THE REVERE CIVILIAN OVERSIGHT INTELLIGENCE FRAMEWORK

Monitoring & Documenting Federal Law Enforcement Conduct

A Reference Guide for Organized, Nonviolent Civilian Accountability Groups

Applying Intelligence Principles to Lawful Public Oversight

LEGAL NOTE	*Everything in this document concerns lawful, First Amendment-protected activity: observing, recording, and reporting on government officials conducting official duties in public spaces. Nothing here constitutes legal advice. Consult qualified legal counsel for jurisdiction-specific guidance.*

PART I: FOUNDATIONAL PRINCIPLES

1.1 Purpose and Legal Foundation

Civilian oversight of law enforcement is a cornerstone of democratic governance. Courts have repeatedly affirmed that citizens have a First Amendment right to record and observe police and federal agents in public spaces while performing official duties. This framework adapts intelligence discipline — the structured, systematic approach to collecting and analyzing information — to the needs of organized community accountability groups.

The goal is not confrontation. It is documentation: creating reliable, admissible, legally defensible records of patterns, incidents, and conduct that may constitute abuse of authority, civil rights violations, or unlawful overreach.

CORE MISSION	*To observe, record, analyze, and report on the presence, tactics, and conduct of federal law enforcement in a defined geographic area, in order to support public accountability, legal action, journalism, and civil rights protection.*

1.2 The Intelligence Cycle — Adapted for Civilian Oversight

Military and professional intelligence operations follow a structured cycle. Civilian oversight groups benefit from the same discipline:

- PLANNING: Define your collection requirements. What specific conduct are you monitoring? What geographic area? What agencies?
- COLLECTION: Systematic gathering of observations, video, photographs, testimonies, and public records.

- PROCESSING: Organizing raw data into usable formats — logs, databases, timelines, maps.
- ANALYSIS: Identifying patterns, trends, anomalies, and correlations across collected information.
- DISSEMINATION: Sharing findings with legal teams, journalists, oversight bodies, and the public in appropriate formats.
- FEEDBACK: Evaluating what worked, what gaps exist, and refining your approach.

1.3 The Concept of a "Theater of Operations"

In military intelligence, a "theater of operations" is the defined geographic area of active activity. For civilian oversight purposes, this concept is essential for focused, systematic monitoring. A well-defined theater:

- Has clearly mapped boundaries (streets, neighborhoods, jurisdictions)
- Includes identified fixed points of interest: federal buildings, detention facilities, known staging areas
- Is subdivided into sectors that can be assigned to individual observers
- Has documented access points, transit corridors, and likely activity zones

Defining your theater is the first operational step. Everything else — personnel assignments, collection plans, communication protocols — flows from it.

PART II: GLOSSARY OF KEY TERMS

The following terms are drawn from professional intelligence and law enforcement tradecraft, adapted here for lawful civilian oversight contexts.

Actionable Intelligence

Information that is specific, credible, timely, and detailed enough to support a concrete decision or response. In civilian oversight, actionable intelligence means documentation sufficient to support a legal complaint, press report, or advocacy action — e.g., timestamped video of a specific agent using force without legal basis, with badge/vehicle identifiers.

After-Action Report (AAR)

A structured post-event analysis documenting what was planned, what occurred, what was documented, and what lessons should be applied to future operations. AARs are essential for organizational learning and for building a longitudinal record of patterns over time.

Area of Interest (AOI)

The broader geographic region relevant to your monitoring mission, extending beyond your immediate theater. Activity or information originating in the AOI may affect conditions within your theater.

Area of Operations (AO)

The specific, defined geographic zone where your group actively conducts monitoring. Distinct from the broader Area of Interest.

Asset

In civilian oversight context: an observer, documentarian, or resource assigned to a specific collection role. Assets should be assigned to defined positions or tasks, briefed on their specific collection objectives, and debriefed after each deployment.

Collection Requirements

The specific categories of information your group has decided it needs to collect. Examples: agency identification, use-of-force incidents, detention without visible process, vehicle staging patterns, communication with local law enforcement. Defining collection requirements prevents unfocused monitoring and ensures documentation is legally useful.

Corroboration

The confirmation of one piece of information by an independent, separate source. A single observer's account is evidence; the same account independently confirmed by video, a second witness, and a public records request becomes much stronger. All collection efforts should build toward corroboration.

Counter-Surveillance Awareness

The recognition that the subjects of your monitoring may themselves surveil your group. Federal law enforcement agencies routinely document and photograph civilians who are documenting them. This is lawful on both sides. Observers should be aware of this dynamic, maintain professional conduct at all times, and never take actions that could be construed as threatening or obstructive.

Credibility Assessment

An evaluation of the reliability and accuracy of a piece of information or a source. Intelligence tradecraft rates both source reliability (how consistently has this source proven accurate?) and information credibility (how plausible is this specific claim given other known facts?). Apply this discipline to all collected information before acting on it.

Secure Handoff

A method of transferring documentation, video files, or sensitive materials without direct contact, used to protect both the material and the people involved. For civilian oversight groups handling sensitive documentation, secure handoff protocols protect observers and preserve chain of custody for evidence.

Escalation Indicators

Observable signs that federal law enforcement activity in your theater is increasing in intensity, scope, or nature. Examples include: increased vehicle presence, deployment of specialized units (e.g., tactical teams), use of unmarked vehicles, establishment of forward staging areas, or coordination with local law enforcement.

Ground Truth

Direct, firsthand, observed information, as opposed to secondhand reporting or inference. Video and photographs from observers who were physically present constitute ground truth. It is the most valuable and defensible form of documentation.

Human Intelligence (HUMINT)

Intelligence derived from human sources: eyewitness accounts, interviews with community members, testimony from individuals who have directly experienced the conduct being documented. In civilian oversight, HUMINT includes statements from people who were detained, photographed, questioned, or subjected to enforcement actions.

Indicator

A specific, observable fact or condition that provides evidence a particular event is occurring or is likely to occur. "Three unmarked white SUVs parked outside the federal building at 0600" is an indicator of possible enforcement activity. Indicators should be defined in advance so observers know what to look for.

Intelligence Preparation of the Environment (IPE)

The process of systematically analyzing your theater before deploying observers. IPE involves mapping the physical terrain, identifying federal facilities and staging areas, researching agency jurisdiction and legal authority in your area, and anticipating likely activity patterns. A thorough IPE allows more effective and safer observer deployment.

Log / Observation Log

A contemporaneous, timestamped written record of what an observer sees, hears, and documents. Observation logs are foundational to any accountability operation. They should include: date, time, location (GPS if possible), observer identity, weather/light conditions, description of subjects/vehicles/actions, and cross-reference to any photographs or video captured.

Mission Creep

The gradual expansion of an operation's scope beyond its original, defined objectives. Mission creep is a serious risk for civilian oversight groups. It can dilute effectiveness, create legal exposure, and undermine the discipline that makes documentation credible and defensible.

Open Source Intelligence (OSINT)

Intelligence gathered from publicly available sources: court filings, federal agency press releases, local news reports, social media, public records requests (FOIA), property records, and other accessible data. OSINT is lawful, ethical, and often highly productive. It should form the analytical backbone of any civilian oversight operation.

Operational Security (OPSEC)

The practice of protecting your group's methods, plans, personnel, and information from being observed, compromised, or exploited. OPSEC is relevant even for entirely lawful civilian operations: if federal agencies know in advance where your observers will be, they may adjust behavior accordingly, reducing documentation value.

Table of Organization and Equipment (TOE)

A record of forces, their composition, and capabilities. Adapted for civilian oversight: a running reference document recording all federal law enforcement agencies known to be operating in your theater, their observable resources (vehicles, personnel counts, equipment), identified operating locations, and observed tactics.

Pattern of Life (POL) Analysis

The systematic analysis of routine behavior patterns over time. Documenting that federal agents follow predictable routines — staging at certain locations at certain times, operating in specific neighborhoods on specific days — provides the foundation for anticipating future activity and detecting anomalous escalations.

Rules of Engagement (ROE)

In civilian oversight: the explicit, agreed-upon guidelines governing how your observers conduct themselves in the field. ROE should define lawful conduct, prohibited conduct, how to respond to law enforcement contact, when to withdraw, and how to handle evidence. Every observer must know and follow your group's ROE.

Sensitive Site Exploitation (SSE)

Adapted for civilian use: the systematic documentation of a location where a significant enforcement action occurred — photographing the physical environment, collecting witness accounts, documenting physical evidence visible in public space — to create a complete record of what transpired at that location.

Situational Awareness (SA)

The continuous, real-time understanding of your operational environment: where your observers are, what federal law enforcement is doing, what the surrounding community is experiencing, and how conditions are developing. SA requires disciplined communication protocols between observers, a designated coordinator tracking the overall picture, and regular status updates.

Source Protection

The protocols and practices used to protect the identity and safety of individuals who provide information to your group — especially community members who may be at risk from federal law enforcement. Source protection is both an ethical obligation and a legal consideration.

Standing Intelligence Requirements (SIR)

The standing, ongoing collection requirements that are always active, regardless of specific current events. Example SIRs for a civilian oversight operation might include: always document all federal vehicles in the theater; always record any visible use of force; always collect agency/unit identifiers from any uniformed personnel observed.

Theater of Operations

The defined geographic area in which your monitoring operation is conducted. A clearly bounded theater enables systematic coverage, efficient resource deployment, and meaningful pattern analysis over time.

Threat Assessment

An analysis of risks to your observers' safety and legal standing, and to the integrity of your documentation. A responsible civilian oversight operation conducts ongoing threat assessment: what legal risks do our observers face in this theater? What conditions might create safety risks? What factors could compromise our documentation?

Time-Sensitive Intelligence

Information that loses value rapidly if not acted upon. A report of an ongoing use-of-force incident is time-sensitive. Pattern documentation of routine staging activity is not. Recognizing which information is time-sensitive and which is long-value helps your group prioritize and respond appropriately.

Unmanned Aerial Vehicle (UAV) / Drone Considerations

Consumer drones may be used for aerial documentation in some circumstances, but are subject to FAA regulations, airspace restrictions, and potential legal restrictions around federal facilities. Consult legal counsel and FAA regulations before using drones. Unauthorized UAV operations can create serious legal exposure and discredit an otherwise well-documented accountability effort.

PART III: OPERATIONAL FRAMEWORK OUTLINE

Phase 1: Intelligence Preparation of the Environment (IPE)

1A. Theater Definition

- Define precise geographic boundaries of your AO
- Subdivide into sectors; assign sector leads
- Map all federal facilities, detention sites, and known staging areas
- Identify choke points, transit corridors, and high-activity zones
- Document access routes and observer positioning options

1B. Agency Research (OSINT)

- Identify all federal agencies with jurisdiction in your theater: FBI, DHS, ICE, CBP, ATF, USMS, etc.
- Research each agency's legal authority, limitations, and oversight mechanisms
- Review recent court decisions on federal law enforcement authority in your jurisdiction
- Collect FOIA-accessible records on agency activity in your area
- Identify Inspector General offices and oversight bodies for each agency

1C. Legal Framework Research

- Document your state's laws on recording law enforcement in public
- Identify applicable federal statutes and constitutional protections
- Research relevant precedents on obstruction, interference, and observer rights
- Establish relationship with legal observer organizations (e.g., NLG, ACLU)

Phase 2: Collection Planning

2A. Define Standing Intelligence Requirements

- All federal vehicle types, plate numbers, and markings observed in theater
- All uniformed personnel: agency, unit markings, visible badge/ID numbers
- All observable enforcement actions: detentions, arrests, searches, use of force
- All communication with or presence of local/state law enforcement
- All visible equipment: weapons, less-lethal munitions, surveillance gear

2B. Observer Roles and Assignment

- Fixed position observers: assigned to specific high-value locations (known staging areas, detention facility perimeters)
- Mobile observers: vehicle or foot teams that can reposition to emerging activity
- Documentation specialists: assigned specifically to video/photo capture; distinct from written log observers
- Legal observers: trained specifically on legal documentation protocols; typically maintain separate records

- Coordinator/analyst: maintains overall situational awareness; not deployed in field; synthesizes incoming reports

2C. Equipment and Documentation Standards

- Video: encrypted storage, timestamping enabled, GPS metadata enabled where possible
- Photography: same standards; multiple angles; wide establishing shots plus close detail
- Written logs: standardized form with required fields; entries made contemporaneously (not from memory after the fact)
- Proper kit: goggles, car camera, first aid kit, burner phone, etc.

Phase 3: Active Collection Operations

3A. Observation Protocols

- Observers maintain legal positioning at all times — never obstruct, interfere, or enter restricted areas
- Continuous log entries at minimum 15-minute intervals during active operations; event-driven entries for any observed activity
- Four-observer team rule for high-risk positions where practicable: one documents, one maintains situational awareness, one vid/photographer, one stand back videoing team
- Predetermined withdrawal criteria: if legal exposure escalates, observers withdraw; documentation never justifies arrest

3B. Communication Protocols

- Encrypted communications for all operational coordination (Signal or equivalent)
- Regular check-in schedule: coordinator pings all field positions on defined interval
- Brevity codes for common reports to reduce communication time
- Emergency protocols: defined signal for immediate withdrawal; designated rally point; legal support contact on standby

3C. Handling Law Enforcement Contact

- Observers know their rights: right to record, right to remain silent, right to refuse consent to search
- All observer interactions with federal agents are themselves documented
- Legal observer contacts legal support immediately upon any detention or arrest of an observer
- No observer acts alone, ever, when approached by federal agents if avoidable

Phase 4: Processing and Analysis

4A. Data Processing

- All field logs transcribed and entered into centralized database within 24 hours of collection
- All video and photo media inventoried, timestamped, and catalogued
- Each incident logged with: date, time, location, involved agents (descriptions/identifiers), actions observed, documentation collected, witnesses
- Duplicate and backup copies stored in geographically separate, encrypted locations

4B. Pattern Analysis

- Weekly review of all collected data for emerging patterns
- Generate: timeline analysis, geographic heat maps of activity, agency activity frequency charts
- Flag anomalies: departures from established patterns; new equipment; new personnel; changes in tactics
- Cross-reference with OSINT: court filings, press reports, FOIA responses

4C. Product Development

- Incident reports: detailed records of individual enforcement events, suitable for legal use
- Pattern analysis reports: analytical products (ex: HEAT maps) documenting trends across time and geography
- Briefing materials: summaries for journalists, oversight bodies, elected officials, legal teams
- Evidentiary packages: organized documentation compilations supporting specific legal complaints

Phase 5: Dissemination

5A. Legal Channels

- Department of Justice Civil Rights Division complaints
- FBI Office of Professional Responsibility
- Agency-specific Inspector General offices
- State Attorney General civil rights divisions
- Private civil rights litigation support

5B. Public Accountability Channels

- Journalism: provide documentation packages to beat reporters and investigative journalists
- Advocacy organizations: ACLU, NLG, PCLOB, relevant policy organizations
- Elected officials: congressional oversight committees, constituent services offices
- Public reporting: community briefings, public records, transparency publications

PART IV: KEY TRENDS AND INDICATORS TO WATCH

Systematic monitoring is only as valuable as the analytical framework applied to what you collect. The following are key trend categories that experienced civilian oversight practitioners and civil rights investigators have identified as meaningful indicators of escalation, abuse, or unlawful conduct.

4.1 Force and Tactics Trends

- Escalation in visible equipment: deployment of tactical gear, less-lethal munitions (rubber bullets, tear gas, pepper spray), armored vehicles
- Changes in force application: shift from verbal commands to physical force; use of pain compliance techniques; use of restraints beyond standard handcuffing
- Crowd control tactics: use of kettling (encircling groups), mass arrest procedures, dispersal tactics against peaceful assemblies
- Less-lethal becoming a primary tactic rather than a last resort before lethal force

4.2 Detention and Due Process Trends

- Detentions without visible legal process: individuals taken without visible warrant, probable cause articulation, or Miranda warnings
- Extended detentions: individuals held for periods disproportionate to the stated offense or with no stated offense
- Detention location patterns: use of non-standard detention facilities; transfer to out-of-jurisdiction facilities; use of vehicles rather than established detention centers
- Denial of legal access: attorneys prevented from contacting detained clients; individuals denied opportunity to contact counsel
- Unmarked or covert detention: use of plainclothes agents and unmarked vehicles for arrests; detentions with no agency identification provided

4.3 Surveillance and Intelligence Collection Trends

- Photography of civilians not engaged in any unlawful conduct
- Use of facial recognition technology, license plate readers, or other automated surveillance in public spaces
- Deployment of surveillance aircraft or drones over civilian areas
- Social media monitoring and documentation collection targeting specific communities or political groups
- Presence of Joint Terrorism Task Force (JTTF) personnel outside counterterrorism contexts

4.4 Jurisdictional and Authority Trends

- Federal presence in areas not within traditional federal jurisdiction without visible lawful basis
- Federal agents operating alongside local/state law enforcement in ways that may circumvent state-level restrictions
- Expansion of operations into new geographic areas or against new communities without apparent legal predicate
- Invocation of authority statutes (e.g., 40 USC 1315) to operate in non-federal-property contexts
- Interagency task forces: the formation or activation of multi-agency operations that may obscure individual accountability

4.5 Targeting and Disparate Impact Trends

- Demographic patterns in enforcement: documenting whether enforcement actions are disproportionately directed at specific racial, ethnic, religious, or political communities
- Geographic concentration: whether operations are systematically concentrated in particular neighborhoods
- Event-based targeting: whether enforcement activity escalates around political events, protests, or public assemblies
- Individual targeting: repeated enforcement contact with the same individuals, suggesting targeted harassment rather than neutral law enforcement

4.6 Transparency and Accountability Trends

- Refusal to identify: agents declining to provide name, badge number, or agency
- Obstruction of documentation: agents ordering observers to stop recording, physically interfering with recording, or seizing recording equipment
- Communication suppression: jamming or interfering with civilian communications during operations
- Media exclusion: press being denied access to public spaces during operations
- FOIA non-compliance: patterns of delayed, withheld, or incomplete responses to public records requests

4.7 Escalation Pattern Recognition

The following sequence of indicators has historically preceded significant escalations in federal law enforcement operations. Monitor for this pattern:

Stage	Indicator	What to Document
1	**Reconnaissance**	Increased plainclothes presence; observation of community gathering places; photography of activists or community leaders

2	**Staging**	Deployment of vehicles and personnel to pre-positioned locations; establishment of command posts; coordination with local agencies
3	**Isolation**	Restriction of access to specific areas; media exclusion; blocking of exit routes
4	**Action**	Arrests, detentions, dispersals, use of force; covert or overt operations against specific targets
5	**Consolidation**	Detention processing; evidence seizure; efforts to prevent documentation from reaching public or legal channels

PART V: BEST PRACTICES

5.1 Legal and Ethical Discipline

| **RULE 1** | *Never obstruct, interfere with, or impede law enforcement operations, even operations you believe are unlawful. Your role is to document, not to intervene. Intervention creates legal exposure and compromises your documentation.* |

| **RULE 2** | *Stay on public property or obtain explicit permission for any private property observation post. Know the exact legal boundaries of your theater — federal building 'security perimeters' are not always lawfully established.* |

| **RULE 3** | *Your documentation is most valuable when it is indisputably lawful. Any conduct by your observers that could be characterized as threatening, obstructive, or unlawful will be used to discredit your entire body of evidence.* |

5.2 Documentation Quality Standards

- Contemporaneous over reconstructed: write log entries in the moment, not from memory afterward. Courts treat contemporaneous records differently.
- Factual over interpretive: logs should record what was observed ("Agent in green tactical vest pointed weapon at individual"), not conclusions ("Agent used excessive force"). Leave conclusions for analysis products.
- Completeness: a record with the full context — including facts that don't support your narrative — is more credible and more legally useful than a selective record.
- Chain of custody: every piece of video, photo, or physical documentation must have an unbroken chain of custody from collection to storage. Document who captured it, when, where, and every hand it passed through.
- Redundancy: critical documentation should exist in at least three independent copies in separate physical or encrypted locations.

5.3 Operational Security (OPSEC) for Lawful Organizations

OPSEC is not about hiding unlawful activity — it is about protecting your observers' safety, your sources' safety, and the integrity of your documentation from interference.

- Use encrypted communications (Signal, encrypted email) for all operational coordination
- Limit knowledge of specific observer assignments to those who need to know
- Assume your communications may be monitored: never discuss anything you would not want to explain in court
- Social media discipline: observers should not post real-time location information during operations; post-operation, be thoughtful about what is shared and when
- Device security: observers should know how to quickly secure their devices if detained; use strong encryption; enable remote wipe

5.4 Observer Safety and Wellbeing

- Never deploy alone: two-person minimum for field positions whenever possible – preference should be for four person teams
- All observers carry the name and direct phone number of a civil rights attorney on their person
- Observers know their rights: commit the basics to memory — right to record, right to refuse consent, right to identify the charge upon arrest
- Establish a buddy check-in protocol: if an observer misses a check-in, the coordinator initiates a welfare check
- Psychological safety: monitoring law enforcement abuse over extended periods can be traumatic. Build in debrief protocols that attend to observer wellbeing, not just information collection.

5.5 Organizational Integrity

- Establish clear leadership and decision-making authority before operations begin. Ambiguous authority in the field creates dangerous confusion.
- Conduct regular full-group debriefs: combine operational review (what did we collect?) with process review (how can we do this better?) and wellbeing check-ins
- Rotate roles to prevent burnout and build organizational depth. Don't let critical knowledge concentrate in one person.
- Maintain written records of organizational decisions, policies, and protocols. These protect the organization and demonstrate professionalism.
- Conduct periodic legal review: as your operation evolves, have legal counsel review your protocols to ensure continued compliance

5.6 Analytical Discipline

- Distinguish observation from inference: clearly mark which statements in your records are direct observations versus analytical conclusions

- Acknowledge gaps: a rigorous analysis explicitly identifies what you do NOT know as well as what you do. Unknown-unknowns are where analytical errors hide.
- Avoid confirmation bias: actively look for evidence that challenges your existing assessments. If your analysis never surprises you, you are probably not analyzing rigorously.
- Version control your analysis: document how your assessments have evolved over time and why. This creates an intellectual audit trail that strengthens your credibility.

5.7 Working with Legal and Advocacy Partners

- Establish relationships with civil rights attorneys, legal observer networks, and journalists before you need them urgently
- Understand what documentation format is most useful for legal proceedings and format your products accordingly — consult with attorneys about evidentiary standards
- Protect journalist sources and methods: information shared with journalists may flow differently than information shared with legal counsel (privilege considerations)
- Coordination with advocacy organizations: share products, not raw source information, with organizations outside your group

PART VI: QUICK REFERENCE — FIELD OBSERVER CHECKLIST

☐	**BEFORE DEPLOYMENT: Know your assigned sector, collection requirements, and legal contacts**
☐	Carry legal observer card with attorney contact info on your person
☐	Device is charged, encrypted, timestamping enabled, GPS metadata enabled
☐	Encrypted communications app open and coordinator contact confirmed
☐	Written log materials ready (physical backup recommended)
☐	Know your withdrawal signal and rally point
☐	Review applicable state recording laws for this theater
☐	Confirm your buddy/partner and establish check-in interval
☐	WHILE DEPLOYED: Log entries every 15 min minimum; event-driven entries for all observed activity
☐	For every federal vehicle: plate number, agency markings, color/type, location, time
☐	For every uniformed agent: agency patch, badge/ID number if visible, physical description, actions

☐	For every enforcement action: timestamp, location, involved agents, individuals affected, actions in sequence, duration
☐	For observer-agent contact: immediately document everything said and done; notify coordinator
☐	AFTER OPERATION: Complete written log; transfer all media with chain of custody documentation
☐	Debrief with coordinator: what was collected, gaps in coverage, any safety issues
☐	Participate in wellbeing check-in