# BDG Investigator's Bulletin

EDITION 4 · JULY 2026

Intelligence • Surveillance • Evidence • Professional Practice

Welcome to the July 2026 edition of the BDG Investigator's Bulletin. In this edition we explore three core themes from our training programmes. We begin with OSINT in Investigations — examining where RIPA engages, the three tiers of internet investigation activity, and the critical CHIS trap. We then hear from former CPS Senior Manager and Higher Court Advocate Mark Paul, who shares his essential tips for investigators giving evidence as professional witnesses — covering preparation, delivery, cross-examination, and handling errors. Finally, we turn to Managing and Grading Intelligence, covering the NIM 5x5x5 system and its application across local authority and multi-agency enforcement. As always, we hope this edition supports your CPD and your day-to-day practice.

# OSINT & Internet Intelligence Investigations (3III)

OPEN SOURCE INTELLIGENCE | RIPA

**3III is defined as:** the use of internet resources to gather information, intelligence and evidence — including overt and covert tactics to access closed areas, gather metadata on individuals, and monitor social media or online activity of a group, individual, or geographical area.

## The Web — the Iceberg Model

Only 4% of the internet is visible. Investigators must understand what lies beneath.


### Surface Web (~4%)

Indexed by search engines. Publicly accessible. Google, YouTube, Companies House, BBC. This is where Tier 1 activity takes place.

### Deep Web (~90%)

Not indexed. Requires direct URL or authentication. Academic databases, medical records, financial records, subscription content, government repositories.

### Dark Web (~6%)

Invisible to standard search engines. Requires Tor or specialist network protocols. Associated with illegal marketplaces, cybercrime services, and anonymised activity. Not everything hidden is illegal — but everything illegal is hidden.

## The Capability Delivery Model

All staff are expected to operate at Tier 1. Higher tiers require training, authorisation, and oversight.

### Tier 1: Core Internet Use

All staff. Public sources, no login required.

### Tier 2: Overt Internet Intelligence & Investigations

Trained investigators. Overt profiles, platform access, advanced search. DSA may be required.

### Tier 3: Covert Internet Intelligence & Investigations

Authorised trained staff only. Covert accounts, closed group access, subject surveillance. DSA required.

### Authorised CHIS/UC Activity

Specialist authorised activity only. Formal CHIS/UC authorisation required.

# When Does RIPA Engage? Key Considerations & Authorisation

OPEN SOURCE INTELLIGENCE | RIPA

Before starting any internet investigation, apply necessity, proportionality, and legality — and ask yourself these questions.

## 9 Key Considerations for Online Activity

### Purpose & scope
What is the intended purpose and scope?

### Target
Is it directed at an individual or organisation?

### Private info
Will it obtain private information?

### Listing sites
Will internet sites be listed to build an intelligence picture?

### Record & retain
Will information be recorded and retained?

### Lifestyle profile
Will it provide a “lifestyle” profile of the subject?

### Combined sources
Will it be combined with other sources to build a picture of private life?

### Repeated viewing
Is it ongoing or repeated viewing?

### Collateral intrusion
Is it likely to include collateral intrusion?

## Privacy Settings

### Reduced Privacy Expectation
Public information on platforms may carry a lower privacy expectation — but privacy concerns can still apply.

### Original Purpose Matters
The person did not share information for covert investigation use. Public access does not always mean lawful use.

⚠ Always check the original reason the person shared the data before using it for covert intelligence work.

## The DSA Authorisation Process

01

### Applicant
Submits the application with full justification for the surveillance activity.

02

### Authorising Officer / JP
Reviews and approves based on Necessity, Proportionality, and Collateral Intrusion.

03

### Legal Compliance
The right authorising role ensures the process remains legally compliant.

⚠ ⚠ **The CHIS Trap**

If you direct a member of the public to gather specific information on your behalf, they may meet the definition of a CHIS under s.26(8) RIPA — triggering formal authorisation and duty of care obligations. Never instruct a third party to conduct covert activity without proper advice as a source can now potentially be engaged in the conduct of a CHIS without direct tasking (e.g self tasking).

# IPCO Annual Report 2024 — What It Means for Investigators

RIPA COMPLIANCE

The Investigatory Powers Commissioner's Office (IPCO) Annual Report 2024 highlights key compliance failures and emerging trends that directly affect investigators using RIPA powers.

### Para 4.74: Joint Inspections with ICO

- Lack of data protection safeguards for covert material
- Deficiencies in policy and procedure
- Lack of training and awareness

### Para 5.19: Common Errors (mainly DSA)

- Activity started before authority was granted
- Activity continued after cancellation
- Activity conducted outside the scope of authorisation

### Para 8.2: AI in Scope of Inspections

- AI tools used to support applications, analyse data, and support retention are now within inspection scope
- Includes off-the-shelf products and AI features embedded in commonly used software
- Not limited to bespoke AI tools

⚠ These findings are a direct reminder: get the authority before you start, stay within scope, and ensure your team is trained. IPCO inspections are active — and errors have consequences.

## Social Media Risks

### Privacy Expectations

Users retain reasonable privacy expectations regardless of platform settings.

### Systematic Monitoring

Regular observation of social media constitutes directed surveillance — RIPA authorisation required.

### Evidence Integrity

Proper preservation and authentication of social media evidence is essential for legal proceedings.

### Collateral Intrusion

Minimise impact on non-target individuals appearing in social media content.

# Giving Evidence — Mark Paul's Top Tips

PROFESSIONAL WITNESS | COURT SKILLS

Mark Paul is a retired solicitor, former CPS Senior Manager, and Higher Court Advocate. Here are his essential tips for investigators giving evidence as professional witnesses.

### Mark's Golden Rule

Listen to the question. Pause to think. Answer clearly and at a slow pace. Direct your answers to the judge or magistrates — not to the advocate.

## Before You Enter the Witness Box

### Read your statement

Multiple times. It forms the basis of every question you'll face.

### Request sight in advance

Courts have approved this.

### Read all exhibited documents

Know your case materials inside out.

### Pre-empt challenges

Be ready on continuity, exhibit integrity, and disclosure.

## In the Witness Box

### Avoid jargon

Explain any technical terms you must use.

### If you don't know, say so

Honesty is your strongest answer.

### Never guess or bluff

Stay within your expertise.

### Stay calm

Cross-examination is not personal.

# Cross-Examination, Memory & Inadmissible Evidence

PROFESSIONAL WITNESS | COURT SKILLS

Cross-examination is a structured attempt to undermine your evidence — know what to expect and how to respond.

## Cross-Examination Tactics to Watch For

### Inconsistency or falsehood

They may suggest you are mistaken — or dishonest.

### Process attacks

Expect challenges to disclosure, continuity, and exhibit integrity.

### Minor discrepancies

Small gaps can be used to erode reliability.

### Respectful tone

A courteous advocate may still be trying to discredit you.

## Memory Refreshing

Giving evidence is not a memory test. Under s.139 Criminal Justice Act 2003, you may refresh your memory from your statement if your recollection at the time of writing was significantly better than it is now.

## Know What NOT to Say

### Bad character evidence

Not already admitted.

### Hearsay

Not already admitted.

### Unfairly obtained evidence

For example, coercion or entrapment.

### Irrelevant material

Keep to what matters.

### Protected personal data

Addresses and similar data under DPA/GDPR.

⚠ If in doubt — ask your legal team before you enter the witness box.

## If Your Team Has Made an Error

- Be candid and honest — do not deflect blame.
- Demonstrate you understand what went wrong and why.
- Explain what steps have been taken to minimise the impact.

# Managing & Grading Intelligence — The NIM 5x5x5

INTELLIGENCE MANAGEMENT | NIM

The National Intelligence Model (NIM) was developed by the College of Policing but is widely used by local authorities — including trading standards, environmental health, and licensing teams. Through Community Safety Partnerships, GAIN networks, and multi-agency tasking groups, councils apply NIM principles to manage risk, prioritise resources, and share intelligence with police and national agencies.

## Why NIM Matters for Local Authorities

### Multi-Agency Tasking

Local authorities participate in CSPs and tasking groups, sharing intelligence on crime, ASB, and local threats using NIM's structured process.

### Intelligence Management

The 5x5x5 grading system provides an objective, standardised way to evaluate, store, and act on intelligence — regardless of source.

### Targeted Interventions

NIM helps prioritise limited council resources on the highest areas of risk — rogue trading, illegal gambling, money laundering in licensed premises.

### Problem-Solving Approach

Rather than reacting to issues, NIM enables proactive control strategies that address persistent local problems at source.

Every piece of intelligence must be evaluated before it is acted upon. The 5x5x5 system has three components: Source Reliability, Information Assessment, and Handling Code.

## Component 1: Source Reliability

### 1 – Reliable

Competence and veracity both confirmed. Can be relied upon — subject to corroboration.

### 2 – Untested

No prior track record or unsubstantiated information. Treat with caution. Seek corroboration.

### 3 – Not Reliable

Grounds exist to doubt authenticity, motive, or competence. Do not act in isolation.

## Component 2: Information Assessment

### A – Known Directly

First-hand witness. Strongest grading.

### B – Known Indirectly but Corroborated

Not witnessed personally but verified by other sources.

### C – Known Indirectly

Told by someone else. No first-hand knowledge.

### D – Not Known

No means of assessment. Anonymous or Crimestoppers-type sources.

### E – Suspected to be False

Reason to believe information is false. Document rationale.

# Handling Codes & Intelligence Report Standards

INTELLIGENCE MANAGEMENT | NIM

| Acquisition | Exploitation | | | | |
|---|---|---|---|---|---|
| **Source** | **Intelligence** | **Handling** | **Intel unit only** | **Action** | **Sanitisation** |
| **1** – Reliable<br>**2** – Untested<br>**3** – Not reliable | **A** – Known directly<br>**B** – Known indirectly but corroborated<br>**C** – Known indirectly<br>**D** – Not known<br>**E** – Suspected to be false | **P** – Lawful sharing permitted<br>**C** – Lawful sharing permitted with conditions<br>A1 – Covert development<br>A2 – Covert use<br>A3 – Overt use | Action | — | **S1** – Delegated authority<br>**S2** – Consult originator |

# Intelligence Report Quality Standards — The 5WH Principles

All intelligence reports must be written to a consistent standard. Apply the 5WH framework:

### The 5WH Framework

- What occurred
- When it happened
- Where it took place
- Why it matters (legal purpose)
- Who was involved
- How it happened

Reports must be concise, avoid abbreviations, be self-contained, and not indicate the nature of the source. Corroborate where possible and document any research undertaken.

# Investigation Essentials Training

BDG TRAINING CONSULTANCY

These topics and much more are covered in BDG's specialist training programmes, designed for local, public and private investigators, enforcement officers and compliance teams.

## RIPA Awareness

Understand when RIPA applies to your investigations. Covers directed surveillance, CHIS, online research thresholds, authorisation requirements, and the Codes of Practice — with scenario-based exercises drawn from real enforcement situations.

**Who is this for?** Investigators, Authorising Officers, RIPA Co-ordinators, Managers.

## OSINT for Investigators

From surface web to dark web — know how to conduct lawful online research, manage the tipping point into directed surveillance, avoid CHIS creation errors, and capture intelligence that will stand up to scrutiny.

**Who is this for?** Investigators, Intelligence Officers, Compliance Teams.

## Court Skills for Professional Witnesses

Covers preparation, delivery, memory refreshing, handling cross-examination, and responding to errors — everything your investigators need before they enter the witness box in mock court scnearios

**Who is this for?** Investigators, Enforcement Officers, Technical Experts giving evidence.

Ready to book or want to know more? All courses are available as in-house, group, or open programme delivery.
Contact: bdgtrainingconsultancy@gmail.com

# BDG Training Consultancy Limited

Overt & Covert Investigation | Training & Development

---

Email: **info@bdgtrainingconsultancy.co.uk**

Website: **www.bdgtrainingconsultancy.co.uk**

Registered in England and Wales

Company Number: 10475761

VAT Registration: GB 430302261