DIRECT DEMOCRACY & SORTITION ASSEMBLIES

A Civic Architecture for the British Isles

DDSA-CSIA-001 | Edition 1.0

Civic Security and Intelligence Architecture

Intelligence under constitutional constraint — every product, every decision, every warrant accountable

---

DOCUMENT INFORMATION

Version: 1.0
Author: Ian R. Graham
Document ID: DDSA-CSIA-001

CLASSIFICATION

Confidentiality: Public Domain
Distribution: Unrestricted — For civic, academic, and public use

---

USAGE NOTICE & PERMISSION

"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

EXECUTIVE SYNTHESIS

The Civic Commonwealth of the British Isles (NBI) requires intelligence and security services. The safety of residents — their protection from hostile foreign states, from terrorism, from covert sabotage of national infrastructure, and from the systematic targeting of NBI civic processes — is a foundational civic duty. The NBI is not naive about the world it operates in. Threats are real, adversaries are sophisticated, and the consequences of intelligence failure are potentially catastrophic.

The question this Framework addresses is not whether the NBI needs security services. It does. The question is what kind of security services are compatible with the NBI's constitutional order, its ethical architecture, and its foundational commitment to resident sovereignty. The answer this Framework provides is unambiguous: security services that are fully accountable to the resident body through the National Sortition Assembly; that operate within an ethics architecture that cannot be set aside for operational convenience; that record everything on a write-once network that the NSA alone owns and can access; and that hold the safety of the nation and the rights of residents as complementary obligations, not competing ones.

This Framework — the Civic Security and Intelligence Architecture (DD&SA-CSIA-001) — establishes five operational departments replacing the legacy security apparatus of the prior state: the Internal Security Department (ISD), replacing MI5; the External Security Department (ESD), replacing MI6; the Civic Signals and Cyber Intelligence Department (CSCID), replacing GCHQ; the Civic Defence Intelligence Department (CDID), replacing the Defence Intelligence Directorate; and the Civic Counter-Terrorism and Extremism Unit (CCTEU), replacing the cross-service counter-terrorism machinery. It also establishes the National Security Coordination Council (NSCC) as the single inter-departmental governance body, and the Civic Security Ethics and Oversight Panel (CSEOP) as the permanent resident-accountability mechanism.

Every intelligence product, every operational decision, every warrant application, every source record, every assessment, and every failure is recorded on the NIN Secure Intelligence Network (NIN-SIN) — a write-once, NSA-owned partition of the National Information Network. Nothing is deleted. Nothing is amended. Nothing is copied outside the partition without NSA authorisation. The NSA accesses NIN-SIN only through formal investigative mandate. The security services hold classified intelligence on behalf of the resident body. The resident body, through the NSA, is the ultimate owner of everything held in their name.

PART I — CONSTITUTIONAL AND ETHICAL FOUNDATION

Section 1: Constitutional Basis and Mandate

1.1 The Security Duty of the Civic Commonwealth

The NBI Constitution places the security of residents among the primary duties of the Civic Commonwealth. This duty has two inseparable dimensions. The first is protection: the NBI must be capable of identifying, assessing, and disrupting threats to its residents, its infrastructure, and its civic institutions from foreign states, non-state actors, and domestic extremist movements. The second is restraint: the NBI's security apparatus must itself be incapable of becoming a threat to the residents it serves. A state that protects residents from external threats by subjecting them to internal surveillance and covert control has not secured its residents — it has merely changed the identity of their oppressor.

The NBI constitutional architecture resolves this tension architecturally rather than rhetorically. It does not simply declare that security services will respect rights — declarations are not architecture. Instead, it builds the incompatibility of abuse into the operational structure of the services themselves: through write-once recording that cannot be manipulated; through sortition-based oversight that cannot be captured; through an ethics architecture that has the same constitutional weight as the operational mandate; and through a warrant system that requires independent Magister authorisation for all intrusive activity.

1.2 Inviolable Constitutional Limits

The following limits apply to every security department established under this Framework and to every individual acting under the authority of any such department. They are absolute. They have no operational override, no emergency suspension, and no classified waiver mechanism.

- No security department may conduct surveillance, investigation, or intelligence-gathering on NBI residents except under a Magister Warrant issued through the process specified in Section 11 of this Framework
- No security department may act to undermine, circumvent, or weaken any element of the DD&SA constitutional architecture, including the Sortition Assembly process, the National Information Network, the Civic Justice Architecture, or the Civic Transparency Enforcement Framework
- No security department may maintain any relationship — operational, financial, or informational — with any Category A–H prohibited organisation as defined in the Civic Transparency and Institutional Integrity Architecture (DD&SA-CTIA-001)
- No security department may conduct, commission, or facilitate any action that would constitute a prohibited consequence under the Civic Justice Architecture (DD&SA-CJA-001), including torture, coerced confession, unlawful detention, or collective punishment
- No security department may conduct any action on NBI territory that targets NBI residents on the basis of their protected characteristics, their civic participation, their political or philosophical views, or their lawful exercise of civic freedoms
- No security department may withhold from the NSA's investigative access any record held on the NIN-SIN — the NSA's ownership of all NIN-SIN content is absolute and non-negotiable
- No security department may conduct offensive operations against foreign states or non-state actors without explicit NSA authorisation through the CNSDF process (DD&SA-CTIA-001, Part II)

1.3 Relationship to the Thirty Inviolable Rules

The Thirty Inviolable Rules of the NBI Constitution form the compliance spine of the entire DD&SA corpus. This Framework is subject to all Thirty Rules without exception. Where any provision of this Framework appears to conflict with any Inviolable Rule, the Rule takes precedence and the Framework provision is void to the extent of the conflict. This Framework does not establish any new Inviolable Rules — it operates within the existing constitutional hierarchy.

Section 2: DD&SA Ethics Compliance Architecture

2.1 Why Security Services Need a Standalone Ethics Architecture

Intelligence and security work involves, by its nature, activities that are ethically hazardous: deception, covert surveillance, the recruitment and handling of human sources, the collection of private information, and in some circumstances, actions that cause harm to prevent greater harm. These activities are not inherently wrong in the context of legitimate security operations against genuine threats. They become wrong when they are conducted without authorisation, without proportionality, without accountability, or against people who are not legitimate targets.

The ethics architecture of this Framework does not attempt to eliminate the ethical hazards of security work — that would be dishonest and would simply drive them underground. It attempts to make every ethically hazardous action visible, authorised, proportionate, and accountable. An officer who deceives a foreign intelligence operative under a Magister-authorised operation with full NIN-SIN recording is operating within the ethics architecture. An officer who deceives an NBI resident without authorisation, for personal or institutional reasons, with no record, is not.

2.2 The Five Ethics Principles

All security operations and all security personnel are bound by the following five ethics principles. These principles have constitutional weight — they are not aspirational statements but operative constraints with consequence pathways attached to their breach.

Ethics Principle 1 — Necessity

No intelligence operation, surveillance activity, source recruitment, or intrusive action may be undertaken unless it is necessary to address a specific, identified threat or intelligence gap that cannot be addressed by less intrusive means. Necessity is not demonstrated by asserting that an operation would be useful. It is demonstrated by showing that the threat is real, the target is appropriate, and no less intrusive alternative exists. Necessity is assessed at the point of Magister Warrant application and reviewed at each operational renewal point.

Ethics Principle 2 — Proportionality

The degree of intrusion authorised for any operation must be proportionate to the gravity of the threat it addresses. Covert surveillance of a resident’s private communications is proportionate to the investigation of a credible threat of mass-casualty terrorism. It is not proportionate to the investigation of suspected minor infringement of civic framework provisions. Proportionality is assessed against the most intrusive element of an operation, not its most benign element.

Ethics Principle 3 — Legality

Every action taken by every security department officer must have an explicit legal basis in this Framework, in the NBI Constitution, or in a Magister Warrant authorised under Section 11. "Legal basis" means a specific, identified provision that authorises the specific, identified action. General mandates ("the ISD may conduct intelligence-gathering") do not constitute legal basis for specific intrusive actions. If no specific provision authorises a specific action, the action is not authorised.

Ethics Principle 4 — Accountability

Every action, decision, authorisation, failure, and consequence in every security department must be recorded on the NIN-SIN at the time it occurs. There is no provision for retrospective recording, delayed recording, or recording "when operationally safe to do so." The accountability obligation is concurrent with the action. An action that cannot be concurrently recorded is an action that cannot be taken. The recording is not a bureaucratic formality — it is the mechanism through which resident sovereignty over the security services is made real.

Ethics Principle 5 — Humanity

All individuals who are the subjects of security department operations — whether NBI residents under Magister Warrant, foreign nationals, or individuals in foreign jurisdictions — retain their fundamental human status. They may not be tortured, subjected to cruel, inhuman, or degrading treatment, used as unwitting experimental subjects, or targeted in ways that treat their lives as expendable. This principle applies even to individuals who have themselves committed or are planning to commit acts of terrible violence. The NBI does not abandon its ethics in response to the ethics failures of its adversaries.

2.3 The Ethics Compliance Record

For every operation above routine intelligence collection, a formal Ethics Compliance Record (ECR) is created on the NIN-SIN at the point of operational authorisation. The ECR documents: the necessity assessment; the proportionality assessment; the specific legal basis; the accountability confirmation (recording protocol activated); and the humanity confirmation (no prohibited means authorised or anticipated). The ECR is updated at each operational review point. It is permanently accessible to the NSA investigative process and to the CSEOP.

Section 3: The Civic Security Mandate

3.1 What the Security Services Are For

The security services of the NBI exist to identify, assess, and where lawfully possible disrupt threats to the safety, integrity, and sovereignty of the Civic Commonwealth and its residents. The mandate is defensive in nature. The services do not exist to project power, to advance commercial or geopolitical interests, to suppress political opposition, or to gather intelligence on residents for purposes unrelated to genuine security threats. The mandate is also bounded: it ends at the point where a security activity would itself constitute a threat to the constitutional order it is supposed to protect.

3.2 Threat Categories

The security services are authorised to direct their activities against the following threat categories, within the departmental jurisdictions specified in Parts II and III of this Framework:

- Category 1 — Hostile State Activity: the activities of foreign states directed against NBI residents, infrastructure, democratic processes, or territorial integrity, including espionage, sabotage, covert political interference, and armed aggression
- Category 2 — Terrorism and Mass-Casualty Violence: the planning, preparation, and facilitation of terrorist acts and other mass-casualty violence by any actor, domestic or foreign
- Category 3 — Critical Infrastructure Threats: hostile acts or planned acts against the NBI's energy, water, food supply, transportation, communications, and health infrastructure
- Category 4 — Cyber and Information Warfare: hostile state and non-state cyber operations against NBI digital infrastructure, including the National Information Network itself
- Category 5 — Weapons of Mass Destruction Proliferation: the development, acquisition, trafficking, or deployment of nuclear, biological, chemical, or radiological weapons
- Category 6 — Serious Organised Crime with National Security Nexus: organised criminal activity that has a demonstrable connection to hostile state actors, terrorist financing, or critical infrastructure compromise
- Category 7 — Threats to NBI Constitutional Integrity: organised covert attempts to undermine, capture, or destroy the NBI's constitutional architecture, including the Sortition Assembly process and the NIN

3.3 What the Security Services Are Not For

The following activities are explicitly outside the mandate of all security departments established under this Framework. These exclusions are not guidelines — they are operative prohibitions.

- Surveillance or intelligence collection targeting NBI residents on the basis of their lawful civic participation, political or philosophical views, religious practice, or lifestyle
- Intelligence support for commercial interests of NBI companies or individuals
- Political intelligence — monitoring of civic advocacy, Assembly deliberations, or resident political activity
- Intelligence collection against NBI residents who have not been assessed as posing a threat within one of the seven authorised threat categories
- Counter-intelligence operations that target journalists, civic advocates, Sortition Assembly members, or Magisters in their civic roles
- Any activity that would constitute prohibited conduct under the Civic Transparency Enforcement Framework (DD&SA-CTIA-001)
- Rendition, extraordinary detention, or transfer of individuals to jurisdictions where prohibited treatment is likely

PART II — DEPARTMENTAL ARCHITECTURE

Section 4: Internal Security Department (ISD)

4.1 Identity and Mandate

The Internal Security Department (ISD) is the NBI's domestic intelligence and counter-intelligence service. It replaces the Security Service (formerly known as MI5) in its entirety. The ISD's mandate is to identify, assess, and where lawfully possible disrupt threats to the NBI from hostile actors operating within NBI territory — foreign intelligence operatives, terrorist networks, domestic extremist movements planning violence, and covert agents of foreign powers targeting NBI institutions.

The ISD does not have powers of arrest. It is an intelligence organisation, not a law enforcement body. Where operational intelligence identifies individuals who should be arrested and charged, the ISD refers the matter to the Civic Policing Framework (DD&SA-CPF-001) through a formal referral process with full NIN-SIN documentation. The ISD does not conduct its own prosecutions, maintain its own detention facilities, or exercise any criminal justice powers.

4.2 Roles and Functions — Plain English Specification

Role 1: Counter-Espionage

ISD officers identify and monitor foreign intelligence operatives working on NBI territory. This means: identifying individuals who are working for or on behalf of foreign intelligence services; understanding what they are trying to find out or do; and disrupting their operations through lawful means. Disruption may include identifying and expelling foreign intelligence officers operating under diplomatic cover, working with the ESD to understand foreign intelligence priorities, and advising NBI institutions on how to protect themselves from espionage.

ISD counter-espionage operations against NBI residents require Magister Warrants specifying the specific intelligence basis for suspecting the resident of acting for a foreign power. A resident's foreign nationality, foreign contacts, or foreign travel are not, on their own, grounds for a warrant. There must be specific intelligence — not mere inference — that the individual is engaged in espionage activity.

Role 2: Counter-Terrorism (Domestic)

ISD officers gather intelligence on individuals and networks within NBI territory who are planning, preparing, facilitating, or inciting acts of terrorism. This means: monitoring communications and activities of individuals assessed as genuine terrorism threats under Magister Warrant; working with international partners to track cross-border terrorism networks; assessing the credibility and imminence of specific threat intelligence; and providing threat assessments to the CCTEU (Section 8) and to relevant civic bodies.

Counter-terrorism intelligence is gathered to prevent attacks — not to compile long-term political dossiers on individuals who hold extremist views but are not engaged in violence planning. The legal test is always: is this individual involved in planning, preparing, or facilitating violence? Holding views that the ISD or any other body considers extreme does not, on its own, constitute a ground for surveillance.

Role 3: Counter-Hostile State Interference

ISD officers identify and assess covert attempts by foreign states to interfere with NBI civic processes, institutions, and public life. This includes: identifying covert influence operations — disinformation, agent-of-influence recruitment, media manipulation — directed at NBI residents; assessing the extent and nature of foreign state interference in NBI civic deliberations; working with the CTIU (under the CTIA-001) where foreign-state interference operates through domestic prohibited organisations; and advising the NSCC on the scope of hostile state interference.

The ISD's role in counter-hostile-state-interference is specifically bounded to foreign-directed activity. It is not a domestic political surveillance function. Where the ISD identifies domestic actors who are wittingly or unwittingly serving foreign interference objectives, those individuals are referred to the CTIU for the civic process, not placed under ongoing ISD surveillance.

Role 4: Protective Security

The ISD provides protective security advice and assessments to NBI civic institutions, critical national infrastructure operators, and the Sortition Assembly process itself. This means: assessing the security risks facing NBI civic bodies and advising on how to mitigate them; advising on personnel security — identifying individuals in sensitive positions who may have been compromised or who pose insider security risks; and producing threat assessments that allow NBI institutions to make informed decisions about their own security posture. The ISD does not operate its own protective security forces — physical protection is the responsibility of the Civic Security Architecture (DD&SA-CSA-001).

Role 5: Counter-Proliferation (Domestic)

ISD officers gather intelligence on attempts by domestic or foreign actors to acquire, develop, or deploy weapons of mass destruction within NBI territory. This means tracking suspected proliferation networks, identifying attempted acquisition of controlled materials, and coordinating with the CSCID on digital aspects of proliferation activity. Counter-proliferation intelligence is among the highest priorities in the ISD mandate — the potential consequences of failure in this domain are existential.

Role 6: Serious Organised Crime — National Security Nexus

The ISD has a specific mandate to address organised criminal activity where there is a demonstrable connection to hostile state actors, terrorist financing, or critical infrastructure vulnerability. This mandate is not a general serious-crime remit — the ISD is not a replacement for law enforcement. It covers the specific intersection: where organised crime is being directed, funded, or exploited by hostile state intelligence services; where criminal networks are serving as logistics infrastructure for terrorism; or where criminal activity represents a direct threat to the NBI's national security rather than primarily a law enforcement matter.

4.3 ISD Staffing and Governance

Director of Internal Security

The ISD is led by a Director of Internal Security, appointed through a process of open application assessed by a sortition-selected Appointment Review Panel. The Director must have demonstrable relevant expertise in intelligence, security, or a directly related field. The Director serves a fixed 5-year term, non-renewable. The Director's appointment, remuneration, and any removal from post are published on the NIN. The Director is not a civic role-holder in the sortition sense — but is fully subject to the Civic Transparency Declaration requirement and the CTEF. The Director reports to the NSCC, not to any individual civic executive.

Staffing Principles

ISD staff are recruited through an open, advertised process with clear competency requirements, subject to full security vetting under the Civic Security Vetting Framework (Section 13). All staff complete the Civic Transparency Declaration on joining and annually thereafter. ISD staff may not hold membership of any Category A–H prohibited organisation — this is an absolute and irrevocable bar that cannot be waived on operational grounds. Intelligence expertise drawn from the legacy Security Service may be transferred to the ISD subject to a full vetting review under the Transition Protocol (Technical Schedule A of this Framework).

Section 5: External Security Department (ESD)

5.1 Identity and Mandate

The External Security Department (ESD) is the NBI's foreign intelligence service. It replaces the Secret Intelligence Service (formerly known as MI6) in its entirety. The ESD's mandate is to gather intelligence on foreign states, foreign non-state actors, and foreign threats to NBI interests and security by operating outside NBI territory. It is the NBI's eyes and ears beyond its borders.

The ESD operates in a domain of inherent ethical complexity: foreign intelligence collection involves operating under cover, recruiting and handling human sources in foreign jurisdictions, and sometimes working in environments where local laws do not permit the activities the ESD conducts. This Framework addresses that complexity directly — it does not pretend it away. The ESD's ethical obligations travel with it: ESD officers carry the NBI's ethics architecture into every operating environment, regardless of what standards prevail locally.

5.2 Roles and Functions — Plain English Specification

Role 1: Foreign Intelligence Collection

ESD officers gather intelligence on foreign states, their governments, their armed forces, their intelligence services, and their intentions toward the NBI. This means: deploying officers in foreign countries under diplomatic and non-diplomatic cover; recruiting and running human intelligence sources in foreign governments, militaries, and institutions; collecting and reporting on foreign states' capabilities and intentions; and producing intelligence assessments that inform NBI security decisions. Foreign intelligence collection is the core function from which all other ESD roles derive.

Role 2: Counter-Proliferation (Overseas)

ESD officers gather intelligence on foreign programmes for the development, acquisition, and delivery of weapons of mass destruction. This means: identifying foreign state and non-state WMD programmes; tracking the international networks that supply controlled materials; assessing the capabilities and intentions of states with nuclear, chemical, biological, or radiological weapons; and working with international partners to disrupt proliferation networks at source. The ESD's counter-proliferation role is a joint priority with the ISD's domestic equivalent, coordinated through the NSCC.

Role 3: Counter-Terrorism (Overseas)

ESD officers gather intelligence on terrorist organisations, networks, and individuals operating outside NBI territory who pose a threat to NBI residents and interests. This means: understanding the structure, capabilities, and intentions of terrorist organisations abroad; tracking the movement and activities of known terrorists; identifying planning for attacks against NBI targets before those attacks reach NBI territory; and working with international partners to disrupt terrorist activity at source. The ESD does not conduct lethal operations — targeting and strike decisions are matters for the NSSP through the CNSDF process.

Role 4: Strategic Intelligence Assessment

The ESD produces regular strategic intelligence assessments on matters of foreign policy significance that affect NBI security: the intentions of foreign states toward the NBI; major geopolitical developments with security implications; the capabilities and activities of foreign intelligence services; and the strategic environment within which the NBI operates. These assessments are produced in classified form for the NSCC and, where the NSA requests them through the CNSDF investigative process, made available to the NSA.

Role 5: Cyber Intelligence (Overseas)

The ESD gathers intelligence on foreign cyber capabilities and cyber operations — the capacity of foreign states and non-state actors to conduct offensive cyber operations against the NBI. This is distinct from the CSCID's role (Section 6), which covers signals intelligence and cyber defence. The ESD's cyber intelligence role is human-intelligence-led: understanding through human sources what foreign cyber actors are planning and what capabilities they possess. The ESD shares this intelligence with the CSCID under formal NSCC-governed protocols.

Role 6: Liaison and Partnership Intelligence

The ESD maintains formal liaison relationships with foreign intelligence services under bilateral and multilateral agreements approved by the NSA through the International Civic Compact process. This means: sharing relevant intelligence with partner services where it serves NBI security interests; receiving intelligence from partner services that the ESD cannot collect independently; and managing the NBI's intelligence relationships with international partners. All liaison relationships are authorised by the NSA, recorded on the NIN-SIN, and reviewed annually. The ESD does not enter any intelligence-sharing arrangement that would expose NBI residents to surveillance by foreign services, or that would allow foreign services to use ESD-provided intelligence for purposes incompatible with NBI ethics principles.

Role 7: Covert Action (Limited and NSA-Authorised Only)

The ESD may conduct limited covert action — activities beyond intelligence collection that are intended to disrupt a specific foreign threat — only under explicit NSA authorisation through the CNSDF process and subject to Magister oversight. Authorised covert action is limited to: disruption of specific proliferation networks; disruption of specific terrorist financing or logistics operations; and, in extremis, operations against specific hostile intelligence operations targeting the NBI.

Covert action does not include: assassination or targeted killing; regime change operations; economic disruption; election interference in foreign states; or operations intended to benefit NBI commercial interests. Any ESD officer who conducts or proposes covert action outside these bounds is referred immediately to the full Civic Consequence pathway.

5.3 ESD Staffing and Governance

Section 6: Civic Signals and Cyber Intelligence Department (CSCID)

6.1 Identity and Mandate

The Civic Signals and Cyber Intelligence Department (CSCID) is the NBI's signals intelligence, communications intelligence, and cyber security service. It replaces GCHQ in its entirety. The CSCID has a dual mandate: offensive signals intelligence collection on foreign targets, and defensive cyber security for NBI infrastructure. Both functions operate under the same ethics architecture and the same NIN-SIN recording obligations.

The CSCID's signals intelligence capabilities are among the most powerful tools in the NBI security architecture — and among the most ethically hazardous. The ability to intercept, analyse, and exploit communications at scale creates the structural possibility of mass surveillance of NBI residents. This Framework eliminates that possibility architecturally, not rhetorically: bulk collection on NBI residents' communications is absolutely prohibited; targeted collection requires Magister Warrant; and every collection activity is recorded on the NIN-SIN write-once archive.

6.2 Roles and Functions — Plain English Specification

Role 1: Foreign Signals Intelligence Collection (SIGINT)

CSCID operators collect signals intelligence on foreign states and foreign non-state actors — intercepting, processing, and analysing foreign government communications, military communications, and the communications of identified foreign intelligence services. All foreign SIGINT collection is targeted against specific foreign entities or categories under a NSCC-approved collection requirement. CSCID does not conduct open-ended trawling of international communications — every collection activity has a defined purpose, a defined target, and a defined review date.

Role 2: Cyber Intelligence

CSCID analysts track and assess the cyber capabilities of foreign states and hostile non-state actors. This means: identifying the tools, techniques, and infrastructure used by foreign cyber actors; attributing cyber incidents and intrusions to their source where possible; producing intelligence assessments on foreign cyber threats for the NSCC and other departments; and working with the ISD and ESD to integrate signals and cyber intelligence with human intelligence.

Role 3: NIN and National Infrastructure Cyber Defence

The CSCID is responsible for the technical defence of the National Information Network and other critical national digital infrastructure. This means: monitoring NIN infrastructure for intrusions, anomalies, and hostile activity; developing and maintaining defensive capabilities that can identify and neutralise hostile cyber operations against NBI digital infrastructure; working with the Civic Infrastructure Authority on infrastructure security standards; and responding to active cyber incidents against NBI critical systems. The defensive function does not require warrants — defending NBI infrastructure against attack is a protective activity, not a surveillance activity.

Role 4: Technical Counter-Intelligence

The CSCID provides technical counter-intelligence support to the ISD, ESD, and other security departments. This means: detecting hostile signals intelligence operations against NBI communications; identifying technical surveillance devices deployed against NBI institutions; assessing the technical means used by foreign intelligence services to target NBI personnel; and advising NBI institutions on technical security measures. Counter-intelligence support is conducted under NSCC coordination.

Role 5: Cryptographic Standards and NIN Security

The CSCID is responsible for developing and maintaining the cryptographic standards that protect NBI government communications, including the NIN-SIN itself. This means: developing and updating encryption standards for NBI classified communications; maintaining the cryptographic infrastructure of the NIN-SIN write-once archive; and advising all security departments on communications security. Crucially, the CSCID's role in maintaining NIN-SIN cryptography does not give it access to NIN-SIN content — the write-once archive's access controls are maintained independently by the Civic Infrastructure Authority, with CSCID providing only the cryptographic tools, not the keys.

Role 6: Offensive Cyber Operations (NSA-Authorised Only)

The CSCID may conduct offensive cyber operations — active intrusions into foreign networks to gather intelligence or disrupt hostile capabilities — only under explicit NSA authorisation through the CNSDF process. Offensive cyber operations are not a routine intelligence tool. They are used where: no other means of gathering critical intelligence is available; where a specific hostile cyber operation must be disrupted before it causes catastrophic damage to NBI infrastructure; or where a specific NSA-authorised covert action requires technical support.

6.3 CSCID Staffing and Governance

Section 7: Civic Defence Intelligence Department (CDID)

7.1 Identity and Mandate

The Civic Defence Intelligence Department (CDID) is the NBI's defence intelligence service, providing intelligence assessment and analysis in support of NBI military and national security decision-making. It replaces the Defence Intelligence Directorate in its entirety, incorporating its imagery analysis, military assessments, and scientific and technical intelligence functions.

The CDID does not conduct its own collection operations. It is an all-source intelligence assessment body: it receives intelligence products from the ISD, ESD, and CSCID, combines them with open-source analysis, imagery intelligence, and scientific and technical assessment, and produces finished intelligence assessments for the NSSP and NSCC on military and strategic matters.

7.2 Roles and Functions — Plain English Specification

Role 1: Military Capability Assessment

CDID analysts assess the military capabilities of foreign states and non-state armed groups — what weapons they have, how many, what condition they are in, how they would be deployed, and what the effects of their use would be. These assessments inform NSSP deliberations in Domain 1 (Military Security) under the CNSDF. Military capability assessments are produced on a regular cycle for key states and on demand for emerging situations.

Role 2: Imagery and Geospatial Intelligence

The CDID processes and analyses satellite and aerial imagery to produce geospatial intelligence — understanding of the physical disposition of foreign military forces, infrastructure, and activities. This means: maintaining a programme of imagery collection on priority targets; building and maintaining databases of foreign military installation locations and characteristics; and providing imagery intelligence support to ESD and ISD operations. Imagery collection against NBI territory requires specific NSCC authorisation and Magister notification.

Role 3: Scientific and Technical Intelligence

CDID scientists and engineers assess foreign scientific and technical programmes with security relevance: foreign weapons development; WMD research and development; satellite and space capabilities; advanced military technology. Scientific and technical intelligence underpins the counter-proliferation work of both the ISD and ESD and provides the technical foundation for NSSP deliberations on nuclear and weapons-related matters.

Role 4: Strategic Warning

The CDID provides strategic warning intelligence — assessing the likelihood and potential timing of major adverse security events including military attack, large-scale terrorism, and WMD use. Strategic warning assessments are provided to the NSCC on a regular basis and to the NSSP when threshold criteria under Technical Schedule B of the CTIA-001 are approached or met. The strategic warning function is specifically designed to prevent surprise — to give the NBI the maximum possible decision time in response to developing threats.

Role 5: Joint Intelligence Assessment

The CDID leads the production of Joint Intelligence Assessments — all-source intelligence assessments that draw on the full range of NBI intelligence collection to address specific strategic questions. Joint Intelligence Assessments are produced when the NSCC requires a comprehensive picture of a developing security situation. They are the primary intelligence product provided to the NSSP for Domain 1, 2, and 3 deliberations. They are produced to the highest analytical standards, with explicit confidence assessments and clear statement of analytical assumptions.

7.3 CDID Staffing and Governance

Section 8: Civic Counter-Terrorism and Extremism Unit (CCTEU)

8.1 Identity and Mandate

The Civic Counter-Terrorism and Extremism Unit (CCTEU) is the NBI's cross-departmental counter-terrorism coordination and intelligence fusion body. It replaces the legacy Counter Terrorism Command, the Joint Terrorism Analysis Centre, and related cross-service counter-terrorism infrastructure. The CCTEU does not replace the operational departments — it coordinates between them, ensuring that counter-terrorism intelligence is properly integrated, assessed, and acted upon.

The CCTEU is not a collection agency. It does not conduct surveillance, run human sources, or gather signals intelligence. Its function is to receive, integrate, assess, and prioritise counter-terrorism intelligence from the ISD, ESD, CSCID, CDID, and from international partners, and to ensure that the right information reaches the right decision-makers at the right time to prevent attacks.

8.2 Roles and Functions — Plain English Specification

Role 1: Intelligence Fusion

CCTEU analysts receive counter-terrorism intelligence from all five NBI security departments and integrate it into a coherent threat picture. This means: matching partial intelligence from different sources to build complete pictures of specific threats and networks; identifying intelligence gaps and directing collection requirements back to the operational departments; and maintaining a live threat picture that reflects the current assessed level of terrorism threat to NBI residents and interests.

Role 2: Threat Assessment and Prioritisation

The CCTEU produces the NBI's national terrorism threat assessment — the overall assessment of the likelihood, nature, and imminence of terrorist attack against NBI targets. This assessment informs: protective security measures across NBI infrastructure; NSSP deliberations in Domain 1 when threat levels reach defined thresholds; Civic Policing Framework operational priorities; and international partner sharing. The threat assessment is updated continuously and provided to the NSCC on a daily basis during periods of elevated threat.

Role 3: Attack Warning

Where CCTEU assessment identifies a credible, imminent threat of terrorist attack, the CCTEU activates the Attack Warning Protocol — a defined escalation process that moves intelligence from assessment into immediate protective action. The Attack Warning Protocol involves: direct notification to the NSCC and relevant NSSP threshold review; alerting Civic Policing and Civic Security bodies; advising the relevant institutions or locations of the threat; and coordinating the intelligence and operational response. All Attack Warning Protocol activations are recorded on the NIN-SIN and reviewed retrospectively by the CSEOP.

Role 4: International Counter-Terrorism Coordination

The CCTEU manages the NBI's participation in international counter-terrorism intelligence sharing arrangements, including those with partner security services and through multilateral bodies approved under the International Civic Compact. International sharing is conducted under the same ethics constraints as domestic operations — the CCTEU does not share intelligence with partners whose use of that intelligence might lead to prohibited treatment of individuals.

Role 5: Counter-Extremism Assessment

The CCTEU assesses the development and spread of ideologies and movements that advocate or enable mass violence, within the specific bounds of its mandate. This is not a general opinion-monitoring function. The CCTEU's counter-extremism role is strictly limited to: assessing movements that are actively engaged in planning or facilitating violence; understanding the pathways from extremist ideology to violent action; and providing intelligence to inform early intervention programmes that are operated independently by civic social services — not by the security services themselves. The CCTEU does not monitor or assess lawful civic advocacy, political dissent, or religious practice, even where these are considered extreme by some.

8.3 CCTEU Staffing and Governance

PART III — GOVERNANCE AND OPERATIONAL ARCHITECTURE

Section 9: National Security Coordination Council (NSCC)

9.1 Purpose and Composition

The National Security Coordination Council (NSCC) is the single inter-departmental governance body that coordinates the activities of all five NBI security departments. It is not a policy-making body — it does not make civic framework decisions. It is an operational coordination body: it ensures the five departments work together coherently, that intelligence priorities are aligned, that resources are allocated rationally, and that no department operates in isolation from the others in ways that create gaps or overlaps in the NBI's security coverage.

The NSCC has no power to authorise operations — authorisation is either through the Magister Warrant system (Section 11) or through the NSA via the CNSDF process. The NSCC sets operational priorities within the bounds established by NSA-approved strategic guidance, coordinating collection requirements, sharing intelligence products, and managing inter-departmental relationships.

9.2 NSCC Functions

- Set and maintain the NBI's integrated intelligence collection priorities, reviewed quarterly and when threat assessments change significantly
- Coordinate intelligence sharing between departments, ensuring that relevant intelligence reaches the department best placed to act on it
- Manage inter-departmental conflicts over jurisdictions, resources, and operational priorities
- Review and approve all requests for international intelligence partnership arrangements before submission to the NSA
- Receive and review ethics compliance reports from each department and refer concerns to the CSEOP
- Produce the annual National Security Assessment — a summary of the NBI's overall security position — for submission to the NSA
- Coordinate the security departments' response to the NSSP during CNSDF sessions

9.3 NSCC Accountability

All NSCC decisions are recorded on the NIN-SIN at the time of the decision. The NSA Liaison Officer receives a weekly summary of NSCC decisions (classified) and reports to the NSA on any matter requiring NSA attention or authorisation. The NSCC does not answer to any individual civic executive body — its accountability runs directly to the NSA through the Liaison Officer and through the NSA investigative access to NIN-SIN.

The NSCC's quarterly intelligence priority assessments are provided to the NSA in summary form (classified summary) and to the CSEOP in full for ethics compliance review. Any NSCC decision that touches on a matter within the CNSDF's six Security Domains is formally notified to the NSSP chair within 24 hours.

Section 10: Magister Warrant Architecture

10.1 The Warrant Principle

All intrusive intelligence activity directed at NBI residents or at communications within NBI territory requires authorisation by an independent Magister. This is not a procedural formality — it is the fundamental mechanism through which the security services are prevented from becoming instruments of state control over the resident body. The Magister is not part of the security services; receives no operational briefings from them except in the context of a specific warrant application; and owes no loyalty to the security services' operational interests.

A Magister Warrant is required for:

- Any interception of a specific NBI resident's communications
- Any covert surveillance of a specific NBI resident's physical movements or activities
- Any access to a specific NBI resident's financial, property, or digital records beyond what is available on the NIN public domain
- Any recruitment or handling of a human intelligence source who is an NBI resident
- Any entry onto or search of premises within NBI territory
- Any technical device placement within NBI territory
- Any interception of bulk communications even of foreign targets where NBI territory infrastructure is used

10.2 Warrant Application Process

Step 1 — Application Preparation

The applying department prepares a written warrant application setting out: the specific individual or premises to be targeted; the specific activity to be conducted; the specific threat category (from the seven in Section 3.2) that justifies the application; the intelligence basis for believing the target is connected to that threat; the necessity assessment (why less intrusive means are insufficient); the proportionality assessment; the duration of the warrant sought (maximum 90 days, renewable); and the recording arrangements that will apply.

Step 2 — Senior Officer Authorisation

The application is reviewed and authorised by the relevant department Director or Deputy Director (not a Case Officer or Section Head). Senior Officer authorisation confirms: that the application is within the department's mandate; that the ethics compliance assessment has been completed; and that the department believes the warrant is justified. Senior Officer authorisation is not sufficient — it is a prerequisite for Magister submission, not a substitute for it.

Step 3 — Independent Magister Review

The application is submitted to an independent Magister drawn from the Civic Warrant Magister pool — a dedicated group of Magisters with specialist knowledge of the legal framework governing security operations. The Magister reviews the application independently of the department, may require additional information or explanation, and may interview the applying officer. The Magister is not a rubber stamp. Where an application fails to demonstrate necessity, proportionality, or specific legal basis, the Magister refuses it.

Step 4 — Magister Decision

The Magister issues a written decision: Grant, Grant with conditions, or Refuse. The decision sets out the Magister's reasoning in sufficient detail to enable meaningful review. Refused applications may be resubmitted with additional evidence. Magisters may not be pressured to expedite decisions on operational grounds — emergency warrant procedures exist (below) for genuinely urgent situations.

Step 5 — NIN-SIN Recording

The complete warrant application, Senior Officer authorisation, Magister decision, and all renewals and closures are recorded on the NIN-SIN at the time of each event. The existence of a warrant is not published on the NIN public portal — it is classified. But its existence, content, and outcome are permanently on the NIN-SIN and fully accessible to the NSA investigative process.

10.3 Emergency Warrant Procedure

Where a genuine emergency requires immediate intrusive action — an imminent attack, an active hostile intelligence operation in progress — the applying officer may seek emergency Magister authorisation by direct contact with the on-call Civic Warrant Magister. The emergency procedure allows verbal authorisation followed by written confirmation within 4 hours. Emergency authorisation must still satisfy all five ethics principles. An emergency warrant obtained on insufficient grounds is treated with equal severity to an operation conducted without any warrant.

10.4 Warrant Review and Renewal

All warrants are issued for a maximum initial period of 90 days. Renewal requires a fresh Magister review with updated intelligence basis — renewal is not automatic. The Magister may refuse renewal if the intelligence basis has not been maintained. All warrants are reviewed at closure: the department records on the NIN-SIN what activity was conducted under the warrant, what intelligence was gathered, and how it was used. Warrant closure reviews are available to the CSEOP for ethics compliance assessment.

Section 11: NIN Secure Intelligence Network (NIN-SIN)

11.1 Constitutional Status

The NIN Secure Intelligence Network (NIN-SIN) is the classified partition of the National Information Network dedicated to the security services. It is not a separate system — it is a structurally partitioned domain within the NIN, operating under enhanced security protocols and subject to the most stringent access controls in the NBI's information architecture. It is owned, in its entirety, by the National Sortition Assembly on behalf of the NBI resident body. The security services hold NIN-SIN content in a custodial capacity only — they are the authors and users of the content, but they do not own it and they cannot control what happens to it in the long term.

11.2 The Write-Once Principle

Every document, record, report, assessment, warrant application, source record, operational log, and communication created by any security department officer in the course of their duties is written to the NIN-SIN once, at the time of creation, and cannot thereafter be amended, copied outside the partition, deleted, or removed by any means. This is the foundational accountability mechanism of the NBI security architecture.

The write-once principle means:

- No intelligence record can be altered after the fact to conceal an operational failure, a legal breach, or a prohibited action
- No source can be burned retrospectively by altering the records of how they were recruited and what they were told
- No warrant application can be adjusted after a Magister refusal to make it appear more compliant
- No operational outcome can be misrepresented in the historical record
- The NIN-SIN contains the true record of what the security services did, in the order they did it, without the possibility of subsequent revision

11.3 Access Architecture

Access to the NIN-SIN is the most stringently controlled operation in the NBI security architecture. Three levels of access exist:

11.4 Classification Architecture

All NIN-SIN content carries a single classification caveat: NSA ONLY — TOP SECRET. No other classification caveat is used on NIN-SIN content. No content is marked "eyes only" for individual officers, "not to be shared with NSA", or with any caveat that restricts NSA investigative access. No sub-classification system within the NIN-SIN is permitted.

The classification "NSA ONLY — TOP SECRET" means:

- The content is not published on the NIN public portal
- The content is accessible only to security department personnel with Level 1 or Level 2 access in the course of their authorised duties
- The content is accessible to the NSA under formal investigative mandate
- The content may not be shared with any individual, body, or foreign government outside these categories without explicit NSA authorisation

- The NSA is the sole authority for any release of NIN-SIN content beyond its normal access architecture

11.5 Mandatory Recording Obligations

The following must be recorded on the NIN-SIN at the time they occur. Recording is not a matter of operational discretion — it is an absolute obligation. Failure to record constitutes a breach of the ethics architecture and activates the Civic Consequence pathway.

Section 12: Personnel Architecture — Vetting, Recruitment, and Ethics

12.1 The Personnel Security Challenge

Security services are uniquely vulnerable to insider threat: an officer who is compromised, motivated by ideology, or operating for personal gain can cause more damage than almost any external adversary. The NBI personnel security architecture addresses this through a combination of rigorous initial vetting, continuous assessment, ethical culture, and recording obligations that make insider misconduct very difficult to conceal. The architecture does not assume good faith and then react when it is violated — it builds in continuous verification as a structural feature of employment.

12.2 Security Vetting Framework

All security department personnel are subject to the following vetting levels, applied to the relevant role:

Vetting is renewed at 5-year intervals for CSV and 3-year intervals for ECSV, and immediately on any significant change of personal circumstances. All vetting decisions are recorded on the NIN-SIN. A failed vetting result is not published — but it is accessible to the NSA investigative process.

12.3 Absolute Bars to Employment

The following are absolute bars to employment in any security department. They cannot be waived on operational grounds.

- Current or prior membership of any Category A–H prohibited organisation as defined in DD&SA-CTIA-001
- Any prior association with a foreign intelligence service in an agent, source, or collaborative capacity
- Any criminal conviction for an offence involving dishonesty, violence, breach of trust, or national security
- Any undisclosed conflict of interest that cannot be fully resolved through the Civic Transparency Declaration process
- Failure to complete a Civic Transparency Declaration or material omission from a completed CTD
- Prior employment in any intelligence service of a state assessed as hostile to the NBI

12.4 Continuous Personnel Security

Personnel security does not end at recruitment. All security department staff are subject to continuous personnel security monitoring, which includes:

- Annual personal circumstance update — all staff report any significant changes in financial position, personal relationships, foreign contacts, or other relevant circumstances
- Anomaly detection — NIN-SIN access patterns are automatically monitored for behaviour inconsistent with authorised roles; anomalies trigger review, not automatic action
- Line manager assessment — all staff receive a documented annual security assessment from their line manager
- Reporting obligation — all staff have a duty to report to their ethics compliance officer or directly to the CSEOP any approach by a foreign intelligence service, any attempt at bribery or coercion, and any knowledge of prohibited conduct by a colleague

12.5 Legacy Service Personnel Transition

Personnel from the legacy security services (MI5, MI6, GCHQ, and related bodies) may apply to transfer to the equivalent NBI security department. Transfer is not automatic. Each transferring officer undergoes a full vetting assessment under the new framework, a DD&SA ethics compliance assessment, and a review of their conduct record under the legacy service. Officers with records of conduct inconsistent with the DD&SA ethics architecture are not eligible for transfer. All legacy service personnel transfer records are held on the NIN-SIN.

Critically: all intelligence records from legacy services that are transferred to NBI custody are assessed for their compliance with the NBI ethics architecture. Records obtained through prohibited means — torture, coercion, unlawful surveillance — are flagged, held separately on the NIN-SIN, and not operationally used pending NSA review. Their existence is recorded and they are not destroyed, because their existence is part of the historical record.

Section 13: Resident Rights and Protections

13.1 The Resident’s Position Under This Framework

Every NBI resident has a right to live without the security services monitoring their private life, their communications, their associations, or their civic activity, unless a Magister has specifically authorised such monitoring on the basis of specific intelligence connecting that resident to one of the seven authorised threat categories. This right is not qualified by national security interests — it is the precondition of legitimate national security work. A security service that can surveil any resident, at any time, on any grounds, is not a security service; it is an apparatus of control.

13.2 Resident Rights Under This Framework

The following rights apply to every NBI resident in relation to the security services:

Right 1 — Freedom from Unlawful Surveillance

Every NBI resident has the right not to be surveilled, monitored, or investigated by any security department without a Magister Warrant. This right is absolute. No security department may conduct surveillance of a resident on the basis of an administrative decision, an operational assessment, or a senior officer’s direction alone — Magister authorisation is always required.

Right 2 — Right to Know of Past Surveillance

Every NBI resident who has been the subject of a security department operation has the right to be notified of that fact after the operation has concluded and the intelligence obtained is no longer operationally sensitive. The NSCC determines when notification is operationally safe. Notification must occur within 5 years of the operation's conclusion in all circumstances, regardless of operational sensitivity assessments. Notification is limited to the fact of the operation and its general nature — it does not include the content of intelligence gathered or the identities of sources. Notification is recorded on the NIN-SIN.

Right 3 — Right to Challenge Unlawful Action

Any NBI resident who believes they have been subjected to unlawful surveillance or unlawful action by a security department may submit a formal complaint to the CSEOP (Section 17). The CSEOP has access to the NIN-SIN under its specific mandate to investigate complaints. Where a complaint is substantiated, the CSEOP refers the matter to the NSA and to the relevant Magister. The resident receives a written response — necessarily limited in classified detail — confirming whether the complaint was upheld.

Right 4 — Right to Civic Advocate Representation

Any NBI resident who is interviewed by a security department officer in connection with an investigation has the right to have a Civic Advocate present. This right cannot be waived by the security department on operational grounds. Where the presence of a Civic Advocate during an interview would compromise a specific operational need, the matter is referred to a Magister for a specific ruling on whether the interview may proceed without an advocate on a one-off basis. Such rulings are recorded on the NIN-SIN.

Right 5 — No Action on the Basis of Protected Characteristics

No security department operation may target a resident on the basis of their race, ethnicity, religion, national origin, gender, sexual orientation, disability, or any other protected characteristic, unless that characteristic is a directly relevant identifying feature of a specific, evidence-based operational target who has been connected to one of the seven threat categories by specific intelligence. Targeting a community rather than an individual on the basis of shared religious or ethnic characteristics is absolutely prohibited.

Section 14: Whistleblower Architecture

14.1 The Security Service Whistleblower's Position

Intelligence officers are in a unique position with respect to whistleblowing: they have seen things that no one else has seen, they are bound by obligations of secrecy that are stricter than almost any other profession, and they work in an environment where institutional culture can make it very difficult to challenge wrongdoing. Legacy security services have a poor historical record on whistleblowing — officers who raised concerns about unlawful conduct have frequently been prosecuted, dismissed, or discredited.

The NBI security architecture treats whistleblowing as essential to system integrity, not as a threat to it. An intelligence officer who identifies and reports a breach of the ethics architecture, an unlawful operation, or an Inviolable Constitutional Limit violation is performing one of the most valuable security functions available. The whistleblower architecture exists to make that function safe, reliable,

and effective.

14.2 Protected Whistleblowing Channels

- Direct report to the CSEOP through a dedicated encrypted NIN-SIN channel — the only body with guaranteed access to the report, which the reporting officer's department cannot read
- Direct report to the NSA Liaison Officer through a channel that bypasses the NSCC entirely
- Direct sealed report to a Civic Warrant Magister where the concern relates to warrant fraud or misrepresentation
- Direct sealed report to the NSA through the CNSDF whistleblower channel established under DD&SA-CTIA-001, Section 12.2

14.3 Absolute Protections

Any security department officer or employee who makes a report through any of the channels above is entitled to the following protections, which are absolute and non-waivable:

- Identity protection: the reporting officer's identity is known only to the CSEOP or the channel recipient, and cannot be disclosed to the department under investigation without the officer's consent
- Employment protection: no adverse employment action — transfer, demotion, dismissal, withdrawal of vetting clearance, or any other measure — may be taken against the reporting officer in connection with their report
- Civic standing protection: no adverse civic consequence may flow from the act of reporting in good faith
- Legal protection: the reporting officer cannot be prosecuted for breach of secrecy obligations in connection with a good-faith disclosure through an approved channel
- Retaliation prohibition: any act of retaliation against a security services whistleblower activates the highest-tier Civic Consequence pathway and is referred to the NBI criminal architecture

14.4 External Disclosure

The whistleblower architecture does not extend to public disclosure of classified intelligence. An officer who discloses classified intelligence publicly — to a journalist, to a foreign government, or otherwise — is not protected by this Framework, regardless of their stated justification. The distinction is: disclosure through the approved channels in this section, which routes concerns to accountable civic oversight; versus disclosure that bypasses oversight entirely and exposes classified intelligence to actors who are not part of the NSA accountability architecture. The first is protected and encouraged. The second is not protected and may constitute a criminal offence.

PART IV — ACCOUNTABILITY, FAILURE MODES, AND INTEGRATION

Section 15: Civic Security Ethics and Oversight Panel (CSEOP)

15.1 Composition and Independence

The Civic Security Ethics and Oversight Panel (CSEOP) is the permanent resident-accountability mechanism for all five NBI security departments. It is an independent body, staffed entirely through sortition, reporting only to the NSA. No security department has any operational relationship with the CSEOP beyond compliance with its requests and reports. The CSEOP is not a management body — it does not set operational priorities, approve operations, or direct the security services. It monitors whether the security services are operating within the ethics architecture and the constitutional limits established by this Framework.

15.2 CSEOP Powers and Functions

- Quarterly ethics compliance audit of all five departments, with NIN public portal publication of findings within 30 days of completion
- Access to NIN-SIN Ethics Compliance Records (ECRs) for all operations, under specific CSEOP access mandate
- Receipt and investigation of resident complaints under Section 13.3 — full NIN-SIN access for the specific case under investigation
- Receipt and investigation of whistleblower disclosures under Section 14.2
- Review of all warrant closure records — access to warrant application, Magister decision, and operational log for any closed warrant
- Referral to the NSA of any matter requiring NSA attention, including any identified breach of an Inviolable Constitutional Limit
- Publication of an Annual Security Ethics Report on the NIN public portal — a comprehensive account of the CSEOP's work, findings, and recommendations

15.3 What the CSEOP Cannot Do

The CSEOP is not an operational body and may not direct security operations, interfere with active Magister Warrant operations, or make decisions on behalf of the NSA. Its function is to monitor and report — not to run the security services. Where the CSEOP identifies a serious ethics breach, it refers to the NSA; it does not itself impose consequences.

Section 16: NSA Oversight and Investigative Access

16.1 The NSA's Role

The National Sortition Assembly is the ultimate accountability body for all five NBI security departments. This Framework uses the NSA's investigative access to the NIN-SIN as the primary accountability mechanism — not regular inspection, not annual review, but the certain knowledge of every security services officer that every action they take is permanently recorded and accessible to the NSA. The deterrent effect of unconditional accountability is more powerful than any inspection regime.

16.2 NSA Investigative Mandate Process

The NSA may initiate an investigation into any aspect of any security department's activities by passing a formal investigative mandate by simple majority vote. The mandate is published on the NIN public portal. A dedicated NSA Security Investigative Panel (NSIP-S) is assembled by sortition from the NSA membership, with no members from the original vetting of the departments under investigation. The NSIP-S accesses the relevant NIN-SIN records at designated terminals, produces a classified report for the NSA, and a public summary (appropriately redacted for operational security) for the NIN public portal.

16.3 Annual Security Accountability Session

In addition to the investigative mandate process, the NSA holds an Annual Security Accountability Session: a classified briefing from the NSCC, covering the overall security threat picture, departmental performance, and any significant operational failures or ethics breaches in the preceding year. The CSEOP Annual Ethics Report is tabled at this session. A public summary of the session — covering the overall threat assessment and headline accountability findings — is published on the NIN public portal within 14 days.

16.4 NSA Authorisation Requirements

The following security activities require explicit NSA authorisation, not merely NSCC approval:

- All offensive operations — covert action, offensive cyber, and any operation involving potential harm to persons
- All intelligence sharing arrangements with foreign services
- Any operation targeting a current or former NSA member, Magister, or senior civic role-holder
- Any operation involving WMD-related activity
- Any operation in a foreign country that involves partnering with a foreign security or military service
- Any significant expansion of the security services' technical collection capabilities

Section 17: Failure Mode Analysis

17.1 Security Services Failure Modes

Failure Mode 1: Mission Creep into Political Surveillance

Description: Security services gradually expand their definition of "threat" to encompass civic dissent, political opposition, or controversial but lawful civic activity — reproducing the legacy pattern of political policing.

Likelihood: High without structural countermeasures. Every legacy security service has done this.

Countermeasures: The seven specific threat categories in Section 3.2 are constitutionally bounded — they cannot be expanded without NSA supermajority vote. The explicit prohibitions in Section 3.3 are operative rather than aspirational. The Magister Warrant requirement for all resident surveillance means that mission creep requires a Magister to approve unlawful targeting — which the Magister is constitutionally independent and has no incentive to do. The CSEOP specifically reviews warrant patterns for evidence of politically motivated targeting.

Failure Mode 2: Source Protection Used to Conceal Wrongdoing

Description: Security departments invoke source protection to withhold evidence of their own misconduct from the CSEOP, the NSA, or the Magister system — claiming that revealing the record would compromise a human intelligence source.

Likelihood: Moderate. This has historically been a common mechanism for concealing security service abuses.

Countermeasures: Source protection codes on the NIN-SIN protect source identities, not operational records. The NSA's investigative access to the NIN-SIN is absolute — source protection codes do not prevent NSA access; they flag the relevant sections as requiring special handling. The NSA investigative panel may read source records without the source identity being disclosed outside the secure terminal environment. Source protection is not a shield against accountability.

Failure Mode 3: Warrant System Gaming

Description: Security departments manage or shape the information provided to Magisters to obtain warrants they would not receive if the Magister had the full picture — selectively presenting intelligence, overstating threat levels, or omitting exculpatory information.

Likelihood: High without countermeasures. This has been documented across multiple legacy warrant systems.

Countermeasures: All warrant applications are recorded on the NIN-SIN write-once at the point of submission — they cannot be altered after submission. The Magister has direct NIN-SIN access to check the cited intelligence basis. Warrant closure reviews examine whether the intelligence basis cited at application was accurate. The CSEOP quarterly review specifically examines the relationship between warrant applications and the intelligence basis cited. An officer found to have misrepresented information to a Magister faces the maximum Civic Consequence pathway.

Failure Mode 4: Security Service Capture of the CSEOP

Description: Security services develop informal relationships with CSEOP members that compromise the Panel's independence — through briefings, access, and the natural tendency of oversight bodies to identify with the institutions they oversee.

Likelihood: Moderate. Short non-renewable sortition terms limit this significantly.

Countermeasures: CSEOP members serve 18-month non-renewable terms — insufficient time for deep institutional capture. All CSEOP contact with security departments is logged on the NIN-SIN. CSEOP members complete full CTD declarations before and after service. The NSA independently reviews CSEOP Annual Reports for any signs of capture — reviewing whether the CSEOP's findings are consistent with the NIN-SIN records it has accessed.

Failure Mode 5: NIN-SIN Recording Gaps

Description: Officers conduct operational activities "informally" — in conversations, by phone, in unrecorded meetings — with the intention that these activities never reach the NIN-SIN, while only the sanitised version is recorded.

Likelihood: Moderate. This is a perennial problem in intelligence services — the "back-channel" culture.

Countermeasures: The NIN-SIN access log records every login, every document created, and the timestamp of every entry. Pattern analysis can identify officers whose NIN-SIN activity is inconsistent with their operational responsibilities — too sparse relative to their caseload. Line managers are specifically tasked with monitoring the completeness of their staff's recording. Whistleblower channels specifically cover recording omissions. Any gap in the record that is identified — whether through audit, whistleblowing, or NSA investigation — results in immediate referral and investigation.

Failure Mode 6: Foreign Intelligence Partner Exploitation

Description: Foreign intelligence services use the NBI's liaison relationships to access NBI domestic intelligence — information about NBI residents that was gathered under Magister Warrant and shared with foreign partners who then use it for purposes incompatible with NBI ethics.

Likelihood: High. This is a documented pattern across "Five Eyes" and similar arrangements — services using alliance structures to conduct surveillance on each other's residents that each service could not lawfully conduct domestically.

Countermeasures: All intelligence shared with foreign partners is documented on the NIN-SIN with the recipient, the content shared, and the authorised purpose. Foreign partners may not be given intelligence about NBI residents beyond what is specifically authorised under a bilateral agreement reviewed by the NSA. "Passing back" arrangements — where NBI intelligence is given to a foreign service that then provides it back to the NBI in a form that avoids domestic warrant requirements — are explicitly prohibited. Any intelligence received from a foreign service that relates to an NBI resident triggers automatic notification of the relevant Magister.

Section 18: Integration with the DD&SA Constitutional Architecture

18.1 Instrument Crosswalk

18.2 The Authorial Signature

"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 Security and Intelligence Architecture (DD&SA-CSIA-001)

Edition 1.0 | April 2026

— END OF DOCUMENT —