

DIRECT DEMOCRACY & SORTITION ASSEMBLIES

A Civic Architecture for the British Isles

DDSA-CPF-001 | Edition 1.0

Civic Policing Framework

Policing by civic compact — accountable, proportionate, and grounded in the consent of the communities it serves

DOCUMENT INFORMATION

Version: 1.0

Author: Ian R. Graham

Document ID: DDSA-CPF-001

CLASSIFICATION

Confidentiality: Public Domain

Distribution: Unrestricted — For civic, academic, and public use

USAGE NOTICE & PERMISSION

This document is published by Direct Democracy & Sortition Assemblies (DD&SA) as part of its open civic corpus. It may be freely shared, quoted, adapted, and built upon for non-commercial civic, educational, journalistic, and research purposes, provided that attribution is given to DD&SA and the document reference number is cited. Commercial reproduction or use in partisan political campaigning requires prior written consent. This document does not constitute legal advice. All constitutional proposals are subject to democratic ratification processes as defined within the DD&SA framework. © DD&SA — Ian R. Graham. All rights reserved under applicable intellectual property law.

“We inherit the lessons of the past, not its chains.”

— DD&SA Founding Principle

dd-sa.org

A living document — subject to civic deliberation and democratic revision.

Contents

Document Status and Classification	6
Section 1: Constitutional Basis and the Policing Compact	6
1.1 The Nature of Civic Policing	6
1.2 Historical Context: What This Framework Rejects	7
1.3 The Non-Punitive Logic Applied to Policing	7
Section 2: Civic Policing Service — Structure and Governance	8
2.1 The Civic Policing Service	8
2.2 The Civic Policing Oversight Commission (CPOC)	8
2.3 The NIN Policing Record (NIN-PR)	8
2.4 CPS Staffing Principles and Ethics Architecture	8
Section 3: Enumerated Powers of Civic Policing Officers	9
3.1 The Enumeration Principle	9
3.2 Stop and Account	9
3.3 Power of Arrest	10
3.4 Powers of Search	10
Consensual Search	10
Search Incident to Arrest	10
Magister Search Warrant	11
3.5 Powers of Detention	11
Initial Detention Period	11
Extended Detention — Magister Authorisation	11
3.6 Powers of Entry	11
Emergency Entry Power	11
Welfare Entry	12
3.7 Use of Force	12
The Graduated Force Framework	12
3.7.1 Lethal Force — Absolute Conditions	12
3.8 Digital and Electronic Powers	13
3.9 Powers Regarding Children and Vulnerable Residents	13
Section 4: Forensic Evidence Architecture	13
4.1 The Civic Forensic Service	13
4.2 Chain of Custody Architecture	14
4.3 Digital Forensics — Write-Once Evidence Capture	14

4.4 DNA, Biometric, and Biological Evidence	14
4.5 Disclosure Obligations	14

Section 5: The Problem Defined — Historical Failures and the Lessons They Teach 15

5.1 The Fundamental Tension	15
5.2 The Parallel Construction Problem	15
5.3 Historical Models — Strengths and Failures	16
The US FISA Wall (pre-2001)	16
The Canadian CSIS/RCMP Model	16
The UK Public Interest Immunity (PII) Regime	17
The US Classified Information Procedures Act (CIPA)	17
The Diplock Court Model (Northern Ireland)	17
The German Trennungsgebot (Separation Principle)	17
The Israeli Military Court Disclosure Practice	18
The UK Special Advocate System	18

Section 6: The Intelligence Referral and Evidential Isolation Protocol (IREIP) 18

6.1 The IREIP — Purpose and Foundational Principles	18
6.2 Stage 1 — The Referral Decision	19
Who Makes the Referral	19
The Referral Document	19
ILO Assessment	19
6.3 Stage 2 — The Clean Team Principle	20
Structural Separation of the Investigation	20
The Independence Audit	20
6.4 Stage 3 — The Magister-Led Disclosure Assessment	20
The Disclosure Assessment Process	20
6.4.2 The Independent Evidence Counsel (IEC)	21
6.5 Stage 4 — Proceedings Management Under CEPO	21
What the Defence Receives	21
In Camera Hearings	22
Three-Magister Panel Requirement	22
6.6 Stage 5 — Post-Proceedings Intelligence Review	22

Section 7: Source Protection in Proceedings 23

7.1 The Legal Basis for Source Protection	23
7.2 The Graymail Defence — Prevention Architecture	23
Level 1 — Pre-charge Disclosure Assessment	23
Level 2 — In-Proceedings Management	23

Level 3 — Absolute Bar on Case Abandonment by Executive Decision	24
7.3 Covert Human Intelligence Source (CHIS) Handling in Proceedings	24
Source Evidence — When Admissible	24
Source Evidence — Inadmissible Pathways	24
Witness Identity Protection	24
Section 8: The Classified Evidence Protocol — Detailed Architecture	25
8.1 Overview	25
8.2 Classified Evidence Categories	25
8.3 The Substitution Standard	25
8.4 Emergency Classification Claims	25
Section 9: Community Policing Architecture	25
9.1 The Community Policing Model	25
9.2 Proportionality in Community Engagement	26
9.3 Early Intervention and Referral	26
Section 10: Civic Custody Architecture	27
10.1 The Philosophy of Civic Custody	27
10.2 Civic Custody Centres	27
10.3 Custody Record	27
10.4 Interview Architecture	27
Section 11: Specialist Operations	28
11.1 Civic Tactical Response Units	28
11.2 Undercover Operations	28
11.3 Surveillance Operations	29
11.4 Serious Organised Harm Investigation	29
Section 12: Accountability Architecture — Complete Specification	29
12.1 Layered Accountability	29
12.2 Individual Complaint Architecture	29
12.3 Pattern Monitoring and Systemic Review	30
Section 13: Failure Mode Analysis — Adversarial Stress-Testing	30
13.1 CPS Failure Modes	30
Failure Mode 1: Institutional Culture Drift	30
Failure Mode 2: Circumvention of the IREIP Through Informal Channels	31
Failure Mode 3: Magister Warrant System Gaming	31
Failure Mode 4: The Fair Trial Pressure Test — A Well-Resourced Defendant	31

Failure Mode 5: The Political Pressure Test — Elite Defendants	32
Failure Mode 6: The False Negative — Missing Genuine Threats	32

Section 14: Integration with the DD&SA; Constitutional Architecture 33

14.1 Instrument Crosswalk	33
14.2 Implementation Roadmap	33
14.3 The Authorial Statement	33

Document Status and Classification

EXECUTIVE SYNTHESIS

The Civic Policing Framework (DD&SA-CPF-001) establishes the complete architecture of policing in the Civic Commonwealth of the British Isles. It addresses three interrelated problems simultaneously. The first is structural: what does policing look like in a society premised on resident sovereignty, non-punitive logic, and sortition-based governance? The second is operational: how do the Civic Policing Service and the Internal Security Department (ISD) work together without either contaminating the other — specifically, how does intelligence gathered covertly under a Magister Warrant become admissible evidence in a transparent civic justice process, without destroying the intelligence source, corrupting the prosecution, or denying the accused a fair hearing? The third is adversarial: how does this architecture withstand the most sophisticated legal, political, and institutional challenges that the powerful, the well-resourced, and the determined can mount against it?

This Framework answers all three problems. On the first: policing in the NBI is a civic service, not a force. Officers serve residents rather than enforcing state authority upon them. Every power held by a Civic Policing Officer is specifically authorised, precisely bounded, and subject to independent oversight. On the second: the Framework establishes the Intelligence Referral and Evidential Isolation Protocol (IREIP) — a mechanism specifically designed to allow intelligence-derived investigations to produce admissible evidence without parallel construction, source exposure, or fair-trial compromise. It draws on the most robust elements of historical models — the Canadian CSIS/RCMP referral architecture, the US Classified Information Procedures Act, the UK Public Interest Immunity regime, the German Trennungsgebot (separation principle), and Israeli military court practice — while rejecting every element of those models that has been identified, in practice, as a vector for abuse. On the third: the Framework builds in adversarial testing as a design principle, not an afterthought.

The result is a policing architecture that is simultaneously more capable than its predecessor — because it is trusted, community-embedded, and constitutionally coherent — and more robustly accountable than anything that has existed in the British Isles. A Civic Policing Officer who abuses their powers does so in the certain knowledge that every action is recorded, every warrant is Magister-authorised, and every prosecution is subject to a disclosure architecture that will expose procedural misconduct. The accountability is not a constraint on effective policing — it is the condition that makes policing legitimate, and therefore effective.

PART I — CONSTITUTIONAL AND PHILOSOPHICAL FOUNDATION

Section 1: Constitutional Basis and the Policing Compact

1.1 The Nature of Civic Policing

Policing in the NBI is founded on a civic compact rather than a command relationship. The compact is as follows: Civic Policing Officers (CPOs) are residents who have taken on a specific civic role — the application of the minimum force and authority necessary to maintain safety, investigate harm, and bring those responsible for harm into the Civic Justice process. In exchange for that authority, CPOs accept the most stringent accountability obligations in the civic architecture, because the powers they hold are the most capable of causing harm when misused.

This compact is not a rhetorical device. It is structurally embedded in the architecture: CPOs hold specific, enumerated powers — not general authority; every use of significant power generates a mandatory NIN record; every CPO is subject to continuous ethics assessment; and the Civic Policing Oversight Commission (CPOC) has real-time access to the complete operational record of every policing action. A police force that holds power by institutional inheritance, which defines its own powers through operational practice, and that investigates its own misconduct is incompatible with the NBI constitutional order.

1.2 Historical Context: What This Framework Rejects

The policing architectures of the British Isles prior to the NBI were shaped by historical forces that are incompatible with the civic constitutional order. The English and Welsh model combined extraordinary legal powers (accumulated through the Police and Criminal Evidence Act, the Regulation of Investigatory Powers Act, the Investigatory Powers Act, and dozens of further statutes) with structural accountability deficits: police forces that self-investigated misconduct, complaint systems without real powers, and an intelligence–law enforcement interface so compromised by informal practice that parallel construction — fabricating the legal discovery trail of intelligence-derived investigations — became operationally routine.

The Metropolitan Police’s history of institutional racism (documented by the Macpherson Report, 1999, and the Casey Review, 2023), the Special Branch’s decades of political surveillance of trade unionists, activists, and civic organisations, the systematic contamination of prosecutions through undisclosed intelligence, and the use of undercover officers in relationships with those they were investigating — all of these represent structural failures of architecture, not simply individual misconduct. This Framework addresses the architecture. Individual misconduct is addressed by the consequence pathways. Both are necessary.

The Scottish, Northern Irish, and Channel Islands policing traditions each offer elements of better practice — community policing models, different approaches to discretion, alternative prosecution frameworks. This Framework incorporates the strongest elements of each while resolving their common failure: the absence of a constitutional framework that makes accountability structural rather than aspirational.

1.3 The Non-Punitive Logic Applied to Policing

The DD&SA non-punitive principle holds that rule-breaking is a system failure, not primarily a moral failure of the individual. This principle does not mean that harmful conduct has no consequences — it means that the consequences are restorative and structural rather than retributive and personal. Applied to policing, this produces a specific operational orientation: CPOs are not agents of punishment. Their role is to stop harm, investigate its causes, preserve evidence, and bring the process to the Civic Justice Architecture where the restorative response is determined. CPOs who use the powers of their office to punish, humiliate, or cause unnecessary harm to individuals are themselves causing harm and are subject to the same restorative consequence architecture.

This orientation has practical implications for how CPOs engage with residents. It does not mean that arrest powers, physical restraint, or detention do not exist — they do, and they are specified in Part III. It means that every exercise of those powers is assessed against a non-punitive standard: was this the minimum coercion necessary to achieve the legitimate civic aim? A CPO who uses more force than necessary, detains longer than necessary, or treats the subject of an investigation with contempt has departed from the civic compact.

Section 2: Civic Policing Service — Structure and Governance

2.1 The Civic Policing Service

The Civic Policing Service (CPS) replaces all legacy police forces operating in the British Isles — including the Metropolitan Police, Police Scotland, the Police Service of Northern Ireland, and all other territorial forces — in a single, constitutionally coherent body. The CPS is a national service organised into regional commands aligned with the NBI's Regional Sortition Assembly structure, with local community policing teams embedded within each Community Assembly area.

The CPS is not a military body and has no military command structure. Ranks are replaced by civic role titles that reflect function rather than hierarchy. The internal culture of the CPS is designed around the civic compact: every CPO understands that their authority derives from the resident body and is exercised on the resident body's behalf.

2.2 The Civic Policing Oversight Commission (CPOC)

The Civic Policing Oversight Commission (CPOC) is the permanent independent oversight body for the CPS. It is staffed through sortition, reports only to the National Sortition Assembly, and has real-time read access to the NIN Policing Record (NIN-PR) — the complete operational record of all CPS activity. The CPOC is not a complaints body — it is a structural oversight body. It monitors patterns of policing conduct across the entire CPS for systemic problems, not individual incidents alone.

The CPOC's structural access to real-time policing records is its most important feature. Legacy oversight bodies — the Independent Office for Police Conduct (IOPC), Her Majesty's Inspectorate of Constabulary — investigated incidents after they occurred, with access to evidence that the police themselves had compiled. The CPOC sees the record as it is made, cannot be denied access to any record, and identifies patterns before they become systemic.

2.3 The NIN Policing Record (NIN-PR)

All CPS activity — every stop-and-account, every arrest, every detention, every search, every use of force, every investigation action, every piece of evidence gathered — is recorded on the NIN Policing Record (NIN-PR). The NIN-PR is a public-access system, not a classified one. Subject to individual privacy protections for suspects and victims, all NIN-PR records are visible to any NBI resident through the NIN public portal. The CPS operates in a glass house by design.

The NIN-PR operates on a write-once architecture identical to the NIN-SIN: records are made once and cannot be amended, deleted, or altered. Corrections are made by new write-once entries linked to the original. The transparency of the NIN-PR is the primary deterrent to policing misconduct: an officer who abuses their powers does so in a record that is visible in real time to the CPOC, to the Magister system, and to any NBI resident who chooses to look.

2.4 CPS Staffing Principles and Ethics Architecture

CPS officers are recruited through an open, advertised process with clear competency requirements. Unlike the legacy model, CPS recruitment does not screen for "command presence" or physical dominance — it screens for emotional intelligence, community understanding, ethical reasoning capacity, and practical problem-solving. Physical fitness standards exist for roles requiring them, but physical capacity is not conflated with professional suitability.

All CPOs complete the DD&SA Civic Policing Ethics Programme (CPEP) before deployment — not a one-week induction, but a structured 12-month programme combining practical training with sustained engagement with the civic constitutional architecture, restorative justice practice, community embedding, and the specific legal framework governing their powers. CPOs who cannot demonstrate ethical reasoning capacity at the end of the CPEP are not deployed.

Five ethics principles apply to all CPS operations, parallel to those of the security services:

- Minimum Necessary Force — every coercive action uses only the minimum force or authority necessary to achieve the legitimate civic aim
- Impartiality — no CPO action is motivated by the personal characteristics, beliefs, or associations of the resident involved
- Legality — every CPO action has an explicit, specific legal basis in this Framework
- Accountability — every significant CPO action is recorded on the NIN-PR at the time it occurs
- Community Service — the CPO's primary orientation is service to the resident community, not enforcement against it

PART II — CIVIC POLICING POWERS

Section 3: Enumerated Powers of Civic Policing Officers

3.1 The Enumeration Principle

CPOs hold only those powers specifically listed in this Framework. This is not a common-law model in which general powers exist subject to specific limitations — it is a constitutional model in which no power exists unless specifically granted. The burden of justification falls on the exercise of power, not on its absence. A CPO who cannot identify a specific provision of this Framework authorising a specific action may not take that action.

Each power listed below is accompanied by: the specific trigger conditions that must be met before the power may be exercised; the specific limits on how the power may be exercised; the recording obligation that applies; and the review mechanism through which the exercise of the power is assessed. Powers without defined trigger conditions are not powers — they are blank cheques. This Framework issues no blank cheques.

3.2 Stop and Account

A CPO may stop a resident or visitor to the NBI and ask them to account for their presence or behaviour where the CPO has specific, articulable grounds for believing that account may reveal relevant information about an identified harm or imminent harm. "Specific articulable grounds" means the CPO must be able to state — on the NIN-PR record, at the time — the specific observation, intelligence, or information that led to the stop. "I was suspicious" is not articulable grounds. "I observed this person attempting to enter a secured area at 0300 having been seen at the same location on three previous nights" is.

Stop and account is not a power of compulsion — the resident is not required to answer. The CPO must inform the resident immediately that they are not obliged to answer and are free to leave at any time. If the resident does not wish to answer and wishes to leave, they may do so. A stop and account that becomes a detention against the resident's will requires arrest powers (Section 3.3).

Every stop and account is recorded on the NIN-PR within 30 minutes of the stop, whether or not the resident provided any information. The record includes: the time, location, and duration of the stop; the specific grounds; the outcome; and the self-identified demographic information of the resident if they choose to provide it. Aggregate stop and account data by geographic area, time period, and demographic is published on the NIN public portal monthly. Any pattern of stops disproportionately targeting residents on the basis of protected characteristics triggers automatic CPOC review.

3.3 Power of Arrest

A CPO may arrest a resident or visitor where:

- Condition A: The CPO has specific, articulable grounds for believing that the individual has committed, is committing, or is about to commit a Notifiable Harm (as defined in the NBI Civic Rules); and
- Condition B: Arrest is necessary because: the individual's identity cannot be established; or there is specific reason to believe the individual will cause further harm or leave the jurisdiction before investigation can proceed; or the harm alleged is of sufficient gravity that immediate protective action is required to prevent escalation

Both conditions must be met. Arrest on Condition A alone — because an offence may have occurred — is not sufficient. The necessity element (Condition B) must be independently established and recorded at the time of arrest.

On arrest, CPOs must immediately and clearly inform the individual: that they are under arrest; the specific reason for the arrest in plain language; that they have the right to a Civic Advocate; that they are not required to answer questions; and that they will be taken to a Civic Custody Centre. These obligations are not discharged by reciting a formula — the CPO must ensure the individual has actually understood, making reasonable adjustments for language, disability, or other need.

3.4 Powers of Search

Consensual Search

A CPO may search a person, vehicle, or premises with the free and informed consent of the person or owner. Consent must be actively given — absence of objection is not consent. The individual must be informed of what is being searched for and why before consent is sought. Consent may be withdrawn at any time and the search must stop immediately on withdrawal. A consent search and its outcome are recorded on the NIN-PR.

Search Incident to Arrest

On lawful arrest, a CPO may search the arrested person for items that may be used to cause injury, items that may facilitate escape, and items directly relevant to the reason for arrest. Search incident to arrest is limited to what is necessary for the specific purposes listed — it is not a general authority to search everything the arrested person has. Items found during a search incident to arrest that are unrelated to any of the three purposes may not be seized without a separate Magister-issued seizure order.

Magister Search Warrant

To search a premises or vehicle not subject to the above provisions, a CPO must obtain a Magister Search Warrant. The warrant application must specify: the premises or vehicle to be searched; the specific items being sought; the specific grounds for believing those items are on the premises; and the relevance of those items to a specific identified harm. The Magister may grant, grant with conditions, or refuse. All warrant applications and decisions are recorded on the NIN-PR. A refused warrant application cannot simply be re-submitted to a different Magister — refusal is recorded and the grounds for the original refusal must be addressed in any resubmission.

3.5 Powers of Detention

Pre-charge detention is the most significant power available to the CPS. It removes a resident's liberty without conviction or even charge. The NBI architecture treats pre-charge detention as an exceptional measure requiring continuous justification, not a routine investigative tool.

Initial Detention Period

Following arrest, a CPO may detain the individual at a Civic Custody Centre for an initial period not exceeding 12 hours. During this period, the individual must be offered: a Civic Advocate; notification of a person of their choosing; access to appropriate food, water, rest, and medical care; and access to any religious or cultural needs they identify. Detention is not permitted for the purpose of conducting interviews — interviews require the active cooperation of the individual or a separate, specific investigation power. Silence cannot be used as grounds for extending detention.

Extended Detention — Magister Authorisation

Where initial investigation cannot be completed within 12 hours, extension requires Magister authorisation. The Magister reviews the specific grounds for extension — what investigation is being conducted, why it cannot be completed, and why the individual's release would compromise it. Maximum extension periods are: 24 hours (Magister authorisation); 48 hours (Senior Magister authorisation, available only for the most serious harm categories); 96 hours absolute maximum (National SA Investigative Magister panel, available only in cases involving imminent threat to multiple lives or national security-linked serious harm under the CNSDF architecture).

Every extension decision is a new Magister assessment — not a rubber-stamp continuation of the previous. If the investigative grounds have not advanced in the intervening period, extension will be refused.

3.6 Powers of Entry

Entry onto private premises without the owner's consent requires either: a Magister Search Warrant (Section 3.4); an Emergency Entry Power (below); or specific statutory authority under this Framework for defined circumstances (welfare checks, hot pursuit).

Emergency Entry Power

Where a CPO has specific, articulable grounds for believing that a person on the premises is in immediate danger of serious harm and delay in obtaining a warrant would result in that harm occurring, the CPO may enter without warrant. Emergency entry must be recorded on the NIN-PR within 30 minutes. A retrospective Magister review of every emergency entry is conducted within 24 hours — not to validate the entry (it has already occurred) but to assess whether the power was properly exercised. Emergency entry that fails the retrospective review generates a CPOC referral.

Welfare Entry

Where a CPO has specific reason to believe that a resident at a specific address may be unable to request assistance due to health crisis, injury, or other incapacitating circumstance, the CPO may enter to conduct a welfare check. Welfare entry is the most limited entry power: the CPO may not search the premises and may not seize items. They may assess and assist the resident and call for any necessary emergency services. All welfare entries are recorded on the NIN-PR.

3.7 Use of Force

The use of force is the most ethically serious power available to a CPO. The NBI architecture treats force as a last resort requiring subsequent justification in every case, not a first option requiring subsequent justification only when something goes wrong.

The Graduated Force Framework

CPOs are trained in and must follow the Graduated Force Framework (GFF), which requires that force be escalated through the following levels only when each preceding level has been tried and failed or is clearly inapplicable:

- Level 1 — Presence and Communication: the CPO's presence and verbal engagement
- Level 2 — Soft Physical Control: guiding contact, non-restraint physical direction
- Level 3 — Restraint: physical restraint techniques designed to control without injury
- Level 4 — Intermediate Force: authorised non-lethal tools (baton, incapacitant spray) where restraint has failed and serious harm is imminent
- Level 5 — Lethal Force: available only in the specific circumstances in Section 3.7.1 below

A CPO who uses Level 4 or Level 5 force must file a Use of Force Report on the NIN-PR within 1 hour of the incident, regardless of whether the individual has been injured. CPOC review of all Level 4 and 5 force uses is automatic and mandatory.

3.7.1 Lethal Force — Absolute Conditions

A CPO may use lethal force only where all of the following conditions are simultaneously met:

- The CPO has specific, articulable grounds for believing that an individual poses an immediate threat of death or grievous bodily harm to a specific identifiable person or persons
- No lesser force option is available that could reliably prevent that harm within the time available
- The use of lethal force is proportionate to the specific threat identified

Lethal force may not be used: as a first or early resort; in pursuit (unless the fleeing individual continues to pose an immediate lethal threat to others, not merely an escape risk); against individuals who are incapacitated, restrained, or no longer posing an immediate threat; or against crowds or groups on the basis of the conduct of one member.

Every use of lethal force triggers an immediate mandatory review by a Magister, an automatic CPOC investigation, and referral to the Civic Justice Architecture. The CPO who used lethal force is suspended from active duty pending investigation — not as a punitive measure, but because the outcome of the investigation determines whether the use was lawful, and duty cannot continue in uncertainty.

3.8 Digital and Electronic Powers

The digital environment creates specific powers and specific constraints. CPOs do not have general authority to access digital devices, accounts, or records. Specific powers are as follows:

- Examination of a device with owner consent: permissible; consent must be freely given and withdrawal-capable; scope of examination limited to what the individual consents to
- Examination of a device incident to arrest: limited to checking for content directly relevant to the specific reason for arrest; no authority to examine all device contents
- Full device examination: requires a Magister Digital Evidence Warrant specifying the device, the specific content sought, and the investigative basis
- Access to cloud accounts, communications platforms, or third-party held data: requires a Magister Digital Evidence Warrant; service providers are required to comply with NIN-PR-recorded warrants within specified timescales
- Real-time communications interception: requires both a Magister Digital Evidence Warrant and an ISD Magister Warrant (as this overlaps with security service powers) — dual-warrant requirement prevents CPS from using security service capabilities without intelligence service involvement and separate judicial scrutiny

3.9 Powers Regarding Children and Vulnerable Residents

Children (under 18) and residents with cognitive impairments, mental health crises, or communication difficulties are subject to enhanced protections in all contact with the CPS. These are not discretionary adjustments — they are mandatory requirements:

- No child may be interviewed without an appropriate adult present — a parent, guardian, Civic Advocate, or trained appropriate adult volunteer
- No child may be detained in standard custody — specialist Youth Civic Welfare Suites are required for all youth detentions
- All interviews of children and vulnerable individuals are video-recorded in full, with the recording stored on the NIN-PR
- CPOs encountering residents in apparent mental health crisis must prioritise Civic Mental Care consultation over enforcement action wherever the immediate safety of others permits
- No child is charged without a specific Magister review of the appropriateness of charges given the child's age and circumstances

Section 4: Forensic Evidence Architecture

4.1 The Civic Forensic Service

The Civic Forensic Service (CFS) is operationally independent of the Civic Policing Service. Forensic evidence — physical, biological, chemical, digital, documentary — is collected, analysed, and reported by the CFS, not by CPOs. This independence is architecturally essential: forensic evidence whose collection and analysis is controlled by the prosecuting party is structurally compromised before it is tendered. The CFS answers to the Civic Justice Architecture — specifically to the Magister who has oversight of the relevant proceedings — not to the CPS.

The CFS operates to published, independently audited scientific standards. Its methods, protocols, error rates, and quality assurance procedures are published on the NIN public portal. Any technique

that does not meet published scientific standards cannot be used as evidence in civic proceedings. The "forensic science" failures of the legacy system — including the West Midlands Serious Crime Squad fabrication scandal, the Damilola Taylor forensic errors, and the widespread use of probabilistic forensic techniques whose error rates were systematically understated to courts — are addressed by the independence, transparency, and auditable standards of the CFS.

4.2 Chain of Custody Architecture

Physical evidence is subject to a continuous, unbroken, NIN-PR-recorded chain of custody from the moment of collection to the moment of presentation in proceedings. Every person who handles a physical exhibit: signs it in and out on the NIN-PR at the time of handling; records what they did with it and why; and confirms the integrity of the exhibit at transfer. Any gap in the chain of custody is disclosed to the defence and to the presiding Magister as a matter of obligation, not discretion. An exhibit with an unresolvable gap in its chain of custody is excluded from proceedings.

4.3 Digital Forensics — Write-Once Evidence Capture

Digital evidence is captured using write-once imaging protocols — creating bit-perfect copies of digital devices and storage media that cannot be altered. The imaging process itself is recorded on the NIN-PR, including the cryptographic hash of the captured image at the moment of capture. Any subsequent examination is conducted on the copy, not the original. The cryptographic hash provides an independently verifiable record that the examined copy is identical to the original capture. Tampering with a digital exhibit is detectable through hash verification and constitutes a serious civic justice integrity breach.

4.4 DNA, Biometric, and Biological Evidence

The NBI maintains a Civic Forensic Database (CFD) for DNA, fingerprint, and biometric records. The CFD operates under strict rules designed to prevent the surveillance-state use of biometric data:

- DNA profiles of individuals convicted of Notifiable Harms are retained on the CFD for a period proportionate to the gravity of the harm, specified in the Civic Rules
- DNA profiles of individuals arrested but not charged, or charged but not found responsible, are deleted from the CFD within 30 days of the conclusion of proceedings, unless a specific Magister retention order is made on specific public safety grounds
- No resident's DNA, fingerprints, or biometric data may be retained on the CFD without either their consent or a Magister retention order
- The CFD is subject to annual sortition-panel audit; audit findings are published on the NIN public portal
- Mass collection of biometric data — facial recognition sweeps, bulk DNA sampling — is absolutely prohibited without a National SA vote and specific Magister oversight framework

4.5 Disclosure Obligations

The disclosure of all evidence — including evidence that assists the defence — is a constitutional obligation of the CPS, not a strategic choice. The NBI disclosure architecture is more rigorous than any legacy model:

- All material gathered in the course of an investigation that is relevant to the proceedings — whether it assists the prosecution or the defence — is disclosed to the defence Civic Advocate as a matter of obligation

- The CPS Disclosure Officer is responsible for identifying all relevant material and must certify in writing that disclosure is complete; false certification is a civic integrity failure
- The Civic Forensic Service produces all forensic results in full to both the CPS and the defence simultaneously — there is no CPS-first model
- Where the CPS believes that specific material should not be disclosed on public interest grounds (see Section 8 — the Classified Evidence Protocol), the matter is referred to a Magister for a Disclosure Ruling — the CPS may not unilaterally withhold material
- Material withheld from disclosure under a Disclosure Ruling is reviewed by an Independent Evidence Counsel (Section 8.3) to confirm that the withholding is justified and not prejudicial to the fairness of proceedings

PART III — THE INTELLIGENCE-TO-EVIDENCE INTERFACE ARCHITECTURE

This Part is the architectural core of this Framework. The problem it addresses is one of the most technically difficult in the entire field of security law: how does a liberal democratic state use covertly gathered intelligence — obtained through methods that are not disclosed and from sources that cannot be named — to bring prosecutions that are fair, transparent, and capable of withstanding the most rigorous adversarial scrutiny? The answer requires a complete, end-to-end architecture. This Part provides it.

Section 5: The Problem Defined — Historical Failures and the Lessons They Teach

5.1 The Fundamental Tension

Intelligence work and legal proceedings operate on diametrically opposite principles. Intelligence work values secrecy: sources are protected, methods are concealed, assessments are provisional, and the evidentiary standards that apply to court proceedings — admissibility, confrontation, cross-examination — are structurally incompatible with how intelligence is gathered. Legal proceedings value transparency: the accused has the right to see and challenge the evidence against them, the source of every piece of evidence must be disclosed, and the reliability of evidence is tested through adversarial examination.

When a state attempts to use intelligence as evidence — or to allow intelligence to guide the gathering of evidence in ways that are not disclosed to the accused — it faces an insoluble dilemma if it has not built a proper architecture to resolve it. Disclose the intelligence fully and the source is burned, the method is exposed, and the intelligence architecture is degraded. Conceal the intelligence and the accused cannot properly challenge the basis of the case against them, rendering the proceedings fundamentally unfair. Legacy states have resolved this dilemma through a series of expedients that this Framework rejects categorically.

5.2 The Parallel Construction Problem

The most serious and most common abuse of the intelligence-to-evidence interface in legacy systems is parallel construction. Parallel construction occurs when law enforcement uses intelligence — gathered covertly, possibly unlawfully, in ways that cannot be disclosed — as a roadmap to build a legal case, and then fabricates or curates the legal discovery trail to conceal the intelligence origin of the investigation.

The US Drug Enforcement Administration's Special Operations Division, documented through Reuters investigations in 2013, routinely used NSA-derived signals intelligence to identify drug trafficking targets and then instructed law enforcement officers to "recreate" the discovery trail through ostensibly legal means — a traffic stop, a confidential informant, a border search — so that the intelligence origin was never disclosed in court. The targets' defence lawyers, judges, and juries never knew that the investigation had begun with covert surveillance that may itself have been unlawful.

Parallel construction is not a marginal abuse. It is the systematic corruption of the justice system by the intelligence system. It allows the state to avoid the warrant requirement (because the warrant-required intelligence is never disclosed), to avoid disclosure obligations (because the intelligence product does not formally exist in the prosecution file), and to avoid fair-trial scrutiny (because the accused's lawyers do not know what to challenge). It has been used against drug traffickers, terrorists, and — in states without adequate constitutional protections — against political opponents, journalists, and civic activists.

5.3 Historical Models — Strengths and Failures

The US FISA Wall (pre-2001)

The Foreign Intelligence Surveillance Act (FISA) system maintained a legal "wall" between intelligence-gathering on foreign agents and criminal prosecution. Intelligence collected under FISA could not be shared with criminal prosecutors except in defined circumstances. The wall was intended to prevent intelligence from contaminating prosecutions. Its failure was twofold: first, it was dismantled after 9/11 on the false premise that it had prevented intelligence sharing that could have stopped the attacks; second, even before its dismantling, it was gamed through informal channels. The lesson: a wall maintained by procedure alone, without structural enforcement, will be circumvented. The NBI architecture uses structural separation — not procedural walls — as its primary mechanism.

The Canadian CSIS/RCMP Model

The Canadian Security Intelligence Service (CSIS) gathers intelligence. The Royal Canadian Mounted Police (RCMP) prosecutes. A formal referral protocol exists between them. In practice, the protocol has been compromised repeatedly: CSIS withheld from the RCMP intelligence that would have assisted the defence (the Arar Commission findings); the RCMP used CSIS intelligence products in ways that were not disclosed to courts (the Air India trial); and the two services developed informal relationships that bypassed the formal protocol entirely. The lesson: a referral protocol between two organisations with shared objectives and overlapping personnel is not sufficient. The NBI architecture adds structural separation of personnel, independent oversight of every referral, and a mandatory disclosure mechanism that operates automatically, not on the initiative of the referring service.

The UK Public Interest Immunity (PII) Regime

UK courts developed the Public Interest Immunity mechanism to allow the government to withhold sensitive material from disclosure on the grounds that its disclosure would damage the public interest. In practice, PII has been used to conceal intelligence sources, protect police misconduct (the Hillsborough inquests), and shield government from embarrassment that has nothing to do with genuine national security. The mechanism places the withholding decision with the government, subject to judicial review. The lesson: judicial review of withholding is essential, but the judicial process must see the withheld material — not merely the government's assertion about it — to make a meaningful assessment. The NBI architecture requires the Magister to read the intelligence before deciding on withholding, and requires an Independent Evidence Counsel to assess the prejudice to the defence, independently of both the CPS and the intelligence service.

The US Classified Information Procedures Act (CIPA)

CIPA provides a mechanism for managing classified information in US federal criminal trials. It requires the government to notify defendants of classified information it intends to use, allows the court to review classified material in camera, and permits substitution of unclassified summaries for classified originals. CIPA is a genuine improvement over having no mechanism, but its weaknesses are instructive: substitution summaries can be so sanitised as to be useless to the defence; the defendant's security-cleared lawyer requirement creates access inequality (most defendants cannot afford security-cleared counsel); and CIPA is routinely used by the government to force defendants to accept inadequate summaries or face the abandonment of their case. The NBI architecture adopts CIPA's in camera review mechanism while addressing each of its specific weaknesses.

The Diplock Court Model (Northern Ireland)

From 1973, Northern Ireland operated a system of single-judge, non-jury trials — Diplock courts — for scheduled terrorist offences, on the grounds that jury intimidation and community pressure made fair jury trial impossible. The model removed one form of injustice (jury intimidation) while creating another (the concentration of conviction authority in a single judge whose assessments were not subject to collective scrutiny). The lesson is not that non-jury trial is categorically wrong — it may be genuinely necessary in specific circumstances — but that single-judge trial without structural safeguards is as vulnerable to capture as jury trial in a hostile environment. The NBI architecture provides, for the most sensitive cases, a three-Magister panel rather than a single Magister, with mandatory adversarial oversight by an Independent Evidence Counsel.

The German Trennungsgebot (Separation Principle)

Germany's Grundgesetz and subsequent constitutional jurisprudence developed the Trennungsgebot — the principle of institutional separation between intelligence services and the police. The constitutional court's concern was the experience of the Gestapo: a single body that combined intelligence collection, arrest powers, and prosecutorial authority had enabled totalitarian control. The Trennungsgebot requires that intelligence services may not hold arrest powers, and police may not conduct covert surveillance equivalent to intelligence-service operations. The NBI architecture adopts and extends this principle: the ISD has no arrest powers; the CPS has no covert surveillance powers beyond those specifically warranted. The interface between them is the formally governed IREIP, not a merged operational relationship.

The Israeli Military Court Disclosure Practice

Israeli military courts developed the "gist" disclosure model — providing defendants with a summary of the classified evidence against them sufficient for them to understand and challenge the case, without disclosing the full intelligence. The model has significant weaknesses in the military court context, where structural unfairness to defendants is well-documented. However, the "gist" principle — that a defendant must receive enough information to mount a meaningful defence, even if not every intelligence detail — is sound and forms part of the NBI architecture in a significantly strengthened form.

The UK Special Advocate System

In Special Immigration Appeals Commission (SIAC) proceedings and certain terrorism-related cases, the UK has used Special Advocates — security-cleared lawyers who can see the classified material but cannot communicate its contents to the defendant, effectively representing the defendant's interests in closed proceedings without the defendant's instructions. This model has been consistently criticised by the Special Advocates themselves, by the European Court of Human Rights, and by the Law Commission: a lawyer who cannot take instructions from their client is not effectively representing that client. The NBI architecture replaces the Special Advocate with an Independent Evidence Counsel whose role is specifically defined to avoid the conflict of interest inherent in the Special Advocate position.

Section 6: The Intelligence Referral and Evidential Isolation Protocol (IREIP)

6.1 The IREIP — Purpose and Foundational Principles

The Intelligence Referral and Evidential Isolation Protocol (IREIP) is the complete architectural mechanism through which intelligence gathered by the ISD may lawfully contribute to a CPS prosecution without contaminating the prosecution's evidential integrity, compromising the intelligence source, or denying the accused a fair hearing. It is built on three foundational principles derived from the historical analysis above:

- **Structural separation:** the intelligence and prosecution processes are physically and organisationally separated until and unless a Magister-governed disclosure decision connects them in a defined, recorded, and challengeable way
- **Mandatory independent oversight:** no element of the IREIP operates through bilateral agreement between the ISD and the CPS — every step requires independent Magister oversight or Independent Evidence Counsel assessment
- **Fair trial primacy:** where any element of the IREIP cannot be operated in a way consistent with the accused's right to a fair hearing, proceedings must be stayed, not continued on the basis of a compromised process

6.2 Stage 1 — The Referral Decision

Who Makes the Referral

Within the ISD, only the Director or Deputy Director (Operations) may authorise a referral to the CPS. Case officers and section heads identify referral candidates — individuals or activities where the intelligence picture suggests criminal conduct serious enough to warrant prosecution — but they do not make referrals. The Director-level authorisation requirement prevents referrals being made for operationally convenient rather than genuinely justified reasons.

Within the CPS, only the Intelligence Liaison Officer (ILO) may receive a referral. The ILO is the sole point of contact between the ISD and the CPS. No ISD officer communicates with any CPS officer other than the ILO on any matter relating to an active investigation or potential prosecution. The ILO has no investigative role in the CPS — they do not run operations, manage evidence, or participate in the prosecution process. They are a structural gateway, not an operational participant.

The Referral Document

The referral is a formal written document — the Intelligence Referral Notice (IRN) — that is simultaneously written to the NIN-SIN (classified, ISD side) and to the NIN-PR (classified, CPS side). The IRN contains:

- A statement of the harm category that the intelligence suggests has been or is being committed
- A summary of the intelligence basis — not the full intelligence, but sufficient for the ILO to assess whether prosecution may be viable
- A statement of what evidence, gathered independently of the covert intelligence, would be required to support prosecution
- A statement of what the ISD is and is not willing to disclose in proceedings, and why — the disclosure position, which is subject to Magister review at Stage 3
- An assessment of whether the intelligence source will need to be protected in proceedings and the mechanism proposed for doing so
- A statement that the referral has not been preceded by, and will not be accompanied by, any attempt to guide CPS investigative activity through intelligence without disclosure — the parallel construction prohibition certificate

ILO Assessment

The ILO reviews the IRN and makes a written assessment: whether the harm category is within CPS jurisdiction; whether independent evidence capable of supporting prosecution exists or can be gathered; and whether proceeding would require reliance on undisclosed intelligence in a way that could not be made fair-trial-compliant. If the ILO assesses that prosecution cannot proceed without reliance on undisclosed intelligence in a way that cannot be made compliant, the referral is declined and that decision is recorded on the NIN-PR. The ISD may seek Magister review of a declined referral.

6.3 Stage 2 — The Clean Team Principle

Structural Separation of the Investigation

Where the ILO assesses that prosecution may be viable, a Clean Team is constituted within the CPS. The Clean Team is the group of Investigation Officers who will conduct the independent investigation and, if proceedings result, manage the prosecution file. The defining feature of the Clean Team is what its members do not know: no Clean Team member has seen the ISD intelligence that gave rise to the referral. They have seen only what the ILO is permitted to share with them — the harm category and the nature of the suspected conduct, without the intelligence basis or source information.

The Clean Team principle, adapted from the US counter-terrorism prosecution model and strengthened against its known weaknesses, operates as follows:

- Clean Team members are selected by the Senior Investigation Officer without ISD involvement and without knowledge of the ISD's intelligence picture
- Clean Team members are prohibited from receiving any further communication from the ILO beyond the initial harm category identification until Stage 3 is completed
- Clean Team members are prohibited from discussing the case with anyone outside the Clean Team during the independent investigation phase
- The Clean Team conducts its investigation using only lawfully available investigative tools — overt inquiries, Magister-warranted searches, forensic analysis, witness interviews, open-source research, and its own surveillance under standard warrant
- The Clean Team's investigation is documented in full on the NIN-PR from the moment it commences — the NIN-PR record must be capable of demonstrating, at any subsequent point, that the investigation was conducted independently of the ISD intelligence

The Independence Audit

The CPOC conducts a mandatory Independence Audit of every Clean Team investigation prior to any charge being laid. The audit reviews: whether the NIN-PR record shows an investigative trail that is internally coherent and could plausibly have been generated without intelligence guidance; whether there is any evidence of contact between the Clean Team and the ISD beyond the formal ILO channel; and whether the evidence gathered is capable of sustaining prosecution independently of any classified material. An investigation that fails the Independence Audit does not proceed.

6.4 Stage 3 — The Magister-Led Disclosure Assessment

The Disclosure Assessment Process

Before charge, the CPS applies to a designated Classified Evidence Magister (CEM) — a specialist Magister with security clearance and specific training in the classified evidence architecture — for a Disclosure Assessment. The CEM is the first point at which the classified intelligence and the prosecution case are considered together in a judicial context.

The CEM reviews:

- The full ISD intelligence package — the complete picture, including source information, collection method, and all related intelligence — from the NIN-SIN, in a secure terminal environment
- The complete Clean Team investigation file from the NIN-PR

- The IRN, including the ISD's stated disclosure position
- The Independent Evidence Counsel's initial assessment (Section 6.4.2 below)

The CEM's task is to answer four questions:

- Question 1 (Contamination): Is there any evidence that the Clean Team investigation was guided by, or built upon, the ISD intelligence rather than conducted independently? If yes — proceedings are permanently stayed.
- Question 2 (Admissibility): Does the prosecution case, considered without any reference to the classified intelligence, contain sufficient admissible evidence to justify charge? If no — charge may not proceed.
- Question 3 (Disclosure obligation): Is any of the classified intelligence material that the ISD wishes to protect from disclosure "relevant" — meaning it tends to support the defence case or undermine the prosecution? If yes — the material must either be disclosed or the proceedings are stayed.
- Question 4 (Fair trial): Can proceedings be conducted in a way that is consistent with the accused's right to a fair hearing, given the classification constraints? If no — proceedings are stayed.

Where the answer to all four questions permits proceedings to continue, the CEM issues a Classified Evidence Protocol Order (CEPO) specifying exactly what classified material may or may not be disclosed, and in what form, during proceedings. The CEPO is binding on both the ISD and the CPS.

6.4.2 The Independent Evidence Counsel (IEC)

The Independent Evidence Counsel is a constitutionally novel role, specifically designed to address the most significant failure of the UK Special Advocate system. The IEC is a legally trained Civic Advocate who is security-cleared, has access to the full classified intelligence picture, and whose sole mandate is to assess the fairness of the disclosure position from the perspective of the accused — not to represent the accused (which would create the Special Advocate conflict of interest), but to independently advise the CEM on whether the disclosure position is consistent with fair trial.

The IEC's position differs from the Special Advocate in three critical ways:

- The IEC takes no instructions from the accused and has no relationship with the defence — this eliminates the impossible conflict of interest inherent in the Special Advocate model
- The IEC's assessment is provided to the CEM, not to the court — the IEC is an oversight mechanism within the Disclosure Assessment, not a participant in adversarial proceedings
- The IEC has a clear, single mandate: to determine whether the classified material, if the accused knew of it, could reasonably be expected to affect their ability to mount a meaningful defence. If yes, the IEC recommends disclosure or stay. The IEC's recommendation is published in anonymised form (redacting intelligence content) on the NIN-PR as part of the CEPO record.

IECs are selected from the senior Civic Advocate pool by sortition, security-cleared on appointment, and serve on individual cases rather than on a standing basis. Their opinions cannot be overridden by the CEM without written, published reasons — if the CEM disagrees with the IEC recommendation, that disagreement is part of the CEPO record and is subject to challenge by the defence.

6.5 Stage 4 — Proceedings Management Under CEPO

What the Defence Receives

Under the CEPO, the defence receives at minimum:

- Full disclosure of all evidence gathered by the Clean Team — without exception, including all material that assists the defence
- An intelligence summary — not the source or collection method, but sufficient factual content for the accused to understand the nature of any intelligence-derived allegation and to mount a meaningful challenge to it. The summary standard is the "meaningful challenge" standard: could a properly advised and represented defendant, having read the summary, effectively challenge the allegation? If not, the summary is insufficient.
- The existence and general nature of any classified material that has been reviewed but withheld — the defence knows that classified material exists and has been considered, even where its content is protected. There is no hidden material.
- The IEC's anonymised assessment, from which the defence can understand what assessment of fairness has been made on their behalf

In Camera Hearings

Where it is necessary for the Magister presiding over proceedings to consider classified material that has not been disclosed to the defence — for example, where the ISD is seeking to maintain a Magister-approved claim of source protection — this is done in a closed in camera session attended by: the presiding Magister panel (three Magisters for all classified proceedings); the CPS senior advocate; the IEC; and no one else. The defence is not present and receives instead a summary of what was determined, prepared by the IEC. The record of the in camera session is preserved in full on the NIN-SIN and is available to the NSA investigative process.

Three-Magister Panel Requirement

All proceedings that involve classified evidence under a CEPO are heard by a panel of three Magisters rather than a single Magister. This is the NBI's response to the Diplock court problem: the concentration of judgment in a single judicial officer is a structural vulnerability in any system, and most acutely in a system dealing with classified evidence where the Magister must make assessments that cannot be fully challenged by the defence. A panel of three provides collective scrutiny, reduces the risk of individual error or capture, and means that the classified material is assessed by multiple independent minds.

6.6 Stage 5 — Post-Proceedings Intelligence Review

After proceedings conclude — whether by finding of responsibility, stay, acquittal, or any other outcome — a mandatory Post-Proceedings Intelligence Review (PPIR) is conducted by the CEM and a CPOC observer. The PPIR assesses:

- Whether the IREIP was followed at every stage, or whether any deviation occurred and was properly documented
- Whether the IEC assessment proved accurate — i.e., whether the classified material that was withheld was correctly determined not to be prejudicial to the defence
- Whether the Clean Team investigation was genuinely independent — reviewing whether any intelligence information found its way into the investigation file in ways not authorised by the CEPO
- Whether the outcome of proceedings is consistent with what would have been expected without any intelligence involvement

PPIR findings are classified (NIN-SIN) but an anonymised summary is published on the NIN-PR. A pattern of PPIR findings showing consistent IREIP failures is referred to the NSA. PPIR findings from individual cases may be used in subsequent proceedings where the IREIP process from that case is directly relevant.

Section 7: Source Protection in Proceedings

7.1 The Legal Basis for Source Protection

The NBI recognises a specific, bounded privilege protecting the identity of human intelligence sources from disclosure in legal proceedings. This privilege is not absolute — it is subject to the overriding principle that proceedings must be fair and that material that is genuinely relevant to the accused's ability to mount a defence cannot be withheld regardless of its sensitivity.

Source protection privilege may be claimed by the ISD when a CEPO application includes intelligence derived from a human source. The claim is assessed by the CEM, not by the ISD. The ISD asserts the privilege; the CEM determines whether it is justified and whether its maintenance is consistent with fair trial.

7.2 The Graymail Defence — Prevention Architecture

Graymail — the practice by which a defendant threatens to disclose classified information in their defence as a means of forcing the prosecution to abandon the case rather than allow that disclosure — is a genuine strategic tool used by sophisticated defendants in intelligence-adjacent prosecutions. The NBI architecture addresses the graymail risk at three levels:

Level 1 — Pre-charge Disclosure Assessment

The Stage 3 CEPO process specifically identifies what classified material the accused would have a legitimate interest in disclosing and either authorises its disclosure in the proceedings or stays the case before it begins. A graymail threat can only operate where there is classified material that the prosecution needs to withhold but that genuinely assists the defence. The CEPO process resolves this before charge — if such material exists and cannot be disclosed, the case is stayed. There is no graymail opportunity because the dilemma has been resolved upstream.

Level 2 — In-Proceedings Management

Where a defendant in proceedings indicates an intention to adduce or elicit classified material in their defence — through questioning of witnesses, production of documents, or submissions — the presiding Magister panel immediately refers the matter to a CEM for emergency assessment. The CEM determines whether the proposed disclosure: is genuinely relevant to the defence; is already subject to a CEPO protection that has been properly assessed; or represents new intelligence material not previously reviewed. The defendant has an absolute right to adduce relevant evidence in their defence, and the graymail architecture does not override this — it ensures that the judicial assessment of relevance is made by an independent Magister with full access to the classified picture, rather than by the prosecuting service.

Level 3 — Absolute Bar on Case Abandonment by Executive Decision

In the NBI architecture, a prosecution may be stayed on fair-trial grounds by a Magister, but it may not be abandoned on operational security grounds by an executive decision of the ISD, the CPS, or the NSCC. The decision to stay proceedings belongs to the Magister. Where the ISD indicates that it would prefer the case to be abandoned rather than classified material disclosed, that preference is taken into account by the CEM in the CEPO assessment, but it does not determine the outcome. If the CEM determines that the material must be disclosed for fair trial, it must be disclosed — or the case is stayed by Magister order, not by executive preference. The separation of judicial from executive authority in proceedings is absolute.

7.3 Covert Human Intelligence Source (CHIS) Handling in Proceedings

Where a prosecution rests in part on intelligence provided by a CHIS — a human source recruited and handled by the ISD — specific additional protections and obligations apply.

Source Evidence — When Admissible

Information from a CHIS may contribute to a prosecution through the following mechanisms: the intelligence provided by the CHIS guided the investigation to independent evidence (Clean Team pathway, fully documented); the CHIS will testify as a witness under identity protection measures authorised by the Magister panel; or the CHIS's reports are used as intelligence-derived material subject to a CEPO, with the IEC assessing the fairness of non-attribution.

Source Evidence — Inadmissible Pathways

The following uses of CHIS-derived material are inadmissible under any circumstances and constitute automatic case-contamination:

- Presenting CHIS-derived intelligence to the court as if it were independent evidence gathered by CPOs
- Using CHIS-derived intelligence to identify and then fabricate a legal discovery trail (parallel construction — permanently stayed)
- Allowing the CHIS to give evidence without disclosing to the Magister that the witness is a managed ISD source
- Using CHIS-derived intelligence to obtain a Magister Warrant that could not have been obtained without that intelligence, without disclosing the intelligence basis to the Magister — warrant fraud, which is a criminal matter as well as a civic breach

Witness Identity Protection

Where a CHIS is willing to testify, the Magister panel may authorise specific identity protection measures: the use of a pseudonym; voice modulation; visual screening; giving evidence by live link from a separate location; or, in extreme cases, written evidence submissions without live testimony. Identity protection measures are authorised by the Magister panel after assessing the specific threat to the source's safety and the specific prejudice to the defence from each proposed measure. The accused's Civic Advocate is informed of the measures and may challenge their proportionality to the Magister panel.

Section 8: The Classified Evidence Protocol — Detailed Architecture

8.1 Overview

The Classified Evidence Protocol (CEP) is the complete framework governing the treatment of all intelligence-derived material in NBI civic proceedings. It operates alongside and through the IREIP. Where the IREIP governs the pre-charge intelligence-to-evidence pathway, the CEP governs how classified material is handled during and after proceedings. The CEP draws on and improves the US CIPA model, the UK PII regime, and the European Court of Human Rights' Article 6 jurisprudence, specifically addressing the weaknesses identified in each.

8.2 Classified Evidence Categories

8.3 The Substitution Standard

Where a CEPO permits the substitution of an intelligence summary for the full classified original, the substitution must meet the Meaningful Challenge Standard: a defendant who reads the substituted summary must be in a position to effectively challenge any factual allegation derived from the classified intelligence. This is a higher standard than any legacy model has imposed. The IEC independently tests every substituted summary against this standard before the CEPO is issued. A summary that the IEC determines does not meet the standard either: is expanded until it does; results in disclosure of the original; or results in the affected allegation being withdrawn from the proceedings.

8.4 Emergency Classification Claims

Where, during proceedings, a classification claim emerges that was not identified at the pre-charge stage — because new evidence was gathered or new classified material was identified — the proceedings are immediately paused. An emergency CEM assessment is conducted within 48 hours. The accused remains in any custody ordered by the presiding Magister during the pause. The CEM issues an emergency CEPO amendment, a new IEC assessment is produced, and the presiding Magister decides whether proceedings can fairly continue. The defence Civic Advocate is informed of the pause and its general reason within 24 hours. Repeated emergency classification claims in the same proceedings constitute a pattern that the CPOC reviews as a potential sign of bad faith by the CPS or ISD.

PART IV — COMMUNITY, CUSTODY, AND SPECIALIST OPERATIONS

Section 9: Community Policing Architecture

9.1 The Community Policing Model

Community policing in the NBI is not a programme or an initiative — it is the foundational operational mode. Every CPS deployment is oriented toward the community it serves before it is oriented toward enforcement. This is not sentiment; it reflects the empirical evidence on police effectiveness: communities that trust their police provide information, cooperate with investigations, and are more resilient against serious organised harm. Communities that distrust their police provide nothing, obstructing investigations and allowing harm to persist.

The Community Safety Officers (CSOs) — non-warranted, non-enforcement roles embedded in Community Assembly areas — are the primary face of the CPS in most interactions with most residents, most of the time. They are not police officers in the traditional sense. They cannot arrest, detain, search, or use force. They provide a visible, accessible, trusted civic presence that connects residents with the CPS, with civic support services, and with early intervention resources before harm occurs or escalates.

9.2 Proportionality in Community Engagement

The CPS does not police communities differentially on the basis of the demographic composition of those communities. All aggregate policing data — stop and account rates, arrest rates, use of force rates, prosecution rates — is published on the NIN public portal broken down by Community Assembly area, by time period, and by the demographic information that residents choose to provide. The CPOC monitors this data specifically for disproportionality patterns and initiates automatic reviews where disproportionality is identified.

The specific failure of racially disproportionate policing in the legacy system — documented across 25 years of official reports and still not resolved at the point of NBI Transition — is addressed in the NBI architecture through three mechanisms: the enumeration of powers (which eliminates discretionary "soft" powers that historically operated to entrench disproportionality); the NIN-PR real-time monitoring (which makes disproportionality visible immediately rather than in retrospect); and the CPOC sortition composition, which specifically includes Community Assembly representatives who bring lived experience of community-police relations into the oversight process.

9.3 Early Intervention and Referral

The CPS is integrated with the wider NBI civic support architecture — Mental Care Facilities, restorative pathway hubs, community advocacy services — through a formal Early Intervention and Referral Protocol (EIRP). CPOs and CSOs encountering residents in circumstances that are better addressed by civic support than by enforcement — mental health crisis, housing crisis, substance dependency, domestic harm where the victim needs support rather than the other party's arrest — are trained and empowered to initiate referrals through the EIRP.

The EIRP is not a mechanism for the CPS to perform the functions of other civic services. It is a structural connection between the CPS and those services, so that a resident encountered by a CPO in crisis reaches the right support rather than the wrong enforcement response. The empirical evidence on the diversion of mental health crises from police to mental health services — the CAHOOTS model in Oregon, the STAR programme in Denver, and the Force programme in Merseyside — demonstrates that appropriate referral produces better outcomes for both the resident in crisis and the broader community at lower cost and with less long-term harm. The NBI adopts and embeds this evidence.

Section 10: Civic Custody Architecture

10.1 The Philosophy of Civic Custody

Pre-charge custody is not punishment. It is not a preview of consequences. It is a temporary measure of last resort applied to prevent specific identified harms — flight, further harm, or destruction of evidence — while an investigation proceeds. Every element of the civic custody architecture is oriented toward this definition: conditions of custody are not harsher than necessary to achieve these specific aims; duration is not longer than necessary; and the resident in custody retains all rights that are not directly limited by the specific custody necessity.

10.2 Civic Custody Centres

Pre-charge custody is held in Civic Custody Centres (CCCs) — purpose-built facilities designed to meet specific minimum standards that are published on the NIN public portal and independently audited quarterly. Minimum standards include:

- Single-occupancy cells of minimum specified floor area, with access to natural light
- Access to regular meals meeting basic nutritional standards, at times aligned with normal meal patterns
- Access to outdoor space for a minimum period each day
- Access to communication with a Civic Advocate, without time restriction and without monitoring
- Access to medical assessment within 2 hours of arrival and on request thereafter
- Access to appropriate religious or cultural facilities
- Documentation of all interactions, all requests and their outcomes, and the detained resident's stated welfare status at regular intervals

CCCs do not hold children in the same facilities as adults. Youth Civic Welfare Suites are separate facilities with enhanced welfare standards, always staffed by officers with specific youth welfare training, and subject to enhanced CPOC oversight.

10.3 Custody Record

The Custody Management Officer (CMO) maintains a continuous custody record for every detained resident, recorded on the NIN-PR in real time. The custody record captures: arrival time and condition; every interaction; every request and its outcome; all welfare checks; all interviews; all access to Civic Advocate; all medical interventions; and the grounds for each decision about the conduct of the detention. The custody record is visible to the presiding Magister reviewing any extension application. A custody record showing that the grounds for detention have not advanced is not a record that will support an extension.

10.4 Interview Architecture

Interviews of detained residents are conducted under the following non-negotiable conditions:

- The detained resident is reminded of their right to a Civic Advocate before every interview and the interview does not proceed until the Civic Advocate is present or the resident has, with the Civic Advocate present, declined to have one present for the specific interview
- All interviews are video-recorded in full — audio and visual — with the recording stored on the NIN-PR

- All interviews begin with a caution in plain language stating that the resident is not obliged to answer and that what they say will be recorded and may be used in proceedings
- No interview may continue for more than two hours without a minimum 30-minute break, subject to the resident's right to stop at any time
- No interview tactic that is designed to deceive, manipulate, or coerce an answer is permitted — specifically: false evidence ploys, sleep deprivation, environmental manipulation, or any approach designed to exploit vulnerability are prohibited

The NBI adopts and mandates the Cognitive Interview technique — the most rigorously evidenced approach to witness and suspect interviewing in the research literature — as the standard interview method. The Cognitive Interview is specifically designed to maximise the accuracy and completeness of information provided, not to maximise confession rates. The distinction is critical: an interview architecture designed to produce confessions produces false confessions. An architecture designed to produce accurate information produces useful information.

Section 11: Specialist Operations

11.1 Civic Tactical Response Units

Civic Tactical Response Units (CTRUs) are specialist CPS teams trained and equipped for high-risk situations — incidents involving weapons, hostage-taking, or terrorist activity in progress. CTRUs are not standing armed patrols. They are deployable on specific, Magister-authorised operations or on immediate response to active threats where delay would cause casualties. CTRU deployment for any purpose other than an immediate active threat requires advance Magister authorisation specifying the operation and its justification. All CTRU operations are subject to full NIN-PR recording and automatic CPOC post-operation review.

11.2 Undercover Operations

Undercover policing — the deployment of CPOs in concealed identity to infiltrate organisations or build relationships with suspects — is the most ethically hazardous tool available to the CPS. The UK's undercover policing scandals — documented by the Pitchford Inquiry from 2015 and covering decades of abusive practice including sexual relationships between undercover officers and the activists they were investigating, the use of dead children's identities, and systematic surveillance of legitimate civic organisations — represent a systemic architecture failure, not merely individual misconduct.

The NBI undercover architecture is built on the specific lessons of those failures:

- Undercover operations require Magister Warrant authorisation and CPOC notification before deployment — no undercover operation may commence without both
- Undercover officers may not form intimate relationships with the people they are investigating under any circumstances — this is an absolute prohibition with no public interest exception
- Undercover officers may not use the identities of deceased persons
- Undercover operations targeting civic advocacy organisations, trade unions, sortition assemblies, or legitimate political or community groups are absolutely prohibited regardless of the suspected conduct of individual members
- All undercover operations are reviewed by an independent Magister at 90-day intervals; any operation that has not produced specific actionable intelligence within 90 days is presumptively

terminated unless the Magister finds specific grounds for continuation

- Post-operation, all individuals who were the subject of undercover operations are notified within 5 years of the operation's conclusion that they were investigated in this way — the same notification obligation that applies to ISD operations on residents
- Undercover officers who engage in prohibited conduct are not indemnified by their employer — they face the same Civic Consequence pathway as any other CPO

11.3 Surveillance Operations

CPS surveillance operations — physical surveillance of individuals, vehicle tracking, use of directed surveillance — require Magister Warrant authorisation on the same basis as ISD surveillance. The CPS does not have access to ISD surveillance capabilities — any surveillance operation requiring technical capabilities beyond the CPS's own warranted toolkit requires a formal ISD request through the IREIP gateway. There is no informal capability-sharing between the ISD and the CPS.

11.4 Serious Organised Harm Investigation

Serious organised harm — drug trafficking networks, organised financial crime, people trafficking, organised violence — is investigated by dedicated Serious Organised Harm Investigation Teams (SOHITs) within the CPS. SOHITs operate under the same powers and the same accountability architecture as all CPS investigations, but with longer investigation timelines (reflecting the complexity of organised harm) and enhanced CPOC oversight (reflecting the greater operational sensitivity).

SOHITs are the CPS's primary interface with the ISD on Category 6 matters (organised crime with national security nexus). All SOHIT referrals to the ISD and all ISD referrals to SOHITs go through the IREIP. No informal relationship between SOHIT officers and ISD officers on matters that could generate a prosecution is permitted.

PART V — ACCOUNTABILITY, FAILURE MODES, AND INTEGRATION

Section 12: Accountability Architecture — Complete Specification

12.1 Layered Accountability

The CPS accountability architecture operates at five layers simultaneously — creating a system in which failure to catch misconduct at one layer is caught at another, and in which accountability is not dependent on any single body operating perfectly.

12.2 Individual Complaint Architecture

Any resident who believes they have been subjected to unlawful or improper conduct by a CPO may submit a complaint to the CPOC through the NIN public portal. Complaints are processed as follows:

- Within 48 hours: the CPOC acknowledges receipt and pulls the relevant NIN-PR records for the incident automatically — the complainant does not need to describe what records exist; the CPOC sees them
- Within 14 days: the CPOC produces an Initial Assessment — whether the complaint raises a case to answer, whether it appears to describe conduct consistent with the NIN-PR record, and what investigation is initiated
- Within 90 days: the CPOC produces a findings report — whether the conduct was within CPO powers, whether it met the ethics principles, and what consequence or learning action follows

- All complaint outcomes are published on the NIN-PR in anonymised form; patterns of complaints against individual officers or units are published in aggregate on the NIN public portal

The CPOC does not investigate complaints — it assesses them and, where a case to answer is established, refers to the relevant Magister for the Civic Consequence determination. The CPS does not investigate complaints about its own officers. There is no internal affairs function — this is the structural lesson of every legacy model that has tried to establish genuinely independent investigation within the police body: it cannot work because the institutional loyalty is impossible to remove from inside.

12.3 Pattern Monitoring and Systemic Review

Individual complaint resolution addresses individual incidents. Systemic problems — the kind that produced 25 years of Macpherson-documented disproportionality, 40 years of undercover scandal, and decades of disclosure failures — are not visible in individual complaints. They are visible only in patterns. The CPOC's pattern monitoring function is designed specifically for this:

- Monthly publication of aggregate policing data by area, demographic, harm type, and outcome
- Quarterly CPOC pattern review: identification of any aggregate pattern inconsistent with the ethics principles or with the minimum standards of the civic compact
- Automatic systemic review trigger: any statistically significant disproportionality in any aggregate measure triggers a mandatory CPOC systemic investigation, independent of any complaint
- Annual systemic review: the CPOC publishes an Annual State of Civic Policing Report on the NIN public portal — the NBI's most comprehensive public account of how its police service is performing

Section 13: Failure Mode Analysis — Adversarial Stress-Testing

13.1 CPS Failure Modes

Failure Mode 1: Institutional Culture Drift

Description: The CPS, despite its constitutional architecture, develops an institutional culture that values solidarity over accountability, that systematically under-records problematic conduct, and that treats the ethics architecture as external constraint rather than internal commitment.

Likelihood: High without continuous structural pressure. Every police service in the legacy system experienced culture drift of this kind. It is not a matter of bad individuals — it is a matter of institutional dynamics that reward solidarity and penalise "grassing."

Countermeasures: The NIN-PR real-time recording eliminates the possibility of the most egregious recording failures — you cannot not record an arrest or a use of force because the gap is visible. Culture drift manifests instead in the quality and honesty of the recording, not its existence. The CPOC pattern monitoring is designed to detect the signatures of dishonest recording — records that are implausibly uniform, records that show consistently minimal grounds for use of force, records that lack the detail of genuine contemporaneous accounts. The sortition-based CPOC composition specifically includes people without police-culture socialisation who can see these signatures. The ethics curriculum's 12-month depth is designed to build a genuinely different officer culture rather than an obeyed rule set.

Failure Mode 2: Circumvention of the IREIP Through Informal Channels

Description: ISD officers and CPS Investigation Officers develop personal relationships — through joint training, shared operational experiences, or informal social networks — that allow intelligence to flow from ISD to CPS investigation teams outside the formal IREIP gateway. The result is soft parallel construction: investigations that are informally guided by intelligence that never formally enters the IREIP.

Likelihood: High. This is the historically observed pattern in every system with a formal separation between intelligence and law enforcement. The CSIS/RCMP model was repeatedly circumvented in exactly this way.

Countermeasures: The Clean Team Independence Audit (Stage 2 of the IREIP) specifically looks for investigative trails that are inconsistent with a genuinely independent investigation. The NIN-PR's timestamped record of every investigative action allows reconstruction of the investigative narrative — if the investigation took turns that were only explicable in light of intelligence the Clean Team was not supposed to have, this is detectable. Joint training between ISD and CPS officers is prohibited for operational personnel — the ILO is the sole interface and must be free from the informal relationship networks that bypass formal gatekeeping. Any identified circumvention permanently stays the affected proceedings and activates the highest-tier consequence pathway for all officers involved.

Failure Mode 3: Magister Warrant System Gaming

Description: CPOs systematically present warrant applications in ways that are technically sufficient but misleading — emphasising supportive intelligence while omitting context that would weaken the application, or applying to Magisters who are known to be less rigorous.

Likelihood: Moderate. This has been documented in every warrant system that has been studied over time. FISA warrant applications from US agencies showed systematic omission of exculpatory material — the "Woods Procedures" were designed to address this and largely failed.

Countermeasures: Warrant applications are write-once NIN-PR records at the point of submission — they cannot be retrospectively amended to remove the evidence of omission. The CEM's access to the full intelligence picture at Stage 3 means that any warrant application that misrepresented the intelligence picture is visible in the comparison between the warrant application's stated basis and the actual NIN-SIN intelligence record. Refused warrants from any Magister are recorded — the practice of "shopping" a refused application to a different Magister is blocked because all Magisters can see the refusal record. The CPOC reviews warrant application patterns for quality and honesty, not merely outcomes.

Failure Mode 4: The Fair Trial Pressure Test — A Well-Resourced Defendant

Description: A sophisticated defendant — represented by the most capable legal team available, with resources to challenge every element of the IREIP — systematically attacks the architecture through legal challenges designed to either expose classified intelligence or force abandonment of the case. This is not a failure mode in the sense of wrongdoing; it is the legitimate operation of adversarial justice. The question is whether the architecture can withstand it.

Assessment: The architecture is designed specifically to withstand this pressure. The three-Magister panel eliminates the single-point vulnerability of a solo judicial officer. The IEC's role specifically anticipates the arguments that a sophisticated defence will make about the unfairness of the disclosure position — because the IEC has made those arguments first, from a position of full intelligence access, the defence's arguments are already addressed in the CEPO. The graymail

architecture specifically prevents the threat of disclosure being used as a stay-forcing mechanism. The Meaningful Challenge Standard for intelligence summaries means that a sophisticated legal challenge to the adequacy of disclosure will have a higher success rate only if the summary genuinely is inadequate — and if it is, the challenge should succeed.

The honest answer is that some well-resourced defendants will succeed in staying proceedings through IREIP challenges, and this is appropriate. The architecture is not designed to convict everyone against whom there is intelligence. It is designed to allow proceedings to proceed only when they can do so fairly. A stay granted because the IREIP could not produce a fair-trial-compliant disclosure is the system working correctly, not failing.

Failure Mode 5: The Political Pressure Test — Elite Defendants

Description: An investigation or prosecution involving powerful individuals — economic elites, former civic role-holders, individuals with significant social capital — is subject to institutional pressure to be abandoned, conducted less rigorously, or structured in ways that protect the defendant from the full application of the law.

Likelihood: Very high. The differential application of criminal law to wealthy and powerful defendants is the most extensively documented failure of every justice system in the historical record. It operates through a combination of superior legal resources (addressed above), informal institutional pressure, and the social network effects that mean those with social capital are treated differently at every stage from investigation to sanction.

Countermeasures: The NIN-PR public record is the primary countermeasure — it is extremely difficult to "quietly drop" an investigation that has been publicly recorded from the outset. Any decision not to proceed with an investigation or prosecution that is visible on the NIN-PR requires a written, NIN-PR-published explanation. Anonymous complaint to the CPOC about investigation abandonment is available to any resident, including investigators who believe they are being pressured. The CPOC has authority to investigate decision-making about investigation and prosecution, not just conduct during investigation. The NSA investigative process is available for any pattern suggesting systematic differential application. These countermeasures do not eliminate elite advantage — social capital is not eliminated by architecture. But they make its exercise visible and documented in a way that creates risk for those who exercise it.

Failure Mode 6: The False Negative — Missing Genuine Threats

Description: The IREIP's requirements are so demanding that genuine threats are not prosecuted because the intelligence-to-evidence pathway is too difficult to navigate. The result is that serious organised harm, terrorism, and hostile state activity goes unpunished because the architecture is more rigorous than operational reality can sustain.

Assessment: This is the most legitimate criticism of a rigorous intelligence-to-evidence architecture, and it deserves a direct answer. Yes, some cases that could be prosecuted if the IREIP were less rigorous will not be prosecuted under this architecture. This is not a flaw — it is a design choice. The alternative — allowing convictions on the basis of intelligence that the defendant cannot challenge and that may be wrong — produces a system that incarcerates innocent people with no reliable mechanism for discovering the error. The Judith Ward case, the Guildford Four, the Birmingham Six, the Stefan Kiszko case — all convictions in which intelligence or police conviction that the defendant was guilty contributed to proceedings in which the defendant could not effectively challenge the basis of the case. The NBI architecture accepts some false negatives as the cost of avoiding false positives

and structural unfairness. What it does not accept is that this trade-off is fixed — the quality of independent evidence gathering, the effectiveness of clean team investigations, and the IREIP's efficiency all improve over time, reducing the false negative rate without compromising the constitutional standards.

Section 14: Integration with the DD&SA Constitutional Architecture

14.1 Instrument Crosswalk

14.2 Implementation Roadmap

14.3 The Authorial Statement

This Framework was written in the knowledge that it will be read by those who wish to find its weaknesses — by the legally sophisticated, by the politically powerful, by those who believe that security demands sacrificing the rights of the many for the safety of the few, and by those who believe that any accountability is an obstacle to effective policing. It was written to withstand every one of those readings.

The historical record is clear: security services and police forces without robust constitutional constraints do not become more effective as constraints are removed. They become less trustworthy, less trusted, less capable of the community cooperation that is the foundation of actual security, and more dangerous to the residents they nominally serve. The NBI architecture does not make that trade. It holds, without apology and without exception, that the safety of the nation is inseparable from the rights of its residents — and that any security apparatus that protects the former by destroying the latter has accomplished nothing worth protecting.

"We do not turn back time; we move forward with the wisdom its patterns reveal."

Ian R. Graham BA (Hons)

Sole Architect, Direct Democracy & Sortition Assemblies (DD&SA)

Civic Policing Framework (DD&SA-CPF-001)

Edition 1.0 | April 2026

— END OF DOCUMENT —