LEDS and HOB Open Space:

LEDS and HOB Governance
V1.0

26 February 2019

Discussion Document

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention. It is to be circulated to and viewed only by members of the LEDS and HOB Open Space.

Governance inspection oversight

Purpose

To stimulate discussion about the governance supporting the Law Enforcement Data Service (LEDS) and the Home Office Biometric (HOB) Programme.

This paper will be discussed in the LEDS and HOB Open Space on 26 February 2019; the discussion will inform how Open Space views and input could be included in the future governance structure.

Summary

1. The Home Office Biometrics Strategy published in June 2018 described the current governance, oversight and standards in place to oversee the Home Office's use of biometric data. The strategy made a commitment to "develop options to simplify and extend governance and oversight of biometrics across the Home Office sector through consultation with stakeholders over the next 12 months". This review will cover both LEDS and HOB as the programmes develop and services operate.

2. Governance for HOB is already established for the biometric systems currently managed for policing (fingerprints) and immigration (fingerprints & face images), with oversight bodies in place; but is subject to the wider Home Office review and encourages stakeholder engagement. For LEDS, the governance regime is to be built over the coming months.

3. Following the brief discussion on governance at the 5 December workshop the areas that should be further discussed were:

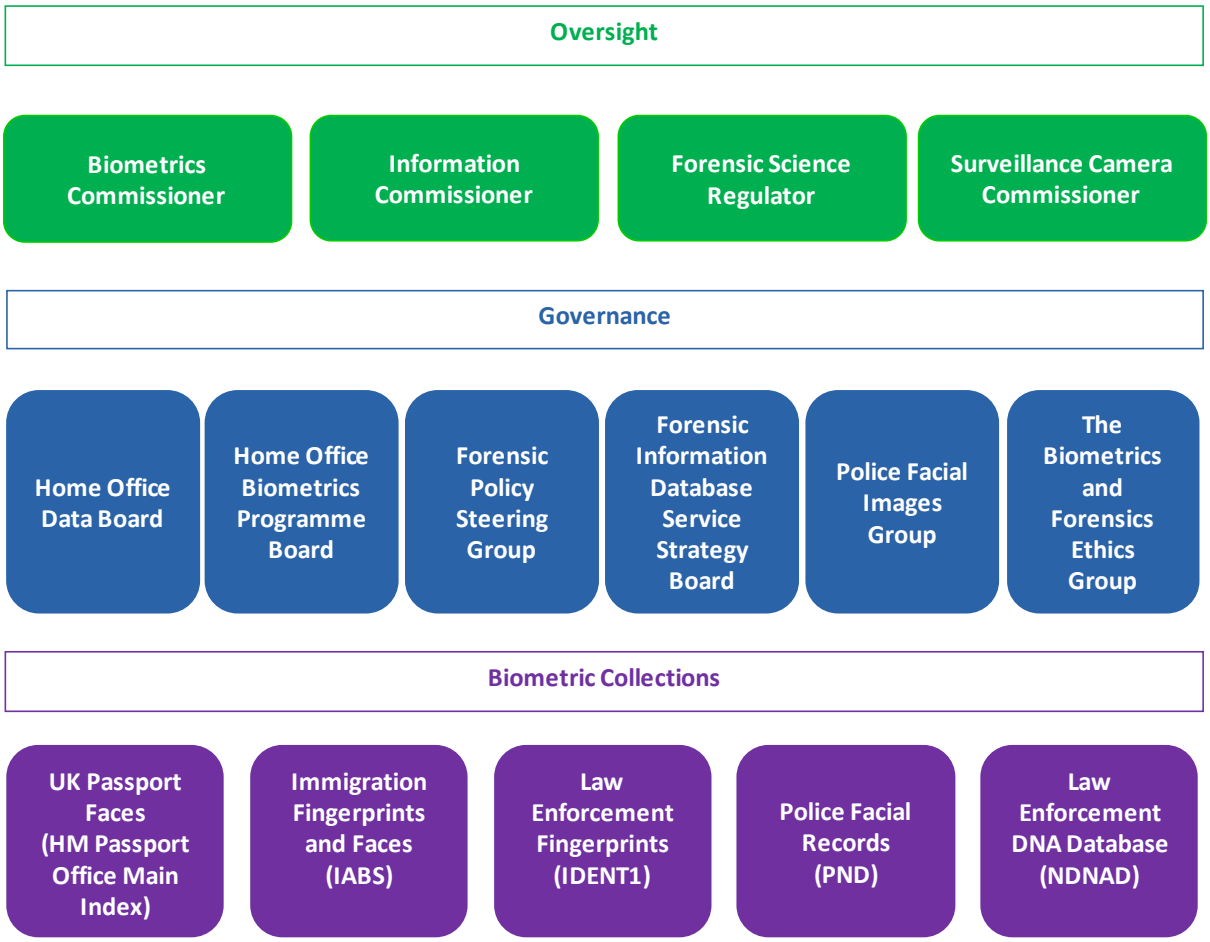
    a. Outcomes and how good governance should look – the subject of February's Workshop,
    b. What principles are needed for deciding on future changes/developments for adding new data/new access requests – to be discussed at a future Workshop.

4. This paper seeks to describe the current arrangements for Governance in HOB and the programme developing LEDS. It then goes on to describe potential changes for LEDS itself. Where possible LEDS will use the model proposed by HOB.

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention

HOB Governance

5. The overarching governance structure for biometric data is outlined in the following diagram. This shows the main governing bodies for biometric datasets and also the external oversight groups.



6. Governance arrangements vary between biometric modalities, reflecting the maturity of the technologies and with the organisation making use of the biometric data. The most mature arrangements are in the field of DNA and fingerprints in law enforcement. The 'FINDS-Strategy Board' (FINDS-SB) monitors the performance of biometric databases and provides oversight of how the police use their powers under Part V of PACE for the taking, use, retention and destruction of DNA samples and fingerprints. FINDS-SB also issues guidance to the police on the use of the databases in meeting the requirements of legislation

7. The governance framework within which HOB operates is broad-ranging with most of the key areas of the programme under additional governance outside the programme (as outlined above) and HOB must be aligned with external governance areas as follows:

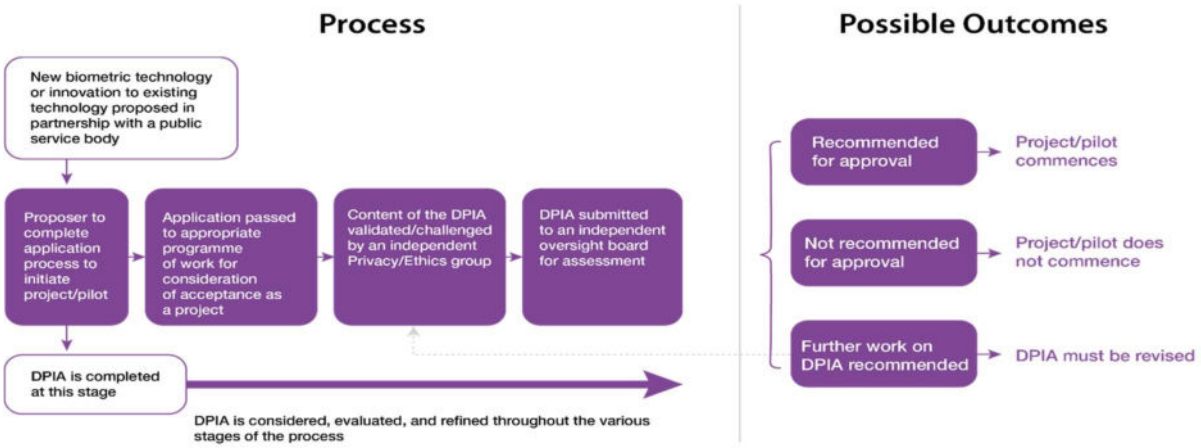
- Programme management (in addition to the HOB Programme Board)
- Commercial (e.g. Home Office policy, central government policy & strategy, EU competition and procurement laws, Government Digital Service, Portfolio Investment Committee, HM Treasury, etc)
- Technical approach, architecture and design (Home Office Technical Design Authority, Government Digital Service)

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention

- User requirements
- Stakeholder approvals/governance/sign off – by stakeholders' change Directors
- Immigration & citizenship Portfolio Board
- Law Enforcement Portfolio Board
- Border Systems Portfolio Board
- Forensic & Biometric Strategy Group
- Forensic Information Databases (FINDS) Strategy Board,
- Over 300 legal policy and compliance requirements.

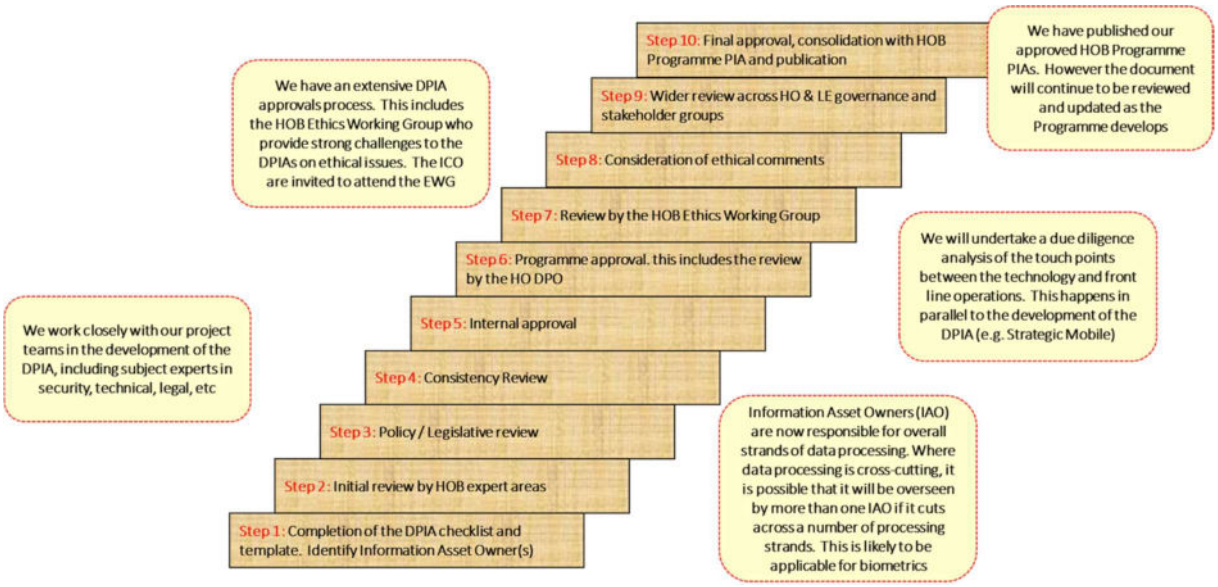
8. The Facial Images and New Biometric Modalities Oversight and Advisory Board, set up following the Home Office Biometric Strategy publication, provides government with policy recommendations relating to the use of facial biometrics and it will also be considering new biometric modalities at an early stage as they emerge in law enforcement. Representatives from the police, Home Office, the Surveillance Camera Commissioner, the Biometrics Commissioner, the ICO and the Forensic Science Regulator attend the board.

9. The Biometrics Strategy published last year outlined the continued emphasis on the completion of Data Protection Impact Assessments (DPIA) and, where appropriate these will be considered by the relevant groups including the recently established Home Office Data Board. Many future capabilities for Home Office and law enforcement use are technically feasible but the "ask" and justified use cases need to be developed by law enforcement with help from HOB and policy.



10. There is an extensive DPIA approvals process and HOB work closely with project teams in the development of the DPIA, including subject experts in security, technical and legal. This includes the HOB Ethics Working Group who provide strong challenges to the DPIAs on ethical issues. The Information Commissioner's Office (ICO) is invited to attend the Ethics Working Group.

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention



11. Other aspects of the governance that covers HOB are as follows:
    - The Commissioners and Regulators overseeing the use of biometrics are the Biometrics Commissioner, the ICO and the Forensic Science Regulator
    - Contract management of the HOB systems
    - Security architecture, coordinated through the HOB Security Working Group, working with suppliers and system accreditors
    - At an individual level, citizens are able to make Subject Access Requests which are managed by each organisation

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. A series of business cases will cover the entire investment by the programme, encompassing the component technology and business transformation work streams included within its overall scope.

14. The programme has adopted a blend of Managing Successful Programme (MSP), PRINCE2 and Scaled Agile practices to manage the overall investment and to achieve the planned outcomes and benefits where appropriate. The Scaled Agile approach has been adopted for the solution development as a mechanism to achieve the required outcomes in accordance with Government Digital Service (GDS) controls. This best practice approach centres around user research and service design by engaging with a broad range of users, analysing their experiences and tools. This will enable “user journeys” to be developed and inform the decision process around future requirements.

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

Programme Board

16. The Programme Board has the following objectives:

16.1. Replace the Police National Computer (PNC) and Police National Database (PND) with a single data service, the Law Enforcement Data Service (LEDS). This service will meet the needs of current PNC and PND users but also be offered to a wider set of organisations and provide access to other data sets and systems such as ANPR. The initial scope of the programme will be focused primarily on enhancing existing national data services, but future tranches will develop new capabilities.

16.2. 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.

16.3. 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

17. 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.

18. 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).

19. 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.

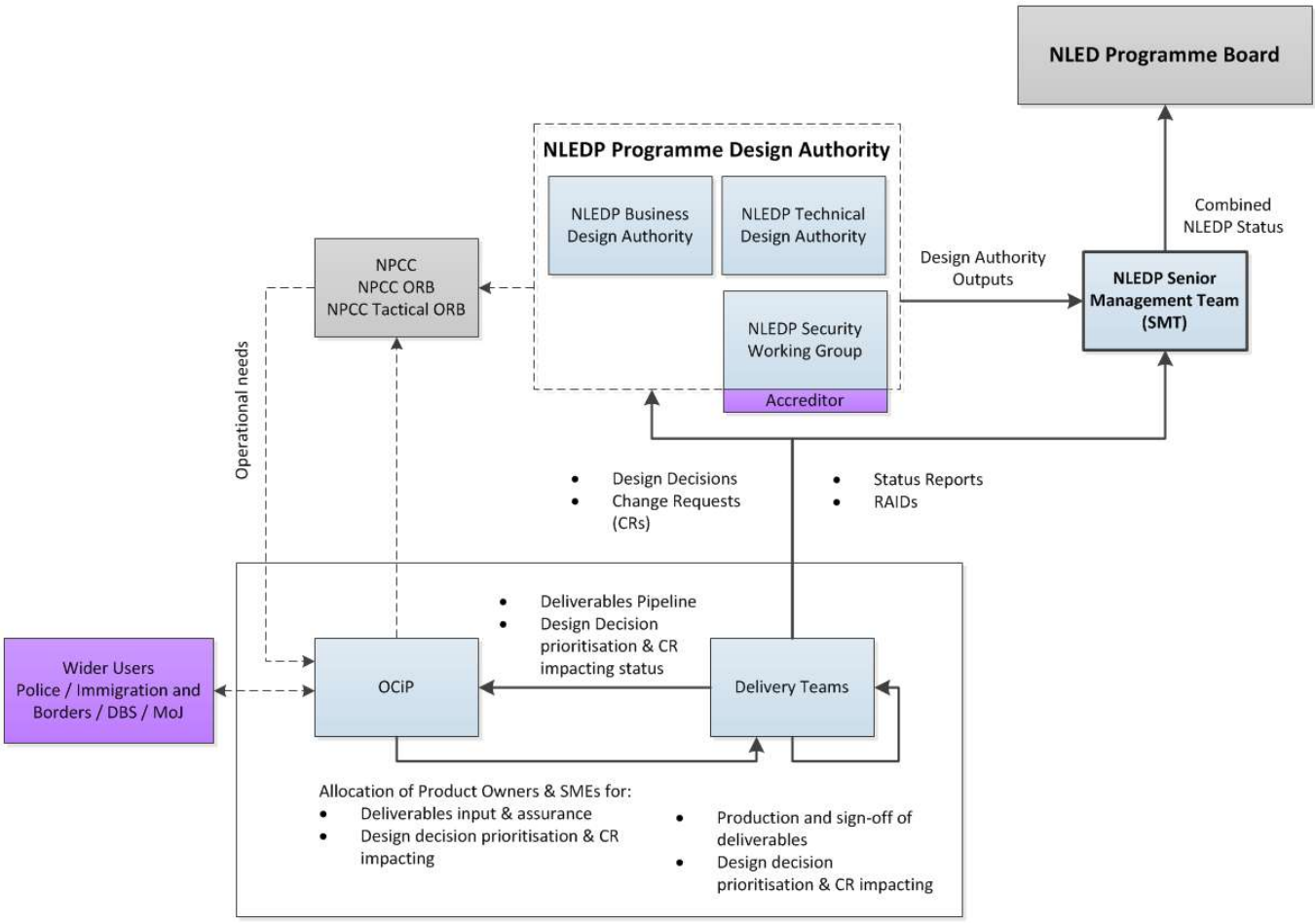
20. The **SRO (Senior Responsible Owner)** is directly accountable to the Chief Operating Officer and Parliament and has personal responsibility for delivery of the NLED Programme. The SRO is authorised to approve expenditure within the programme budget and to agree rescheduling. The SRO chairs and is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

21. 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.

22. 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.

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention

23. **OCiP** (Operational Communication in Policing) operates as a business design authority to ensure there is a 'voice of 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.



OCiP Governance Model

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention

Programme Assurance

24. 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

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention

Information Assurance

25. 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.

26. 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.

27. 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.

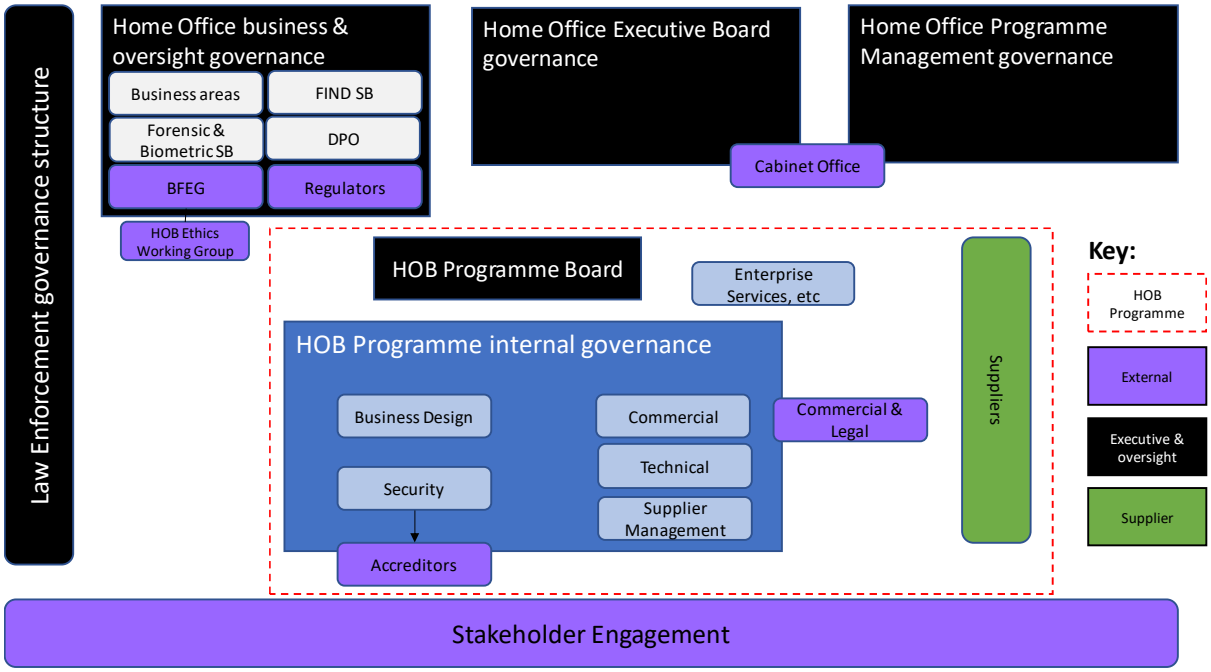
28. **Key questions for Open Space participants on the existing governance for LEDS and HOB are as follows:**

    - **Is this the kind of governance model that you would have expected?**
    - **Can you identify any gaps in the governance model and highlight what is missing?**
    - **At which points in the model would Open Space participants see their input being best placed?**

Future Governance

High Level Governance Model

29. Below is a high-level HOB governance model:



30. LEDS future governance is evolving and if possible, the LEDS governance should align to the HOB governance model where possible.

31. The existing respective governance of PNC and PND has evolved considerably since the inception of these systems. While broadly similar the different purposes, legislation, jurisdictions, contracts and funding create different reporting mechanisms. Both operate with their data controlled under the National Police Chiefs' Council's (NPCC) National leads, with the data processed by the Home Office and/or sub-contractors and under the oversight of Police's National Senior Information Responsible Owner (SIRO).

32. Under the planned LEDS Data Sharing Agreements (DSA), the broad user community for LEDS will, by agreement, delegate Data Control decision making to the nominated lead controller unless they require an exception on a specific decision. The lead controller in this role is termed the LEDS Controllers' Spokesperson.

33. Each organisation, as part of the information they need to provide to enable their access to LEDS, should complete a National Information Sharing Declaration (NISD) as part of their Data Sharing Agreement (DSA) to be signed by the organisation's Data Controller. This document specifies what data they can legally share with whom (organisationally) and any additional caveats related to roles including security clearance levels. This Data Sharing agreement will have organisation specific annexes specifying individual fields of each data record types that the organisation can have access to. Additionally, access controls will be placed on individuals within the organisation, not all individuals will be able to access all records that an organisation has access to. The process for monitoring and making changes to this will need to be established.

Roles

34. The LEDS Service Owner will be the Home Office's Director of Police and Public Protection Technology (PPPT). **The Service Owner will be directly accountable to the Home Office Permanent Secretary and Parliamentary Select and Audit Committees, as well as to the Police National SIRO** for matters impacting policing data and has personal responsibility for the availability of the LED Service. The Owner is authorised to approve expenditure within the delegated operating, maintenance and development/innovation budgets and to agree rescheduling.

35. Below is a list of example roles that each LEDS user organisation will need in order to comply with legislation:

- Data Protection Officer (named person) within each organisation responsible for that organisations use of the system of LEDS,
- Nominated data controller spokesperson (named person or role within an organisation). Responsible for how that organisation
- Data processor (named person or role within an organisation)

National Policies

36. LEDS is required to and requires its users to comply with various policies and rules that this non-exhaustive list includes:

- Example LEDS policies and agreements:
  - Code of Practice and associated public guide
  - National Information Sharing Agreements
  - Data Sharing Agreements

- Example external policies and legal requirements:
  - Amazon Web Services – Data processing policies
  - Data Protection Impact Assessments (DPIAs)
  - Data Sharing agreement(s) between Data Controllers

37. In addition to this LEDS operates in multiple jurisdictions including England and Wales, Scotland, Northern Ireland, Jersey, Guernsey and the Isle of Man. The Law Enforcement agencies in these jurisdictions are required to confirm their access to, use of and sharing of data on LEDS is legal and justified and in accordance with any local laws and practices.

38. Devolved administrations and respective Civil Society Organisations will be consulted for the Code of Practice.

Governance groups

39. LEDS will have two main types of Governance; Internal Governance Groups in the Home Office and External Governance groups outside the Home Office. An example internal governance body is the Police Live Services Board that is chaired by the Director of Police and Public Protection Technology. Example external bodies would be the NPCC IMORCC (Information Management and Operational Readiness Coordination Committee).

Holding to account

40. An example of holding to account could be that if a user is shown to be using LEDS in a way that is not consistent with its terms of use within the Code of Practice and other related documents, then that organisation or individual may have their access withdrawn, until their practices can be demonstrated as having been amended.

41. This will not preclude any separate sanction as determined locally in the case of an individual who is in material breach of the Code of Practice or related documents. The sanctions will range from mandatory retraining, and subject to investigations criminal and disciplinary proceedings.

Public Transparency

42. Greater transparency will aid holding to account (Appendix A contains a proposed timeframe for annual publication). We propose to make public the following reports and publications;
    - **Code of Practice** - to incorporate the operational principles and the behavioural standards required to use LEDS/PNC/PND. The Chief Constables of police forces in England and Wales will be legally required to take the Code into account. By itself the Code will not be legally binding on other organisations. However, all organisations that use LEDS will be required to sign up to the Code of Practice and commit to be bound by it and the Governance and Inspection regime.
    - **Data Sharing Agreement** - to provide a formal mechanism for sharing data through the LEDS platform. This will include organisations that have controller and processor status within one document. This will include a requirement to be bound by the Code of Practice, the governance and inspection regimes.
    - **Public Guide** - to provide a more detailed understanding of how LEDS will work, specifically providing a link between the **Code of Practice** and the daily and strategic **Operation of LEDS, and,**
    - **Annual Home Office report -** initially the focus will be on factual/statistical outcomes from LEDS. Over time this will include a forward plan of new and remedial work and a response to other reports.
    - **Data Protection Impact Assessment –** Full and detailed DPIA having been scrutinised by Civil Society prior to publication. With an accompanying Policy Equality Statement.
    - **Inspections report –** we would wish to see an annual report by the independent inspection regime. This will be subject to discussions between the Home Secretary and HMICFRS.
    - We are also proposing an **Annual Civil Society/Academic public report –** to provide for greater public scrutiny of plans and LEDS performance. Driven by engagement through the Open Space and other meetings as required. We are planning on holding periodic Ministerial meetings with Open Space members to bolster confidence in the enduring nature of the process. To aid accountability we will design in the ability for academic access to selected LEDS statistics.

43. **Inspection** has traditionally focussed on the use made of the systems by end user organisations against expected standards. In relation to policing, Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service has a statutory responsibility to carry out inspections of the 43 territorial England and Wales police forces, plus the following national agencies and non-Home Office forces:

- National Crime Agency;
- Police Service of Northern Ireland;
- British Transport Police;
- Police forces of the armed forces;
- Ministry of Defence Police;
- Civil Nuclear Constabulary; and
- Her Majesty's Revenue & Customs.

43. In addition to this, at the request of the relevant dependency or overseas territory, inspections may take place of forces in British Overseas Territories and Crown Dependencies, such as Gibraltar. Similar voluntary inspection arrangements are in place with the Gangmasters and Labour Abuse Authority.

44. Specifically, PNC and PND inspections are conducted by HMICFRS for all organisations. The plan is for HMICFRS to continue this inspection role for LEDS. This will be expanded in future to more explicitly cover the provision of the services by the Home Office.

The inspection body

45. The nominated inspection body for LEDS is Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service (HMICFRS). As part of the Data Sharing Agreement all signatories to and users of LEDS will agree to abide by HMICFRS inspection policies and regime as well as to implement advice and guidance. These policies will need to be reviewed in the light of the Code of Practice, but the inspection will need to ensure performance against a given standard, and also questioning those standards and the ways of working.

46. The relationship between inspection, regulatory and oversight bodies such as, the Independent Office for Police Conduct (England and Wales), Police Investigations and Review Commissioner (Scotland), Police Ombudsman for Northern Ireland, and in certain circumstance Coroners, will need to be articulated in relation to LEDS.

The inspection regime

47. It is proposed, subject to changes by and agreement of HMICFRS, that
    a. Thematic inspections in addition to organisation specific inspections should be conducted. Those thematic inspections to be chosen independently by HMICFRS but delivered against a workplan with input from governance, oversight bodies and LEDS and an annual workplan of inspections published and followed up with an annual report,
    b. Explicit mapping between inspections, governance and oversight with required resources,
    c. Management Information functionality should be built into LEDS that specifically meets the needs of those thematic inspections,
    d. Interface between HMICFRS as the inspection body and the LEDS Live Service and Policy team is defined to ensure faster and more holistic change,

e. Understanding of which inspection organisation would take primacy for inspections of LEDS (as a service) in the event of an enquiry,
f. inspection of LEDS itself needs to be defined and brought into the routine regime,
g. The use of data by LEDS organisations including those that don't use their data well in comparison to other organisations,
h. The provision of the service by LEDS,
i. Quality of data uploaded including examples of data not being uploaded
j. Currency of data uploaded including examples of data being unduly delayed
k. Departures from the Code of Practice or areas where the Code of Practice might need to be changed or further clarified,
l. Significant or systemic areas of data sharing opportunities missed in comparison to the behaviours expected,
m. Role Changes for Commissioners or regulators and interactions with HMICFRS,
n. Data protection breaches brought to the attention of the Information Commissioner's Office and reports on the mitigations and remedial actions,
o. Noteworthy practice that should be disseminated,
p. Areas of concern including suggestions for changes to training,
q. Future thematic inspection plans.

Key questions posed by this paper

1. **How will the Home Office and Civil Society know if the governance is working?**
    a. What outcomes do we expect?
    b. Do we think the governance model described above can deliver these outcomes?
    c. Are there any critical steps which are missing?
        i. For Governance?
        ii. For Inspection?
    d. Is the role of external actors (including civil society) identified correctly?
    e. At what points in the model do we think public input would be most effective?

2. **Structure – What are the governance/oversight gaps how could this be strengthened?**

    i. Is the routine engagement by the Open Space group at a Ministerial level of engagement the correct approach? Why?
    ii. If more programmes or systems (thematic) are represented should the routine engagement be at a Parliamentary level?
    iii. Would civil society be interested in producing an annual (or other frequency) report as outlined on p.12? What conditions would need to be satisfied for this?

3. **Will there be sufficient public understanding?**

    i. Will the public be sufficiently informed?
    ii. What is needed to cut through the complex issues?
    iii. How should the Home Office and Law Enforcement respond to public concerns?
    iv. People & Culture - How is trust established and managed (behaviours & redress)?
        a. Openness? Is it better to have expert analysis published with the statistics?
        b. How is challenge provided if standards are not met?

This Document has been written to stimulate discussion on the governance for LEDS and HOB. It is not a statement of Home Office policy or intention

Appendix A – Proposed Timeline for Publicly Published Reports On Governance

2019	**September**	**Academia** driven by civil society engagement in the Open Space. Academic holds the pen receiving direction from Open Space on the summary of issues discussed and resolved, discussed and not resolved, and outstanding issues that still require work. **Objective - start the public debate for the Public Consultation and inform the input into the Practitioners thoughts on the Code of Practice.**
	October	**Home Office** working in partnership with the College of Policing publish the draft Public Guide formal (practitioner) consultation. **Objective – Publish a guide for public consumption that details the expected standards, how these should be interpreted and what impact these standards might have to individual data subjects.**
	October	**Home Office** working in partnership with the College of Policing publish the draft Code of Practice formal (practitioner) consultation on Code of Practice published in public domain. **Objective – Publish a draft set of legal principles to become legally binding upon Chief officers in England and Wales and administratively binding on all LEDS Users.**
	November	**Home Office** publishes its DPIA updating the PIA that covers the PNC/PND/LEDS. **Objective – Legal requirement to write and to publish details of the DPIA.**
	November	**Home Office** publishes (limited) details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to aid understanding of the DPIA.**
	November	**Home Office** publishes Policy Equality Statement details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement to aligned to the DPIA. With sufficient details to aid understanding of the DPIA.**
2020		
	June	Code of Practice Public consultation updated with comments received. **Objective - conclude the public debate on the Code of Practice with a three-month consultation especially about National Register of Missing Persons**
	June	Public Guide to assist understanding of the Code of Practice consultation updated with comments received. **Objective - conclude the public debate on the Code of Practice/Public Guide with a three-month consultation especially about National Register of Missing Persons**
	September	**Academia** driven by civil society engagement in the Open Space. Academic holds the pen receiving direction from Open Space on the summary of issues discussed and resolved, discussed and not resolved, and outstanding issues that still require work. **Objective - start the public debate for the Public Consultation and inform**

		the input into the Practitioners thoughts on the Code of Practice. This links to the desire from Biometrics commissioner to start a public debate.
	November	**Home Office** publishes its DPIA (2020) updating the 2019 version updating on mitigating actions. **Objective – Legal requirement to write and to publish details of the DPIA.**
	November	**Home Office refreshes** publication of details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to aid understanding of the DPIA**
	November	**Home Office** publishes Policy Equality Statement details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to aid understanding of the DPIA**
	December	Parliamentary laying of updated Code of Practice and Public Guide
2021	**January**	NCA – Publish early stats on the National Register of Missing Persons
	June	Refreshed Code of Practice Public consultation updated with comments received. **Objective - conclude the public debate on the Code of Practice with a three-month consultation especially about Initial use of LEDS with PNC data**
	June	Refreshed Code of Practice Public consultation updated with comments received. **Objective - conclude the public debate on the Code of Practice with a three-month consultation especially about Initial use of LEDS with PNC data**
	September	**Academia** driven by civil society engagement in the Open Space. Academic holds the pen receiving direction from Open Space on the summary of issues discussed and resolved, discussed and not resolved, and outstanding issues that still require work.
	November	**Home Office** publishes its DPIA (2021) updating the 2020 version updating on mitigating actions. **Objective – Legal requirement to write and to publish details of the DPIA.**
	November	**Home Office refreshes** publication of details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to aid understanding of the DPIA**
	November	**Home Office** publishes Policy Equality Statement details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to aid understanding of the DPIA**
	December	Parliamentary laying of updated Code of Practice and Public Guide
	February	
2022		**Home Office** report to refer to **(NCA)** full year National Register of Missing Persons statistics and narrative. Initial PNC in LEDS operation

	June	**Home Office** Refreshed Code of Practice Public consultation updated with comments received. **Objective - conclude the public debate on the Code of Practice with a three-month consultation especially about Initial use of LEDS with PND data**
	June	**Home Office** Refreshed Code of Practice Public consultation updated with comments received. **Objective - conclude the public debate on the Code of Practice with a three-month consultation especially about Initial use of LEDS with PND data**
	September	**Academia** driven by civil society engagement in the Open Space. Academic holds the pen receiving direction from Open Space on the summary of issues discussed and resolved, discussed and not resolved, and outstanding issues that still require work.
	November	**Home Office** publishes its DPIA (2022) updating the 2021 version updating on mitigating actions. **Objective – Legal requirement to write and to publish details of the DPIA.**
	November	**Home Office refreshes** publication of details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to aid understanding of the DPIA**
	November	**Home Office** publishes Policy Equality Statement details of law enforcement user organisations and the purposes for which they use PNC and PND. **Objective – Legal requirement aligned to the DPIA. With sufficient details to understanding of the DPIA**
	December	Parliamentary laying of updated Code of Practice and Public Guide
2023	**February**	**Home Office** report to refer to **(NCA)** full year National Register of Missing Persons statistics and narrative. Full year of PNC data in LEDS operation and partial PND in LEDS operation.