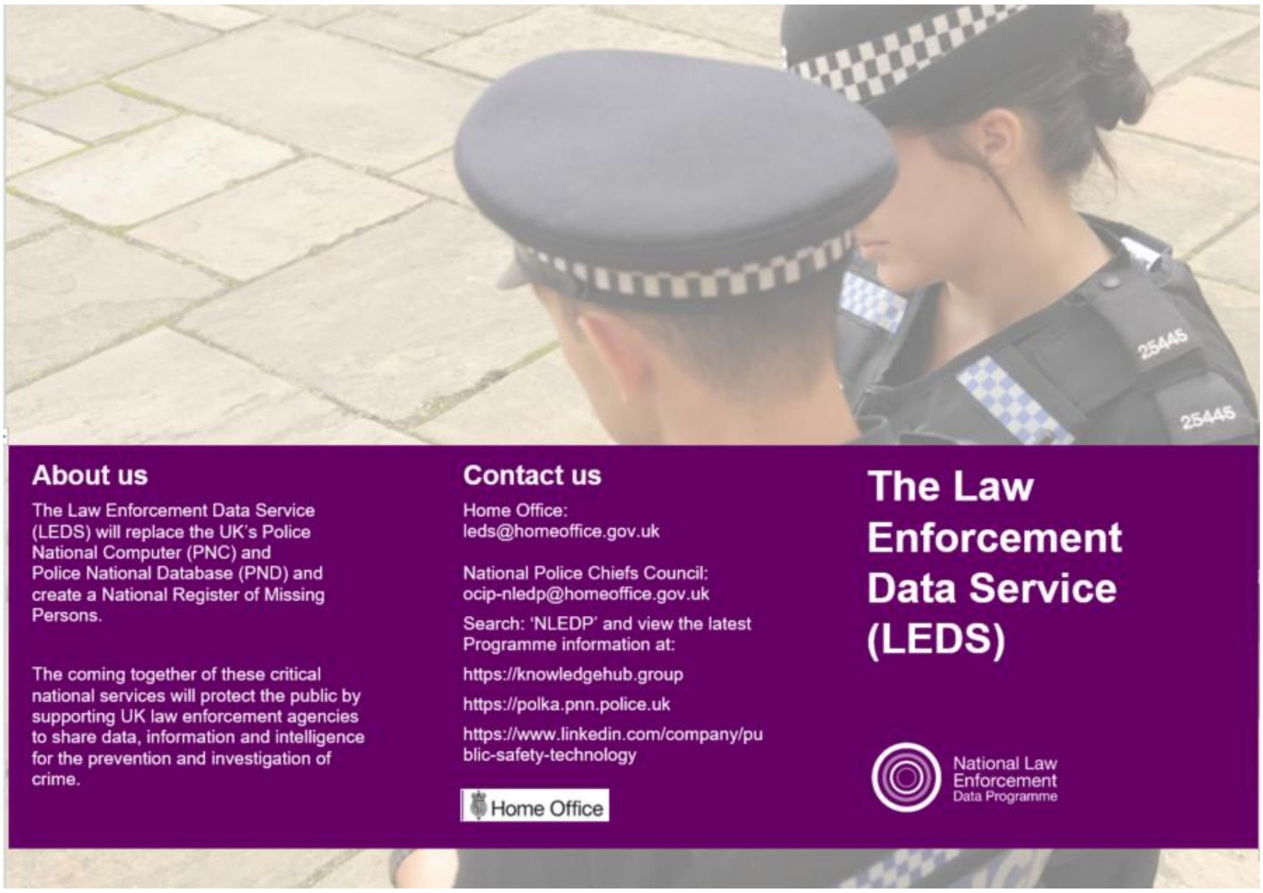
National Law Enforcement Data Programme (NLEDP)

Programme Brief



About us

The Law Enforcement Data Service (LEDS) will replace the UK's Police National Computer (PNC) and Police National Database (PND) and create a National Register of Missing Persons.

The coming together of these critical national services will protect the public by supporting UK law enforcement agencies to share data, information and intelligence for the prevention and investigation of crime.

Contact us

Home Office:
leds@homeoffice.gov.uk

National Police Chiefs Council:
ocip-nledp@homeoffice.gov.uk

Search: 'NLEDP' and view the latest Programme information at:

https://knowledgehub.group

https://polka.pnn.police.uk

https://www.linkedin.com/company/public-safety-technology

Home Office

The Law Enforcement Data Service (LEDS)

National Law Enforcement Data Programme

Director Data and Identity Directorate: [redacted]

Head of Data Policy Unit: [redacted]

Head of Data Strategy/Data Policy Unit: [redacted]

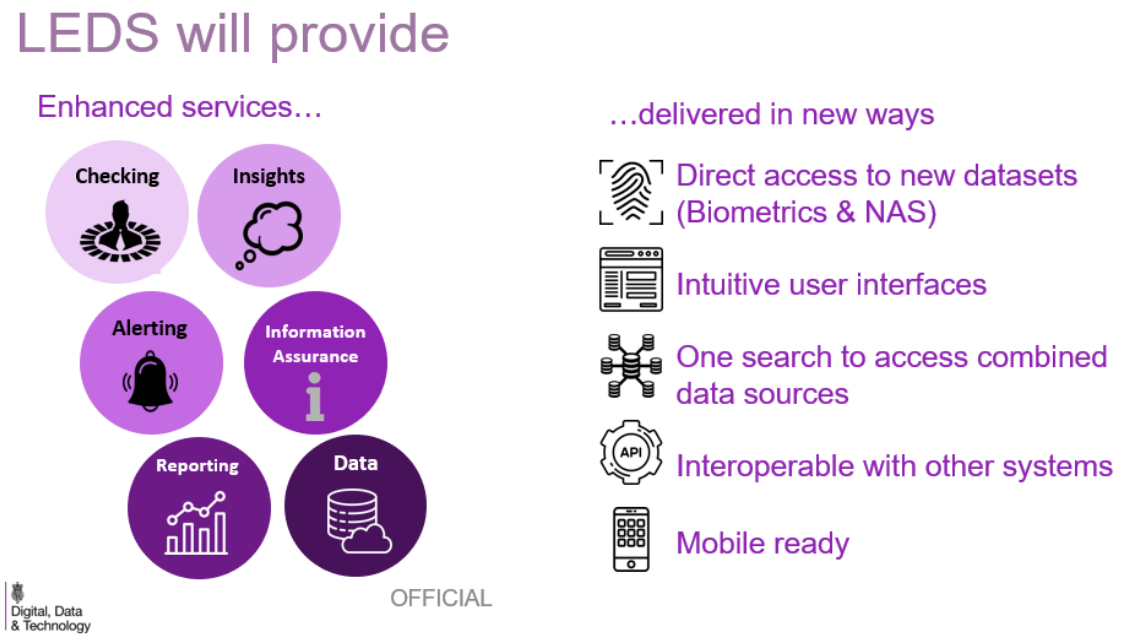
Data and Identity Directorate Policy Lead for NLEDP: [redacted]

Public Protection Portfolio Compliance Lead: [redacted]

LEDS Open Space Project Manager: [redacted]

LEDS Open Space Co-ordinator: [redacted]

1. The National Law Enforcement Data Programme has been established to protect the public by building a modern and affordable Law Enforcement Data Service to replace, the Police National Computer and the Police National Database and to create a National Register of Missing Persons.



LEDS will provide

Enhanced services…

Checking

Insights

Alerting

Information Assurance

Reporting

Data

…delivered in new ways

Direct access to new datasets (Biometrics & NAS)

Intuitive user interfaces

One search to access combined data sources

Interoperable with other systems

Mobile ready

Digital, Data & Technology

OFFICIAL

2. The enhanced services in scope for LEDS feed into one of these 6 Business Services:
   - **CHECKING** – check background information, check custody status, verify identify, check historic threats and warnings.
   - **ALERTING –** alert management, alert presentation. Ability to set up alerts to be told automatically when a record has been changed; scaling up existing PND functionality and making it available across both data sets. A pilot is currently underway with Offender Managers to understand requirements and inform the design of the alerting capability.
   - **INSIGHTS –** Interrogate (search/explore), Analytics (Pattern, Predictive, Risk), Enrichment (associations) potential for predictive analytics, links with Management of Risk in Law Enforcement (MoRiLE).
   - **REPORTING –** standard Management Information, statistical reporting, user reporting.
   - **DATA –** matching, ingest (updates from forces “Updategrams”, direct data entry) and data management & compliance.
   - **INFORMATION ASSURANCE –** Audit, Authentication, Authorisation (Roles and Attribute Based Access Controls).

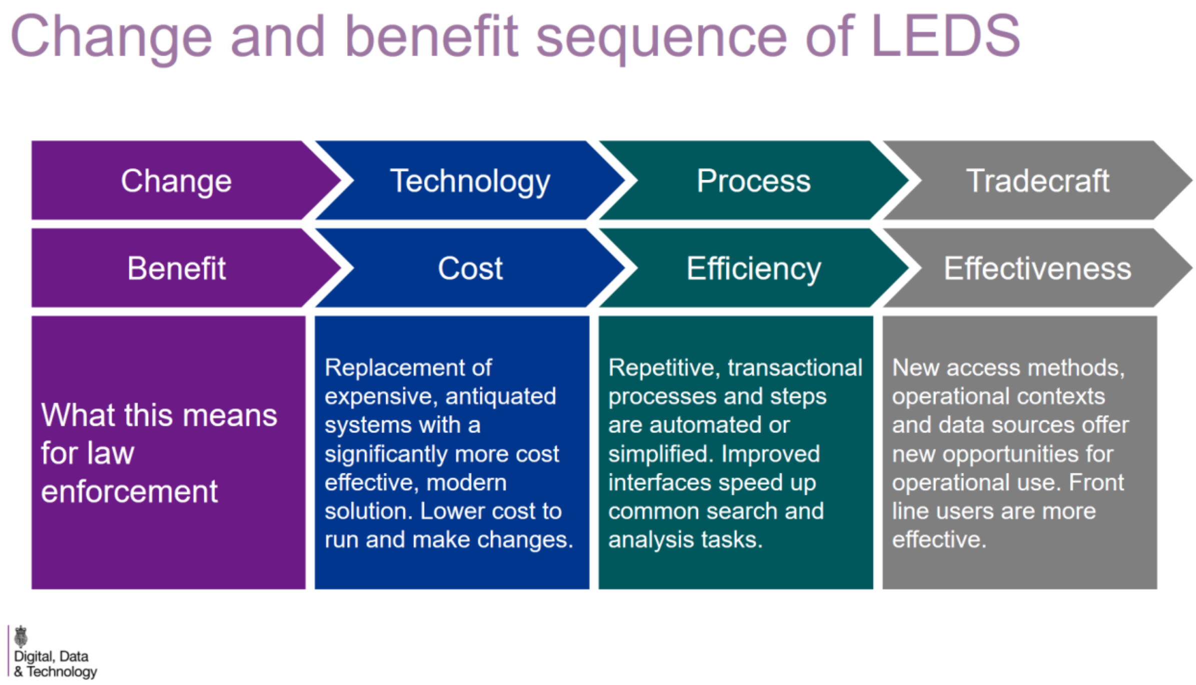
3. Since 1974 PNC has grown to be the backbone of UK policing in respect to everyday checks on identity, threat, status and background. PND has in a much shorter time become a critically important repository of information through which policing and other agencies can share vital intelligence and reports across force and agency boundaries.

4. There is now a clear need to update how these data services are delivered to law enforcement. PNC is 45 years old and needs urgent modernisation. Furthermore, dividing national data between two separate systems makes management of and access to information inherently inefficient and restricts the information that can be provided to police officers in operational situations. It is also costly to maintain two different systems. Some of the key issues that need addressing are:

    - Getting a single view of all the pertinent information relating to a person (and objects) across the two systems is a time-consuming manual process that isn't suitable for immediate front-line checks for emergency responses.
    - The systems (PNC in particular) are not easily or affordably adaptable to meet the changing demands or priorities of law enforcement or new legislation. For instance, constraints have made it difficult to evolve PNC to support the safeguarding of vulnerable individuals (an example of this is that it does not retain data about historic missing person events).
    - PNC is at the end of its life and the skills and knowledge required to manage it are becoming increasingly limited with security vulnerability growing because of the age of the technology it is delivered through.
    - While some PNC and PND data can be accessed on mobile devices, current connectivity limits the extent to which the data can be utilised at the point of need.
    - Current user interfaces are not intuitive, meaning lengthy training sessions are required to get the most out of the PNC and PND. This training commitment is difficult and expensive to maintain. Intuitive and efficient data services, such as those commonly deployed on smart phones or through modern web applications, are required employing up to date design approaches that optimise the user experience. By contrast PNC requires users to look through many different screens to view information that could easily be consumed on a single concise page.
    - PND has made steps to support automated alerting to users about new events relating to people of interest, such as offenders being managed back into the community. There is great scope to develop this further across all the national data, which will support early proactive intervention as and when the information that might trigger intervention becomes 'known' and uploaded onto the systems.

5. Additionally, at present, there is no single system to record and share information about people who go missing. The National Law Enforcement Data Programme (NLEDP) is also working to deliver a National Register of Missing Persons (NRMP). This will provide a snapshot of live missing persons enquiries across police forces in England and Wales. It will help officers when they encounter a missing person particularly if that missing person is outside their home force area. The Pilot function of the NRMP is scheduled to Go-Live by the end of 2020

6. Placing all of this information into one system will not mean data is available for all users to search. While all the collections of data will be physically in one system, they will be logically separated with role-based access controls (RBAC) allowing user access only to the data and activities they are permitted to access.



Change and benefit sequence of LEDS

Change	Technology	Process	Tradecraft
Benefit	Cost	Efficiency	Effectiveness
What this means for law enforcement	Replacement of expensive, antiquated systems with a significantly more cost effective, modern solution. Lower cost to run and make changes.	Repetitive, transactional processes and steps are automated or simplified. Improved interfaces speed up common search and analysis tasks.	New access methods, operational contexts and data sources offer new opportunities for operational use. Front line users are more effective.

Digital, Data & Technology

7. LEDS is initially a technology refresh and platform replacement and we estimate more than £100m saving in PND/C running costs by FY30/31 if LEDS is implemented and utilised.

8. We are developing LEDS with people at the heart of it. When the technology element is completed we will focus on operational process streamlining and efficiencies in usability for the frontline. The business design teams have taken the proposed LEDS services out to end users (including those that use PNC or PND data indirectly) to explore the potential value of LEDS in a series of workshops to include how small time saving efficiencies can be developed in LEDS to improve the day to day life of users and the business. This should see better service to the public including better safeguarding of people and their data.

9. These sessions have focussed on the business scenarios and processes that are in place today and how LEDS could help those users by reducing the time taken to complete common tasks more quickly or effectively or improving operational outcomes with new capabilities.

10. The cost saving of decommissioning PNC and PND is significant, but the benefits go way beyond this. There’s a significant amount of additional value to be realised – such as including LEDS in new police officer recruit training, so they can be fully operational from day one in accessing data and using it correctly and effectively. Much of this however requires further collaboration and investment from police and other Law Enforcement Agencies (LEAs) to realise the full potential.

NLEDP in detail

11. The product elements that make up LEDS are shown in the diagram below.

Redacted picture

LEDS is a service that provides its subscribers with a fully supported data access capability and **LEDS Products are the mechanism through which the service is delivered. There are 9 candidate products currently being considered.**

- **My LEDS** - information about the user, for example their work interests or training status.
- **Search Tools** - capabilities to facilitate checking, enquiring, investigating and analysing.
- **Alerts -** New information about a person or event a LEDS user is interested in for example a missing person has been found or a registered sex-offender has moved into an area.
- **Training and User support -** A capability to provide a learning environment for end users combined with the ability to provide support for users in their use of the system.
- **Central services -** enable LEDS and user organisations to administer
    - **Data updates, Admin (general), Reporting, Audit and other Bespoke or Non-Standard Services (NSS)**

- A product is a discreet set of features, functions and data set that allows a targeted user group the ability to efficiently, effectively and compliantly perform a specific business operation.

- The product can be delivered by a user interface (i.e. an application) or through a system interface (‘API’) and often both.

- LEDS is made up of a series of products that provide data, these are underpinned and enabled by technology, and these products make up the LEDS service.

NLEDP current governance

12. The Home Office National Law Enforcement Data Programme (NLEDP) is classified as a major investment programme requiring approval of investment by the Home Office Portfolio and Investment Committee (PIC), acting as a sub-committee of the Home Office Executive Management Board. The Infrastructure and Major Projects Authority (IPA) also provides oversight throughout the life of the programme.

13. The overall governance structure including corporate, programme, supplier and external interfaces is detailed below.

Programme Board

14. The Programme Board has the following objectives:

    14.1. Replace the Police National Computer (PNC) and Police National Database (PND) with a single data service, the Law Enforcement Data Service (LEDS) and create a National Register of Missing Persons. This service will meet the needs of current PNC and PND users.

    14.2. The NLED Programme Board approves changes to scope and scheduling and provides feedback and guidance to the programme. The NLED Programme Board is chaired by the SRO and reports to the Home Office Digital Data and Technology Management Board and Strategic Capabilities Board.

    14.3. The **SRO is personally accountable to Parliament** for the success of the programme outcomes. The role of the Programme Board members is to provide expertise from their particular areas of responsibility, to support the SRO in any decisions he needs to make. The Non-Executive members also provide information to the board.

Programme Organisation Structure

15. The NLEDP Programme Leadership Team (PLT) makes decisions on the day to day running of the programme; non-operational decisions, approval of training and staff events – this is chaired by the Programme Director.

16. It provides the governance, authority and direction required to ensure alignment of NLEDP resources with the programme strategy, objectives and priorities and to optimise NLEDP investments. The Programme Director is the final decision authority and issues are escalated to the NLED Programme Board and/or the Senior Responsible Owner (SRO).

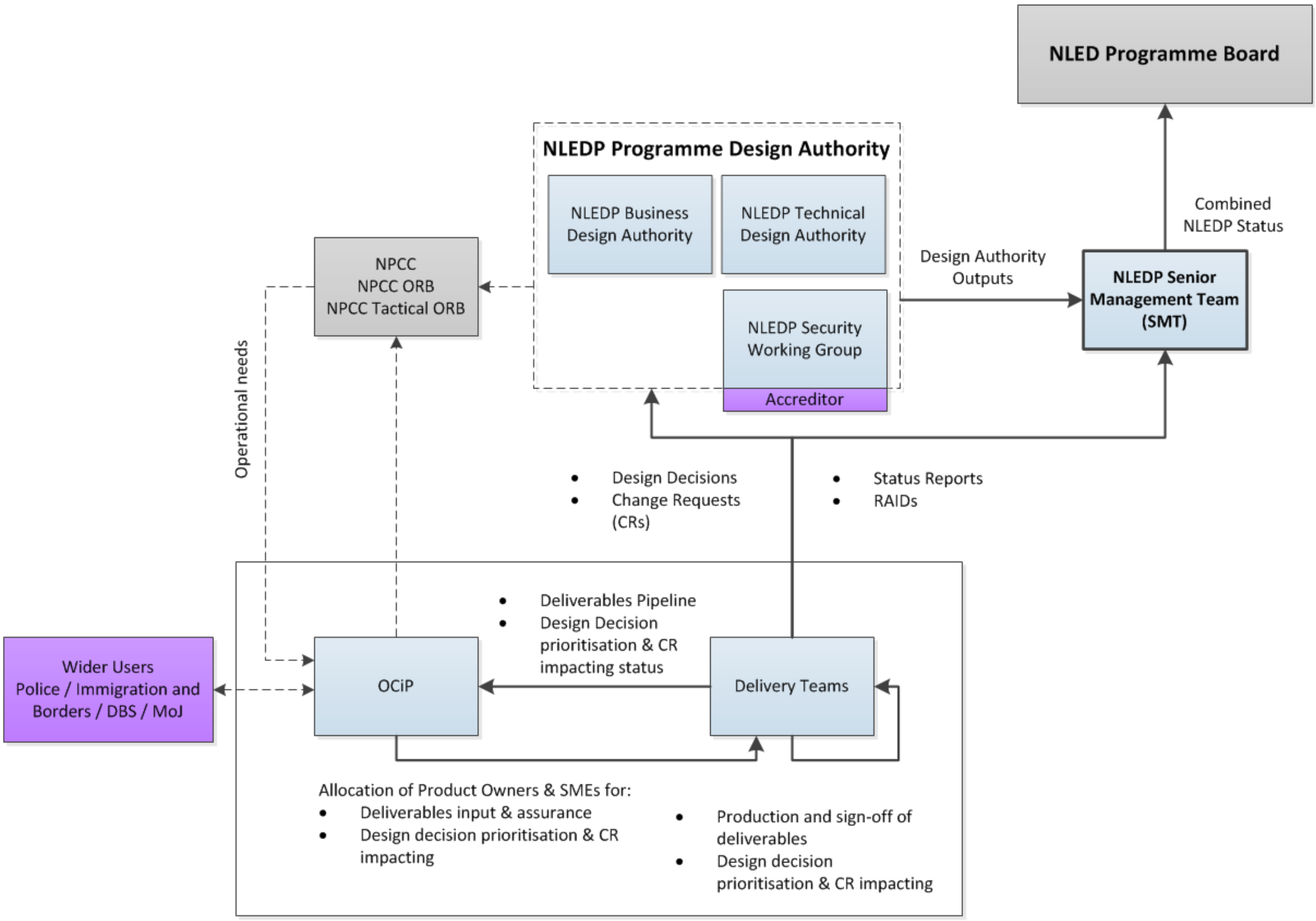
17. The NLEDP PLT accountable to the SRO, acts as the key escalation point for any programme risks and issues and has signing authority for spend and reports to the NLED Programme Board.

18. The **SRO (Senior Responsible Owner)** is directly accountable to the Chief Operating Officer and Parliament and has personal responsibility for delivery of the NLED Programme. The SRO is authorised to approve expenditure within the programme budget and to agree rescheduling. The SRO chairs and is supported by the NLED Programme Board.

19. The **NLED Programme Board** approves changes to scope and scheduling and provides feedback and guidance to the programme. The NLED Programme Board is chaired by the SRO and reports to the Law Enforcement Portfolio Board.

20. The **NLEDP Business Design Authority (BDA)** identifies, captures, develops and assures the business requirements; identifies, captures and tracks benefits; resolves business design and business architecture conflicts; and designs and maintains the target operating model. It reports to the NLED Programme Board and informs other wider Home Office BDA’s where appropriate.

21. **OCiP** (Operational Communication in Policing) operates as a business design authority to ensure there is a 'voice of the Police Service' within NLEDP. OCiP feeds into the NLEDP BDA with a clear police view on issues requiring deliberation. The Head of OCiP sits on the NLED Programme Board.


NLED Programme Board
NLEDP Programme Design Authority
NLEDP Business Design Authority
NLEDP Technical Design Authority
NLEDP Security Working Group
Accreditor
NPCC
NPCC ORB
NPCC Tactical ORB
Combined NLEDP Status
Design Authority Outputs
NLEDP Senior Management Team (SMT)
Operational needs
Design Decisions
Change Requests (CRs)
Status Reports
RAIDs
Deliverables Pipeline
Design Decision prioritisation & CR impacting status
Wider Users Police / Immigration and Borders / DBS / MoJ
OCiP
Delivery Teams
Allocation of Product Owners & SMEs for:
Deliverables input & assurance
Design decision prioritisation & CR impacting
Production and sign-off of deliverables
Design decision prioritisation & CR impacting

OCiP Governance Model

Programme Assurance

22. The programme is subject to oversight and approvals from PIC, Government Digital Service (GDS) and HM Treasury (HMT) and falls under the assurance activity of the Infrastructure and Projects Authority. In addition, the programme holds fortnightly meetings with IPA, Her Majesty's Treasury, Crown Commercial Service (CCS), Cabinet Office, GDS and PIC to provide updates and early engagement.

Governance/Assurance	Purpose	Frequency
Executive Management Board (EMB)	To ensure alignment to HO strategies and corporate objectives	Quarterly
Strategic Capabilities Board	Oversight of all HO programmes and projects	Every two months
Law Enforcement Systems Portfolio Board	To co-ordinate the direction of programmes and provide context across the Law Enforcement space	Quarterly
Portfolio and Investment Committee (PIC)	To review business cases, confirm the continuing viability of the investment and authorise requests for funding	Quarterly/As required
IPA/GDS/HMT/CCS and PIC	To regularly review progress to ensure successful programme delivery	Fortnightly
Project Valuation/Strategic Gateway Reviews	To provide an opportunity for the SRO and Programme Director to receive feedback on progress from independent assessors outside the Home Office	Annually
HMT TAP (Treasury Approval Point)	When required to release funds to the programme once business cases have been approved. TAP is a discretionary approval point for HMT and will not automatically be required for each business case iteration	Soon after approval of each business case by PIC (PBC)
Ad-hoc meetings with the PIC assessors	To ensure engaged and informed assessors, and to receive early indication of potential issues or problems	As required by the programme

Approval and Assurance Cycles

Information Assurance

23. The programme is implementing an Information Assurance Governance regime that aligns with the broader programme governance model and reflects the ‘lessons learnt’ from both IABS, IDENT1 and other Home Office programmes.

24. The focal point of the information assurance approach is the NLEDP Security Working Group (SWG) which is a cross system and multi-stakeholder group which has the responsibility to manage the risks and ensure effective controls are in place for the systems and data under NLEDP. It sits between the individual SWGs that are in place for each end system and the NLED Programme Board which is there as an escalation route.

25. Through the definition of a common approach the model addresses the challenges that arise from the differing risk appetites and approaches taken to IA governance by the customer base – the HO (through business leads and the SIRO command within HO Corporate Services), Policing (through NPCC, Police SIRO and the various business areas), and others.

NLEDP approach to privacy and ethics

26. All key documents will be discussed with Civil Society Organisations and also with the Independent Digital Ethics Panel for Policing and the Biometrics and Forensics Ethics Group.

27. A full annual Data Protection Impact Assessment (DPIA) is being written following the publication last year of the Privacy Impact Assessment. The DPIA will be discussed in advance with the Information Commissioner’s Office. This will consider the impact of LEDS on Privacy, Ethics and Data Protection as if the Home Office was a Controller of the Data. User Organisations will also be required to conduct an annual DPIA.

28. Prior to the start of LEDS the programme has engaged fully with a range of Civil Society Organisations on an open basis to bake in a range of different thoughts in the development of LEDS. An independent annual report of that process will be published.

29. A Code of Practice for LEDS users will be written, consulted on and published. The consultation will be open to members of the public and an associated guide will be written to enable public understanding of the implications of LEDS on their data and their rights.