

I LOVE THE CIA

Citizen's OSINT Reference Manual



by Marie-Soleil Seshat Landry (Marie Landry Spy Shop)

GUMROAD
EXCLUSIVE

I LOVE THE CIA

THE CITIZEN'S GUIDE TO RESPONSIBLE OSINT REPORTING

*A Professional Reference Manual for Ethical Intelligence
Contribution*

MARIE-SOLEIL SESHAT LANDRY

Landry Industries Inc.

ORCID: 0009-0008-5027-3337

marielandryspyshop.com

OSINT

HUMINT

GEOINT

SIGINT

FININT

IMINT

MASINT

OPSEC

FC/NV

IC

SIFT

LEGAL NOTICE & DISCLAIMER

This publication — *I Love The CIA: The Citizen's Guide to Responsible OSINT Reporting* — is an independent, professional reference work. It is not affiliated with, endorsed by, sponsored by, or produced by the Central Intelligence Agency, the United States Government, or any intelligence community entity. All contact methods, channel descriptions, and procedural guidance described herein are derived exclusively from publicly available, unclassified open sources including cia.gov, official congressional testimony, and unclassified academic publications.

Nothing in this manual constitutes legal advice. Consult a licensed attorney before taking any action based on the guidance herein. The author and publisher accept no liability for actions taken by readers in reliance on this material.

This work is published under independent authorship. All rights reserved. Marie-Soleil Seshat Landry / Landry Industries Inc. / ORCID 0009-0008-5027-3337.

First Edition • 2026 • Landry Industries Inc., Moncton NB Canada • marielandryspyshop.com

TABLE OF CONTENTS

PREFACE

PART I — FOUNDATIONS & CONTEXT

- 01 What Is This Book?
- 02 The CIA at a Glance
- 03 The Intelligence Cycle for Citizens

PART II — THE SUBMISSION ARCHITECTURE

- 04 Official Channels
- 05 The CRAFT Report Method
- 06 Digital Hygiene for Submitters

PART III — WHAT TO REPORT

- 07 High-Priority Categories
- 08 The OSINT Sweet Spots
- 09 What NOT to Send

PART IV — ADVANCED TECHNIQUES

- 10 Verification Frameworks
- 11 Specialised Collection Disciplines
- 12 The Analyst Mindset

PART V — ETHICS, LEGALITIES & CULTURE

- 13 The Legal Landscape
- 14 Disinformation & Counter-Intelligence Awareness
- 15 The Culture of Intelligence

PART VI — REFERENCE APPENDICES

- A Submission Template & Checklist
- B OSINT Tool Kit
- C Reading List
- D Glossary
- E The Citizen Intelligence Pledge

CONCLUSION

ABOUT THE AUTHOR

Preface

On the dissolution of walls between professional intelligence and the informed citizen.

In an age when a researcher working from a kitchen table can geolocate a military vehicle from a blurry social media post, and when open-source analysts have beaten governments to major intelligence conclusions, the boundary between professional collection and civilian observation has permanently shifted. The question is no longer whether civilians can contribute to national intelligence — they demonstrably do. The question is how to do it responsibly.

The Central Intelligence Agency maintains a publicly accessible tip submission channel. What is surprisingly opaque — given its public availability — is the practical guidance around using it well: what information is actionable, how to document findings professionally, what legal boundaries apply, and when the CIA is the right destination versus the FBI, a journalist, or a civilian OSINT organisation.

"This manual draws entirely on open-source materials. Nothing here is classified. Everything here is, in the truest sense, open-source intelligence about open-source intelligence."

This manual fills that gap. It is written for the serious OSINT practitioner who has found something that felt nationally significant and wants to handle it with the professionalism the subject demands.

The title is deliberate. Civic engagement with national intelligence — conducted legally, ethically, and carefully — is not a character flaw. It is a form of democratic participation.

PART I

FOUNDATIONS & CONTEXT

Understanding the landscape before you transmit

What Is This Book?

Scope, limitations, and the vocabulary you need before you begin.

SCOPE & LIMITATIONS

This manual covers exclusively public-channel submission. It does not describe, speculate about, or encourage clandestine cooperation, covert recruitment, or unofficial contact with intelligence officers. Everything described is equivalent to submitting through a publicly advertised website form — because that is precisely what it is.

- All contact methods described are listed on cia.gov or equivalent official open sources.
- No classified submission protocols are described or implied.
- This guide applies to foreign intelligence reporting only — domestic activity routes to the FBI.
- Jurisdictional notes (Canadian, Five Eyes) are flagged throughout.
- The guide is descriptive and educational — not operational.

INTELLIGENCE VOCABULARY

Before engaging with intelligence processes, precision of language is essential.

TERM	FULL NAME	DEFINITION
OSINT	Open Source Intelligence	Intelligence from publicly available sources
HUMINT	Human Intelligence	Intelligence from human sources / informants
SIGINT	Signals Intelligence	Intelligence from intercepted communications
GEOINT	Geospatial Intelligence	Intelligence from satellite and aerial imagery
FININT	Financial Intelligence	Intelligence from financial records and structures
MASINT	Measurement & Signature Intel	Technical intelligence from physical sensors

TERM	FULL NAME	DEFINITION
IMINT	Imagery Intelligence	Intelligence derived from photographic media
IC	Intelligence Community	The 18 US agencies forming the national intel structure
FC/NV	Fact-Constant / Narrative-Variable	Framework separating facts from interpretation

■ **LEGAL /
OPERATIONAL
NOTE**

This manual concerns OSINT exclusively. If you hold HUMINT (a human source), SIGINT (intercepted communications), or classified materials, consult a lawyer before taking any action.

The CIA at a Glance

A factual, unclassified orientation to the agency you are considering contacting.

MISSION & JURISDICTION

The CIA's statutory mission — defined by the National Security Act of 1947 — is to collect, analyse, and disseminate **foreign intelligence** to the President and senior policymakers. This distinction is critical: the CIA is legally prohibited from collecting intelligence on US persons inside the United States. That is the FBI's jurisdiction.

JURISDICTION

Domestic US criminal activity → FBI (tips.fbi.gov). Foreign nationals, foreign governments, or activities with a clear foreign nexus → CIA. If uncertain, consider filing with both agencies.

PUBLICLY KNOWN ORGANISATIONAL STRUCTURE

DIRECTORATE	FUNCTION
Directorate of Analysis (DA)	Produces all-source intelligence analysis for policymakers — primary consumer of your OSINT tip
Directorate of Operations (DO)	Manages HUMINT and clandestine activities — not the destination for public submissions
Directorate of Digital Innovation (DDI)	Cyber, data analytics, open-source exploitation — most directly relevant to OSINT
Open Source Enterprise (OSE)	Dedicated OSINT collection unit; institutionalisation of open-source intelligence within the IC
Directorate of Science & Technology	Technical collection capabilities; relevant for assessing MASINT and technical OSINT

HISTORICAL CONTEXT

The CIA's predecessor, the Office of Strategic Services (OSS, 1942–1945), already recognised the value of open-source collection. Its Research and Analysis Branch — staffed largely by academics — produced products from newspapers, academic publications, and intercepted public broadcasts. The 9/11 Commission's finding that much relevant pre-attack information existed in open sources triggered a formal renaissance, culminating in the 2006 establishment of the Open Source Center (now OSE).

"The intelligence community should exploit open source information more effectively. — 9/11 Commission Report, 2004"

The Intelligence Cycle for Citizens

How professional intelligence is produced — and exactly where your contribution fits.

THE FIVE-STAGE CYCLE

- 1 Planning & Direction**
Decision-makers identify intelligence requirements — the questions they need answered. Your tip is most valuable when it addresses an existing priority.
- 2 Collection**
Information is gathered from all sources: HUMINT, SIGINT, GEOINT, OSINT. Your public submission enters the process here.
- 3 Processing**
Raw collected information is converted into usable form: translated, decoded, geo-referenced, formatted.
- 4 Analysis & Production**
Analysts evaluate and integrate processed information to produce finished intelligence assessments.
- 5 Dissemination**
Finished intelligence is delivered to the consumers who requested it. A valuable tip may ultimately influence a Presidential Daily Brief.

THE VALUE FUNNEL

Most tips are screened out. The factors determining whether a tip advances:

- **Specificity** — vague tips are discarded immediately.
- **Verifiability** — documented sources with clear provenance are processed faster.
- **Foreign nexus** — tips with a clear foreign intelligence angle route correctly.

- **Timeliness** — time-sensitive information about imminent activities is prioritised.
- **Originality** — information that adds to, rather than duplicates, existing holdings.
- **Corroboration** — tips that confirm or contradict existing assessments are noted.

PART II

THE SUBMISSION ARCHITECTURE

Channels, report structure, and digital hygiene

Official Channels

Verified public submission mechanisms — and how to use each correctly.

THE CIA.GOV CONTACT FORM

The primary public submission channel is the CIA's official contact page at cia.gov. Before using any submission portal, verify you are on the genuine domain.

LEGAL / OPERATIONAL NOTE

ANTI-PHISHING: The legitimate portal is at cia.gov. Verify the SSL certificate and full domain. Never submit through a link provided by email, social media, or third parties. Phishing sites impersonating intelligence agency tip pages are known to exist.

- Select the subject category that most closely matches your information type.
- Draft your full submission as a separate document first — paste into the form field.
- If operational security is a concern, consider the Tor Browser option below.
- Attach supporting documentation where the form permits.

TOR BROWSER & THE .ONION ADDRESS

The CIA maintains a .onion address accessible via the Tor Browser for submitters who wish to protect identity and location metadata. The CIA announced its dark web presence in 2019 specifically to enable anonymous submissions from individuals in restrictive environments.

CANADIAN CONTEXT

For non-US submitters: using Tor for anonymous tip submission to a foreign intelligence service occupies a legal gray area in some jurisdictions. CSE and CSIS maintain their own tip mechanisms for domestically-relevant intelligence. Consult applicable national law.

POSTAL MAIL

Physical mail remains viable for submitters with physical evidence or documents. The public mailing address is available at cia.gov.

- Photograph all physical evidence before mailing — you will not receive it back.
- Document chain of custody: record when and how you obtained the item.
- Use a return address only if acknowledgment is acceptable for your threat model.
- International mail (from Canada) passes through customs — factor into OPSEC planning.

EMBASSY CHANNELS

For tips of exceptional urgency, US embassies maintain public contact mechanisms. Standard embassy contact forms are the correct channel for non-urgent tips from overseas submitters. Do not approach embassy personnel in an unplanned, unsolicited manner regarding intelligence matters.

The CRAFT Report Method

How to structure your submission so an analyst can assess its value in under two minutes.

The CRAFT Method adapts professional intelligence report writing conventions to the civilian submission context. A submission built on this framework signals analytical competence and dramatically increases the probability of productive processing.

- C Context**
Establish provenance: what platform, account, date, and time? Is this a primary source (direct observation) or secondary (reported)? Context allows an analyst to assess source reliability without further investigation.
- R Relevance**
Explain, concisely, why this information may bear on US national security interests. A one-sentence hypothesis saves analyst time. Be explicit about uncertainty.
- A Authenticity**
Describe your verification steps. Reverse image search? Cross-reference? Metadata check? An unverified tip with documented verification attempts is far more valuable than one with no provenance trail.
- F Facts Only**
Separate observed facts from analytical inferences in clearly labelled sections. 'The account posted a video showing [item]' is a fact. 'This proves [actor] is planning [action]' is an inference. Both may be useful — but must be labelled.
- T Timeliness**
Date and sequence all information. Intelligence loses value rapidly. Provide UTC timestamps. If reporting an evolving situation, provide a chronological timeline.

SUBMISSION TEMPLATE

FIELD	CONTENT / INSTRUCTIONS
Subject	One-line description (e.g., 'Suspected sanctions evasion — maritime')
Date of Information	UTC date/time of observation
Source	Platform, URL, account name, or 'direct observation'
Context	How found; nature of source; reliability assessment
Observed Facts	Factual description only — what you literally saw/read/heard
Preliminary Analysis	Your hypothesis — clearly labelled as inference
Verification Steps	What you checked and what each check produced
Supporting Materials	Screenshots, archived URLs, coordinates, file hashes
Confidence Level	High / Medium / Low — with brief justification

Digital Hygiene for Submitters

Protecting yourself, protecting sources, and ensuring your submission causes no inadvertent harm.

THREAT-MODELLED OPSEC

Appropriate operational security depends entirely on your threat model. For most practitioners submitting tips about publicly observable foreign activity, basic hygiene suffices. For those in higher-risk categories — journalists, researchers near hostile state actors — stronger measures are warranted.

RISK LEVEL	RECOMMENDED POSTURE
Low	Standard browser, home device. Verify HTTPS and domain. Standard VPN optional.
Medium	No-log commercial VPN. Avoid corporate networks. Dedicated browser profile.
High	Tor Browser to CIA .onion address. Dedicated device not linked to normal identity. Public WiFi.

METADATA SCRUBBING

- **EXIF data** in photographs often contains GPS coordinates, device model, and precise timestamp.
- **Office/PDF documents** may contain author name, organisation, revision history, and tracked changes.
- **Screenshots** are generally safer than original files but may carry OS-level metadata.
- **Tools:** ExifTool, MAT2, PDF metadata editors. Strip all metadata before attaching to submissions.

THE ONE-WAY PRINCIPLE

You will almost certainly never receive confirmation that your tip was received, assessed, or acted upon. This is deliberate: acknowledging a tip, or confirming receipt, could reveal collection priorities and methods. The absence of acknowledgment is not evidence of failure — submit, document what you submitted, and move on.

**SOURCE
PROTECTION**

A significant underappreciated risk: your analysis may inadvertently identify an individual who is already a protected asset or cooperating witness. Report what you observed — activities, indicators, anomalies. Let the IC make personnel determinations with their full operational picture.

PART III

WHAT TO REPORT

The valued intelligence spectrum — and the exclusion list

High-Priority Categories

Based on publicly stated CIA mission priorities, congressional testimony, and unclassified collection requirements.

TERRORISM PLANNING & FACILITATION

- Online recruitment by foreign designated terrorist organisations.
- Logistics and financing networks with a clear overseas node.
- Physical location indicators: training camps, supply routes, staging areas verifiable via imagery.
- Propaganda infrastructure on foreign platforms.

WEAPONS PROLIFERATION

- Commercial satellite imagery showing construction consistent with WMD-related facilities.
- Shipping manifests and AIS data showing anomalous cargo movements to sanctioned entities.
- Open-source procurement documentation suggesting dual-use technology transfer.
- Public statements by state or non-state actors indicating weapons programs.

FOREIGN INTELLIGENCE SERVICE ACTIVITIES

- Transnational repression activities targeting diaspora communities.
- Influence operations using sockpuppet networks traceable to foreign state infrastructure.
- Front organisations with documented undisclosed foreign state funding.
- Recruitment approaches to individuals with US government or defence contractor affiliations.

ADVERSARIAL CYBER INFRASTRUCTURE

- Command-and-control servers, phishing domains, botnet nodes attributable to nation-states.
- Technical attribution of malware or intrusion campaigns to state actors.

— Infrastructure reuse patterns linking separate attack clusters.

■ **LEGAL /
OPERATIONAL
NOTE**

The foreign nexus requirement is non-negotiable. Domestic terrorism concerns belong to the FBI. If the character of an activity is genuinely uncertain, file with both agencies through their respective public channels.

The OSINT Sweet Spots

Areas where civilian open-source analysis has a proven track record of intelligence-grade output.

GEOLOCATION

Geolocation — determining the precise geographic coordinates of an event from visual or signals evidence — is one of the civilian OSINT community's most consistently impressive capabilities. For a geolocation tip to be actionable:

- Include the original source material with archive URL.
- State the specific geographic claim with decimal-degree coordinates.
- Describe the methodology: landmarks, shadow analysis, satellite comparison.
- Assign a confidence level with radius of uncertainty where applicable.

MARITIME & AVIATION ANOMALIES

AIS data is publicly available via MarineTraffic and VesselFinder. GPS spoofing, AIS signal gaps, and anomalous port calls by sanctioned vessels are active OSINT collection areas with direct policy relevance. ADSB Exchange and FlightAware provide aviation tracking data useful for monitoring government aircraft and logistics movements.

FINANCIAL & CORPORATE OSINT

Commercial satellite imagery combined with shipping data, corporate registrations, and trade documentation has been used effectively by organisations including C4ADS and OCCRP to trace sanctions evasion, illicit arms transfer, and the financial architecture of adversarial state enterprises.

SOCIAL NETWORK ANALYSIS

Structured social media analysis — mapping account relationships, identifying coordinated inauthentic behaviour, tracing information cascades — produces network intelligence that complements classified collection. Document methodology rigorously: an undocumented analysis is analytically worthless.

What NOT to Send

The exclusion list — and why each category must be routed elsewhere.

DOMESTIC US CRIMINAL ACTIVITY

The CIA has no law enforcement mandate inside the United States. Domestic criminal activity — including domestic terrorism, narcotics, financial crime without a clear foreign principal — routes to the FBI (tips.fbi.gov), DEA, or relevant local authority. Routing domestic tips to the CIA delays rather than accelerates action.

PERSONAL GRIEVANCES & BUSINESS DISPUTES

A significant proportion of public tips are vehicles for personal grievances dressed in national security language. Agencies actively filter for this pattern. Submitting a personal grievance as a national security tip wastes analyst capacity and flags the submitter as unreliable for future legitimate submissions.

CLASSIFIED MATERIALS

If you have come into possession of classified government materials through any means other than authorised official access, do not submit them without first consulting an attorney. Legal exposure is significant and varies by jurisdiction.

RAW UNVERIFIED DATA WITHOUT CONTEXT

A screenshot with no translation, no source context, and no stated relevance is noise, not intelligence. Apply the CRAFT method before submitting — your tip should add analytical value, not add to the raw data volume the IC already possesses.

INFORMATION ABOUT US PERSONS

Executive Order 12333 imposes significant restrictions on CIA collection, retention, and processing of US person information. Tips focused primarily on US citizens or permanent residents — even with foreign connections — should route to the FBI.

PART IV

ADVANCED TECHNIQUES

Verification, specialised disciplines, and the analyst mindset

Verification Frameworks

OSINT without verification is rumour. These frameworks are the professional standard.

THE SIFT METHOD

STOP: Before sharing or acting on information, pause. The first impulse on encountering striking information is often the most dangerous one.

INVESTIGATE THE SOURCE: Determine who produced the information, their track record, funding, and agenda. State media requires different handling than independent investigative journalism.

FIND BETTER COVERAGE: Search for corroborating or contradicting reporting. Significant accurate claims should appear across multiple independent sources.

TRACE CLAIMS: Find the original source — the primary document, the original video, the first report — and assess it directly rather than through intermediaries.

REVERSE IMAGE SEARCHING

- Run through Google Images, Yandex Reverse Image Search, and TinEye as a minimum.
- Check whether the image appears earlier, in a different context, or labelled differently.
- Use FotoForensics or similar tools to check for editing artifacts.
- For videos: extract representative frames and reverse-search each.

THE TWO-SOURCE RULE

A factual claim should be independently confirmed by at least two sources before being stated as established. Sources must be: independent of each other (not citing each other), primary where possible, and drawn from different platforms or media types.

CONFIDENCE LANGUAGE

LEVEL	STANDARD IC PHRASING	OPERATIONAL MEANING
High	We assess with high confidence	Multiple independent reliable sources; minimal analytical doubt

LEVEL	STANDARD IC PHRASING	OPERATIONAL MEANING
Medium	We assess with moderate confidence	Credible sources with some gaps or inconsistencies
Low	We assess with low confidence	Limited, ambiguous, or potentially unreliable sources; significant uncertainty

Specialised Collection Disciplines

What is achievable in each intelligence discipline from open sources alone.

IMINT: READING SATELLITE IMAGERY

Commercial platforms including Google Earth Pro, Sentinel Hub, Planet Labs, and NASA Worldview provide imagery reaching sub-meter resolution. Key open-source IMINT skills:

- **Shadow analysis** — object height calculable from shadow length and sun angle (SunCalc.net).
- **Vehicle identification** — military vehicles, aircraft, containers identifiable by size and pattern.
- **Activity indicators** — disturbed earth, new construction, vehicle tracks, equipment staging.
- **Temporal comparison** — comparing imagery across time reveals buildup, construction progress, movement.
- **Scale reference** — road widths, vehicle sizes, known building footprints provide calibration.

MARITIME: AIS & DARK SHIPPING

TOOL	FUNCTION
MarineTraffic / VesselFinder	Real-time and historical AIS vessel tracking
Global Fishing Watch	Vessel tracking with anomaly detection algorithms
UN Comtrade	Shipping manifest data for trade flow analysis
OFAC Sanctions List	Vessel and entity identification against sanctioned parties

FINANCIAL OSINT (OSFININT)

Open-source financial intelligence uses corporate registrations, property records, court filings, trade data, and regulatory disclosures to map the financial architecture of entities of interest. Primary resources: OCCRP Aleph, OpenCorporates, FinCEN data, and SEC EDGAR.

LINGUISTIC ANALYSIS

- Machine translation (DeepL, Google Translate) is acceptable for initial screening, not final analysis.
- Dialect and register matter: formal state media Russian differs meaningfully from Telegram channel slang.
- Code words used by specific communities require community-specific expertise.
- Always note the language and dialect of source material in your submission.

The Analyst Mindset

Professional intelligence analysis techniques adapted for the civilian OSINT reporter.

WRITING FOR AN INTELLIGENCE AUDIENCE

- **Bottom-line-up-front (BLUF):** lead with your key finding, not your methodology.
- **Active voice, precise verbs:** 'the vessel departed' not 'departure was observed to have occurred.'
- **Specific attributions:** 'commercial satellite imagery dated [DATE]' not 'satellite photos.'
- **Separated fact and analysis:** use 'this suggests,' 'available evidence indicates.'

RED-TEAMING YOUR OWN FINDINGS

Before submitting, actively attempt to disprove your own conclusion:

- What alternative explanations exist for the activity observed?
- Could this be deliberate deception or planted information?
- Am I over-weighting this because it confirms a prior belief?
- What would I need to see to conclude the opposite?
- Is this already widely known and already in agency holdings?

THE "SO WHAT?" TEST

Every submission should survive the 'So What?' test: if this information is accurate, what policy decision, operational response, or analytical update might it inform? Articulating strategic or tactical relevance — even speculatively — substantially increases the probability of productive processing.

"The most important single thing is to be willing to be wrong. — Sherman Kent, father of intelligence

analysis"

PART V

ETHICS, LEGALITIES & CULTURE

The framework within which responsible contribution must operate

The Legal Landscape

A practitioner's orientation to the laws most relevant to civilian OSINT reporting.

**LEGAL /
OPERATIONAL
NOTE**

The following is educational background, not legal advice. Laws vary by jurisdiction and circumstance. Consult a licensed attorney for advice specific to your situation.

THE ESPIONAGE ACT (US)

The Espionage Act of 1917 (18 U.S.C. §§ 793–798) criminalises unauthorised disclosure of national defence information.

- The Act has been interpreted broadly — 'national defence information' extends beyond formally classified material.
- Transmitting information that 'the possessor has reason to believe could be used to injure the United States' may trigger liability.
- Legally obtained public information submitted through official channels presents a fundamentally different legal posture.
- Non-US citizens (including Canadians) can face Espionage Act charges for actions outside the US if related to US national defence.

ITAR / EAR: TECHNICAL DATA RESTRICTIONS

ITAR and EAR control the export of defence-related and dual-use technologies. If your OSINT involves technical details about weapons systems, propulsion, cryptographic systems, or other controlled technologies, specific restrictions may apply even to transmitting that information to a US government agency.

PRIVACY LAW (CANADIAN CONTEXT)

For Canadian-based researchers, PIPEDA and provincial privacy legislation govern collection, use, and disclosure of personal information. For researchers accessing EU-based data, GDPR restrictions on processing personal data of EU residents may apply regardless of the researcher's location.

WHISTLEBLOWER PROTECTIONS VS. UNAUTHORISED DISCLOSURE

Whistleblower protections — in the US and under Canada's Public Servants Disclosure Protection Act — apply to individuals reporting wrongdoing through designated official channels. They do not generally cover disclosure of classified information to foreign nationals, journalists, or the public.

Disinformation & Counter-Intelligence Awareness

The landscape contains adversaries who actively work to manipulate your output.

HOW FOREIGN SERVICES SEED FAKE TIPS

State-sponsored disinformation operations routinely target official tip channels with fabricated or distorted intelligence.

- Fabricated documents designed to appear leaked, containing false information.
- Genuine documents with altered key details — dates, names, figures.
- Authentic imagery from unrelated events presented as evidence of specific incidents.
- Coordinated multi-account 'evidence' designed to appear as independent corroboration.

THE DANGLE

Foreign intelligence services sometimes approach individuals who have publicly identified themselves as OSINT researchers or intelligence enthusiasts. A 'dangle' is an approach designed to assess recruitable status or willingness to serve as an unwitting conduit for false information.

FIELD NOTE

If you are approached by someone who is unusually interested in your OSINT activities, offers exclusive information, or asks detailed questions about your submission habits and channels — treat this as a potential intelligence service approach. Do not share submission history or methodologies.

COGNITIVE BIASES IN OSINT

BIAS	DESCRIPTION
Confirmation bias	Treating evidence confirming existing beliefs as more credible than contradicting evidence

BIAS	DESCRIPTION
Availability bias	Over-weighting recent or vivid information relative to statistically representative data
Nationalism bias	Treating one's own government or national media as inherently more reliable than foreign sources
Anchoring	Over-relying on the first piece of information encountered about a topic
Recency bias	Assuming current patterns will persist; under-weighting historical context

SYNTHETIC MEDIA DETECTION

- **Hive Moderation API** — currently among the highest-accuracy synthetic image detectors.
- **InVID / WeVerify** browser extension — video verification and keyframe extraction.
- **FotoForensics** — JPEG error level analysis for editing artifact detection.
- **Microsoft Video Authenticator** and equivalent enterprise-grade tools.

The Culture of Intelligence

Institutional and community context for the citizen OSINT contributor.

WHY THERE IS NO ACKNOWLEDGMENT

Confirming receipt of a specific tip would reveal that the agency considers the subject matter worth tracking. Patterns of confirmation and non-confirmation would, in aggregate, map collection priorities and gaps. The one-way submission model is a deliberate operational security posture, not negligence.

THE CIVILIAN OSINT ECOSYSTEM

Organisations including Bellingcat, the Centre for Information Resilience, ACLED, C4ADS, and dozens of academic research centres produce OSINT-derived intelligence that rivals official government outputs in their focus areas. These organisations represent a legitimate alternative to direct government submission for practitioners who prefer an intermediary channel.

CHANNEL SELECTION GUIDE

SITUATION	RECOMMENDED CHANNEL
Foreign military buildup / terrorist logistics	CIA or relevant IC agency
Government wrongdoing / abuse of power	Journalist with appropriate legal protections
Corporate/financial corruption — foreign nexus	OCCRP or equivalent + relevant agencies
Disinformation targeting your country	National cyber/media authority + journalist
Imminent threat to life	Law enforcement first, then IC agencies
Historical atrocity documentation	Academic/NGO channels + IC where appropriate
Uncertain domestic/foreign character	FBI and CIA — file with both

PART VI

REFERENCE APPENDICES

Templates, tools, reading lists, and glossary

CHAPTER A

Submission Template & Checklist

A reusable framework for any OSINT tip submission.

OSINT TIP SUBMISSION — TEMPLATE	
Date of Submission (UTC)	_____
Subject / Topic	_____
Source Type	☐ Social Media ☐ Satellite Imagery ☐ Document ☐ Other: _____
Source URL	_____
Observed Facts	(Describe only what you directly observed — no interpretation)
Preliminary Analysis	(Your hypothesis — clearly labelled as inference)
Confidence Level	☐ High ☐ Medium ☐ Low

PRE-SUBMISSION CHECKLIST

- ☐ All URLs archived (archive.today or Wayback Machine)
- ☐ EXIF / metadata stripped from all attached files
- ☐ Screenshots taken from a clean browser session
- ☐ Factual observations and analytical inferences clearly separated
- ☐ Source reliability assessed and documented
- ☐ Confidence level assigned and justified
- ☐ Legal review: is any material classified or restricted?

— ☐ Correct agency confirmed: CIA (foreign) / FBI (domestic) / both (uncertain)

CHAPTER B

OSINT Tool Kit

Verified open-source tools organised by collection discipline.

GEOLOCATION & IMAGERY

Google Earth Pro	Historical satellite imagery, elevation data, 3D terrain
Sentinel Hub	EU Copernicus satellite imagery — free tier available
SunCalc.net	Shadow length and sun angle calculator
Overpass Turbo	OpenStreetMap data extraction and spatial queries

VERIFICATION & MEDIA FORENSICS

InVID / WeVerify	Video verification browser extension
FotoForensics	JPEG error level analysis
TinEye	Reverse image search with historical tracking

MARITIME & AVIATION

MarineTraffic	Real-time AIS vessel tracking
ADSB Exchange	Unfiltered aviation tracking
Global Fishing Watch	Dark vessel detection

FINANCIAL & CORPORATE

OpenCorporates	Global company registry data
OCCRP Aleph	Investigative data platform
SEC EDGAR	US SEC filings

Reading List

Essential references for the professional OSINT practitioner.

OFFICIAL CIA PUBLICATIONS (UNCLASSIFIED)

- **Studies in Intelligence** — CIA's in-house academic journal; unclassified editions at cia.gov
- **CIA World Factbook** — annual country reference
- **Psychology of Intelligence Analysis** — Richards Heuer; canonical text on cognitive bias
- **Sherman Kent and the Profession of Intelligence** — foundational tradecraft text

OSINT METHODOLOGY

- **Open Source Intelligence Techniques** — Michael Bazzell; comprehensive guide
- **The OSINT Framework** — online resource at osintframework.com
- **Verification Handbook** — European Journalism Centre
- **Bellingcat Online Investigation Toolkit**

INTELLIGENCE COMMUNITY (ACADEMIC)

- **Intelligence: From Secrets to Policy** — Mark Lowenthal
- **The Art of Intelligence** — Henry Crumpton
- **Legacy of Ashes: The History of the CIA** — Tim Weiner

DISINFORMATION & INFORMATION WARFARE

- **Active Measures: The Secret History of Disinformation** — Thomas Rid
- **This Is Not Propaganda** — Peter Pomerantsev
- **Lie Machines** — Philip Howard

The Citizen Intelligence Pledge

An ethical charter for individuals who choose to engage in citizen OSINT reporting.

1

Truth First

I report only what I have genuinely observed and verified. I clearly distinguish facts from inferences. I do not submit information I believe to be false, misleading, or manufactured.

2

Do No Harm

I consider the potential consequences of my submission, including the possibility of endangering individuals. I do not submit information that primarily serves personal interests dressed as public ones.

3

Legal Compliance

I do not access, obtain, or transmit information through illegal means. I consult legal counsel when uncertain about the legal status of materials.

4

Source Protection

I take reasonable steps to protect the identity of any individuals whose safety could be compromised by my submission, including those identified through open sources.

5

Analytical Humility

I acknowledge the limits of my knowledge and capability. I use confidence language accurately. I do not overstate the significance or certainty of my findings.

6

Accountability

I maintain records of my submissions and the information on which they were based. I accept that I may be wrong and that my submissions will be assessed critically.

7

Democratic Values

I do not use the intelligence-reporting mechanism for political persecution, ethnic targeting, or suppression of legitimate dissent.

The Invisible Republic

A closing note on the nature and limits of civilian intelligence contribution.

The evidence that civilian OSINT can do remarkable things is by now overwhelming. Geolocation of war crimes from open-source footage. Maritime tracking of sanctions violators in real time. Student volunteers documenting atrocities from satellite imagery. Amateur analysts beating governments to major intelligence conclusions. The democratisation of collection capability is a permanent feature of the information environment.

What is equally true is that the intelligence enterprise is vast, technically sophisticated, and operated by professionals who have access to sources and methods that no open-source practitioner will match. The citizen OSINT reporter is not a replacement for that enterprise. They are, at best, a supplementary sensor.

"The invisible republic this manual gestures toward has no flag, no anthem, no membership card. It has only the commitment to getting it right."

The quality of the information environment — and of the decisions made from it — depends, in part, on how seriously each practitioner takes that commitment.

ABOUT THE AUTHOR

Marie-Soleil Seshat Landry is the CEO and Founder of Landry Industries Inc., based in Moncton, New Brunswick, Canada. She operates as an independent OSINT investigator, AI systems architect, materials science researcher, and policy document author.

Her published work spans intelligence methodology — including the WTF 8.0 Workflow for Truthfinding framework and the FC/NV / 1=1=1 hallucination-free AI governance architecture — materials science research under the Hempoxies platform, and policy frameworks including the Universal Declaration Against Clandestine Influence.

She publishes under ORCID 0009-0008-5027-3337 with over 135 records on Zenodo and operates the Landry Industries Spy Shop at marielandryspyshop.com.

I Love The CIA: The Citizen's Guide to Responsible OSINT Reporting
First Edition · 2026 · Landry Industries Inc., Moncton NB, Canada
ORCID: 0009-0008-5027-3337 · marielandryspyshop.com
All rights reserved.