NATURE CRIME ALLIANCE
people. planet. justice.

Guidelines | Enhancing information-sharing between civil society and law enforcement on environmental crime

NOVEMBER 2025

NATURE CRIME
ALLIANCE
people. planet. justice.

Guidelines | Enhancing information-sharing between civil society and law enforcement on environmental crime

CONTENTS

NOVEMBER 2025

PREFACE

The Nature Crime Alliance has developed these guidelines, with support from United for Wildlife, to improve the processes for civil society organisations (CSOs) and environmental non-governmental organisations (NGOs) to share information with law enforcement. The Nature Crime Alliance conducted interviews with subject matter experts, and disseminated surveys to civil society organisations and law enforcement to identify best practice to help improve the capability of CSOs to successfully support law enforcement investigations of environmental crime.

This document aims to address a critical challenge, namely ensuring that high-quality information collected by civil society organisations is effectively shared with the appropriate law enforcement authorities in a way that is useful for investigations and prosecutions.

It is important to acknowledge that collaboration with law enforcement represents just one tool available to civil society in addressing crime problems. Many CSOs pursue a wide range of strategies aimed at prevention, such as community engagement, advocacy, policy reform, and efforts to reduce consumer demand for illegally sourced products. These approaches remain vital to tackling the complex social, economic, and political drivers of environmental crime.

However, where the primary objective is the detection, arrest, and prosecution of offenders, and the prevention of further criminal activity, this falls squarely within the mandate of law enforcement. These guidelines are intended specifically for this situation, when civil society organisations wish to strengthen the ability of law enforcement agencies to detect and investigate environmental crimes.

These guidelines focus on the role of CSOs in the collection and sharing of information related to environmental crime. Civil society organisations encompass a broad spectrum of groups, including community-based organisations, labour unions, advocacy networks, and faith-based groups. However, in the context of environmental crime, the most relevant actors are typically non-governmental organisations dedicated to environmental protection.

While NGOs are often associated with international operations, for the purposes of this document, the term also includes domestic civil society groups engaged in environmental monitoring, advocacy, and enforcement support at the national level.

ACKNOWLEDGEMENTS

For their time and valuable contributions, the Nature Crime Alliance thanks the members of the INTERPOL Wildlife Crime Working Group, the INTERPOL Environmental Security Unit, UK National Wildlife Crime Unit, ADM Capital Foundation, Conservation South Luangwa, EAGLE network, the Environmental Investigation Agency, Lilongwe Wildlife Trust, United for Wildlife, Wildlife Conservation Society and Wildlife Investigators Training Alliance. Thanks also go to the Nature Crime Alliance Secretariat team involved in peer reviewing this publication, particularly Tsvetilena Bandakova and Davyth Stewart.

ABOUT THE NATURE CRIME ALLIANCE

The Nature Crime Alliance is a global, multi-sector network that raises political will, mobilises financial commitment, and bolsters operational capacity to fight nature crime and the other international criminal activities with which it converges. Its Secretariat is hosted by World Resources Institute.

Find out more at **naturecrimealliance.org**

ACRONYMS

AIS	Automatic Identification System (for tracking vessels)
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CSO	Civil Society Organisation
HUMINT	Human intelligence
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCB	National Central Bureau (INTERPOL)
NGO	Non-Governmental Organisation
OSINT	Open-source intelligence
WITA	Wildlife Investigators Training Alliance

INTRODUCTION

Effective, intelligence-led policing of environmental crime depends on the continuous collection of information from a wide range of sources, including Non-Governmental Organisations (NGOs) and other Civil Society Organisations (CSOs). When appropriately gathered and shared, this information can help law enforcement agencies enhance existing intelligence, identify criminal actors and activities, and develop new lines of enquiry.

Beyond individual investigations, information collected by CSOs can also support strategic analysis. Analysis conducted by CSO can help identify high-risk environmental sectors, highlight source, transit, and destination countries of concern, and track emerging criminal trends or shifts in ***modus operandi***. This type of information is valuable to law enforcement for strategic planning, priority-setting, and anticipating new threats, complementing its use in operational investigations.

In addition to their national role, CSOs can also add significant value in transnational cases. Many operate across borders through regional structures or global partnerships, giving them a unique ability to spot cross-jurisdictional links and connect investigators with counterparts abroad. Unlike formal law enforcement communication systems, which can sometimes be slow, CSOs often maintain long-standing informal relationships that help to quickly identify trusted contacts in other countries. This complementary role makes them particularly valuable in cases where criminal activity spans multiple jurisdictions.

A global threat

INTERPOL conducts regular global threat assessments to identify environmental crime risks and establish strategic priorities for the international law enforcement community. These assessments may focus on specific sectors, such as wildlife crime, based on the scale of the threat and global enforcement needs. In its most recent ***Wildlife Crime Threat Assessment (2024)***,[1] INTERPOL concluded that the global threat level posed by wildlife crime is high, with an upward trend expected over the next three to five years across all geographical regions. Wildlife crime was ranked among the top 10 highest-scoring global threats across all crime types, highlighting its growing scale, complexity, and impact.

This 2024 threat assessment also underscores the complexity of wildlife crime, noting that transnational criminal networks involved in these offences operate with increasing sophistication, expertise, and adaptability. These characteristics demand an equally adaptive and coordinated response. The threat assessment emphasises the need for a multi-disciplinary approach that brings together law enforcement agencies, non-governmental organisations, and other stakeholders. INTERPOL has an ongoing mission to strengthen its engagement with civil society organisations and other non-law enforcement institutions in the collection and analysis of relevant data.

INTERPOL and its Working Groups are well positioned to facilitate coordination between law enforcement, government agencies, and civil society organisations. Further, with its neutral mandate, global membership, and operational reach, INTERPOL serves as a trusted platform for setting enforcement priorities, supporting cross-border investigations, and strengthening cooperation between state and non-state actors in the fight against environmental crime.

In a survey disseminated by the Nature Crime Alliance, many law enforcement agencies reported high levels of engagement with civil society organisations and acknowledged the value of CSO contributions. A total of 95% of respondents indicated that they had previously used information provided by CSOs to support operational activities. Moreover, 86% of respondents rated the quality of this information as either good or excellent, underscoring the significant potential of CSOs to contribute meaningfully to environmental crime investigations when information is credible, well-documented, and aligned with enforcement needs. Best practices were identified and are set out in these guidelines.

It is also important that civil society organisations align their information collection and engagement strategies with INTERPOL's identified high-risk areas, across all types of environmental crime. By focusing efforts on the most urgent and strategically important threats, CSOs can maximise the impact of their contributions and better support law enforcement operations.

As an example of INTERPOL's strategic priorities, the INTERPOL ***Wildlife Crime Threat Assessment (2024)*** identifies eight priority species groups considered to pose the highest risk and requiring coordinated enforcement attention. These include birds, reptiles, elephants (and ivory), big cats and other felines, rhinos (and rhino horn), primates, turtles and tortoises, and pangolins (including their scales and derivatives). These priority species, and their parts, will guide the work of the INTERPOL Wildlife Crime Working Group and are intended to inform law enforcement and civil society efforts focused on wildlife crime.

The value of CSOs

Many civil society organisations have established dedicated investigative teams, often staffed by former or retired law enforcement officers, to identify and collect information on environmental crime. These teams may conduct undercover investigations, cultivate relationships with confidential informants, and gather firsthand accounts from local communities—particularly those living in or near forests or other vulnerable ecosystems. These CSOs also monitor businesses involved in natural resource extraction to ensure compliance with environmental laws.

Some CSOs operate in a manner similar to investigative journalists, using covert methods to access information and build trust with sources in order to expose environmental wrongdoing. In many cases, they also work closely with community members who provide detailed observations of illegal logging, mining, and other activities occurring in their surroundings.

In addition to field investigations, many environmental CSOs employ intelligence analysts. These experts examine open-source information—including shipping and trade records, satellite imagery, company disclosures, and government reports—cross-referencing data to detect indicators of environmental crimes, corruption, or related offences such as tax evasion.

While some CSOs have established effective mechanisms to engage with law enforcement, unfortunately others lack the means or relationships to do so. In such cases, CSOs may resort to publishing their findings in the media to raise public awareness. While understandable, this approach can unintentionally compromise investigations by alerting suspects, leading to the destruction of evidence, endangering sources, or undermining future prosecutions.

Stronger collaboration

These guidelines aim to assist law enforcement and CSOs to collaborate effectively to support investigations related to environmental crime. The goal is for CSOs to make information-sharing with authorities a standard practice before pursuing any public campaigns.

The quality, accuracy, and reliability of the information collected by CSOs can vary significantly depending on the methods used. Therefore, it is essential that CSOs apply well-documented procedures to verify and record their findings.

High-quality submissions increase the likelihood of enforcement action and help build long-term trust between CSOs and law enforcement, positioning the CSO as a reliable and valuable source of information and a key partner in the fight against environmental crime.

At the same time, these guidelines call on law enforcement agencies to take information provided by CSOs seriously, to verify it and act on it where appropriate. While inaction may sometimes be due to limited capacity, inadequate resources, poor coordination, or institutional inertia, such explanations are often not visible to external observers.

In the eyes of the public—and frequently from the perspective of CSOs themselves—failure to act is most commonly interpreted as a sign of corruption. This perception can further erode public trust in enforcement institutions and seriously undermine collective efforts to combat environmental crime.

GUIDELINES

1. Helping law enforcement to understand the role of CSOs in environmental crime investigations

This chapter provides law enforcement with an overview of the different functions that CSOs may perform in the collection of information, while also identifying key ethical and legal considerations that must be observed.

Civil society organisations contribute in diverse and often complementary ways to the detection and disruption of environmental crimes. Their roles vary, from community monitoring and open-source analysis to covert documentation of offences and engagement with affected stakeholders. As non-state actors, CSOs are not subject to the same mandates or protections as law enforcement agencies, and must therefore operate with caution, professionalism, and a clear understanding of the limits of their authority. Recognising these roles and constraints is critical to fostering effective and lawful collaboration between civil society and law enforcement agencies.

Information collected by CSOs

The information collected and shared by CSOs varies widely and may be derived from a combination of direct field observations, investigative techniques, and structured analytical processes. The types of information collected by CSOs often fall into the following categories:

I. Geographic information identifying criminal activity hotspots, such as:	• Locations of poaching incidents or wildlife snares. • Border crossings or trade routes frequently used for smuggling. • Remote storage sites or location of illegal logging operations.
II. Descriptions of criminal methods, including:	• Techniques used to harvest, transport, or conceal illicit commodities. • Use of fraudulent documents to facilitate illegal trade. • Methods used to bribe officials or avoid detection.
III. Temporal information pinpointing when crimes are most likely to occur, such as:	• Time of day or week when border crossings are least monitored. • Seasonal trends in poaching or illegal fishing.
IV. Financial intelligence, including:	• Indicators to identify suspicious financial transactions. • Evidence of illicit financial flows. • Offshore holdings used for money laundering.
V. Profiles of criminal networks, identifying:	• Key actors, facilitators, and enablers, and their roles and responsibilities within the criminal networks. • Relationships between suspects. • Organisational structures and hierarchies.

Incidents

Civil society organisations may also provide specific data related to particular incidents, including:

- Evidence of the commission of specific criminal acts, such as wildlife poaching incidents, illegal timber trafficking, or the unlawful disposal of waste.
- Identification of individuals or entities involved in illegal activities, including names and aliases of suspects or company names linked to illegal operations.
- Information about specific methods being used to commit criminal acts, such as concealment methods for smuggling goods.
- Communication channels used by suspects (e.g. phone numbers, encrypted messaging platforms, and website addresses used to facilitate the sale of environmental goods).
- Vehicle and vessel information, such as trucks used to smuggle commodities across borders, shipping containers used to transport items or vessels involved in illegal fishing operations.
- Financial or bank account details, information about offshore holdings, or mechanisms used to hide proceeds of crime.
- Addresses and operational sites, such as the location of black-market shops or warehouses used to store illicit goods.

Methods of collection

CSOs gather information through a range of methods, depending on their mandate, technical capacity, and access to sources. Common approaches include:

Human intelligence (HUMINT) such as testimonies and witness statements

This includes information gathered directly from individuals on the ground—such as local residents, indigenous community members, or frontline defenders—that can provide unique insights into ongoing environmental crime. These accounts often form the first indication of illegal activity and are essential to building situational awareness in remote or under-monitored areas. Examples include:

- First-hand accounts from local residents or indigenous communities of illegal logging, poaching, or dumping activities.
- Statements from community leaders, forest rangers, or whistleblowers.
- Interviews conducted during field missions or community engagement initiatives.

It is important that testimonies and witness statements are carefully documented, verified, and handled in a way that protects the identity and safety of the source.

Audio and visual recordings

Audio-visual material can be used to substantiate claims, illustrate the scale or impact of criminal activity, or capture real-time evidence. Such methods are often used during undercover investigations or market surveillance. Examples include:

- Hidden cameras or voice recorders to capture covert recordings of illicit transactions or meetings.
- Photos or video footage of seized wildlife products or logging operations.
- Surveillance footage from markets or suspect facilities showing trade hubs or known trafficking routes.

Where possible, recordings should be time-stamped, geotagged, and stored securely to ensure admissibility and integrity.

Open-source intelligence (OSINT)

Civil society organisations frequently analyse publicly available data sources to detect and document environmental crime. Open-source intelligence (OSINT) is an essential component of modern investigative work. This form of information gathering is cost-effective, non-intrusive, and often yields valuable insights when cross-referenced with other forms of information. OSINT includes not only freely accessible information but also data from commercial databases available through paid subscriptions, such as global trade records or high-resolution satellite imagery.

Given the sheer volume of open-source information available, analysing this data can be overwhelming for many law enforcement agencies. Environmental crime units, in particular, may lack the dedicated personnel or analytical resources required to monitor, process, and interpret open-source data on a regular basis. In this context, CSOs can serve as valuable partners by helping to bridge the capacity gap.

Some CSOs have reported using specialised software tools to monitor and analyse a broad range of online platforms, including social media channels and cryptocurrency payment providers. These tools help identify suspicious data patterns, verify or contradict official records, and can uncover links between seemingly unrelated actors or operations. This information allows analysts to detect potential violations of environmental laws, identify high-risk areas or actors, and establish network linkages that would otherwise be difficult to identify. When triangulated with field observations, witness accounts, or financial records, OSINT significantly strengthens the credibility and evidentiary value of information shared by CSOs. Examples of commonly used open-source data include:

- **Satellite and remote sensing data** used to detect deforestation and identify illegal logging patterns, locate unauthorised mining activities, monitor pollution incidents such as oil spills or chemical leaks, and analyse high-resolution satellite imagery for infrastructure expansion, encroachment into protected areas, or new extraction activities.
- **Government and corporate records** used to analyse Environmental Impact Assessments to identify omissions or false reporting, review emissions and carbon footprint reports to uncover unreported environmental damage, examine fishing quotas and logging permits for irregularities or non-compliance, scrutinise customs declarations for inconsistencies in trade volumes or declared commodities, and access corporate registries to determine beneficial ownership or identify links between companies involved in environmental crimes.
- **Shipping and trade databases** used to monitor illegal fishing in marine protected areas using tools such as Global Fishing Watch, identify discrepancies or anomalies in wildlife trade permits using the CITES Trade Database, and analyse AIS vessel tracking data to detect transhipments at sea, illegal port entries, unauthorised extraction or trade patterns. Subscription-based trade databases can be used to analyse shipping trends, flag unusual patterns in wildlife or timber exports, or link export volumes to suspicious actors.
- **News reports and social media**, used to track real-time developments in environmental crime investigations and prosecutions, identify emerging trends or locations of interest reported by journalists or citizen monitors, monitor social media posts, videos, and images to identify potential online trade or reports made by eyewitnesses or whistleblowers, and track activity on online marketplaces and classified platforms where wildlife products, timber, or other illicit goods may be advertised or sold.

Monitoring online marketplaces

INTERPOL threat analysis has repeatedly recognised that criminals are increasingly using social media and online marketplaces to traffic protected species, taking advantage of these platforms' anonymity, wide reach, and transboundary nature. The online trade in wildlife, however, remains relatively unsophisticated compared to other cybercrimes, with much of the activity still occurring on open-access platforms like Facebook, TikTok and Instagram, as well as regional platforms (such as WeChat and Line in Asia, and Mercado Libre in Latin America).

The scale of this criminal activity can be demonstrated by one study by IFAW[2] of online marketplaces in the US that found nearly 400 animals or parts of protected species were being advertised for sale every week, with almost no supporting documentation. This study revealed that many traders deliberately avoid using flagged keywords such as "ivory," making detection more difficult and underscoring the need for human-led monitoring alongside algorithmic tools.

The online trade of illegally sourced wildlife has created an opportunity for collaboration between law enforcement and civil society. The online platforms are typically open-source, meaning that CSOs can lawfully access, monitor, and analyse online activity without the need for judicial authorisation. This accessibility allows CSOs to conduct proactive surveillance of online marketplaces, identify patterns in trafficking methods, and flag advertisements for illegal wildlife products. CSOs also have greater flexibility to monitor content across borders, where law enforcement may face jurisdictional constraints in collecting digital evidence from foreign platforms.

The role of CSOs in transnational cases

Transnational environmental crime is where CSOs can play a particularly valuable role in supporting law enforcement. Many CSOs have an international footprint—through regional offices, global networks, or collaboration with like-minded organisations—which allows them to identify and connect with trusted law enforcement contacts across multiple jurisdictions. This global reach means that CSOs can be important intermediaries, who can facilitate cross-border cooperation by introducing investigators to their counterparts abroad. Unlike law enforcement, which often relies on formal, and sometimes slow, communication channels, CSOs can leverage informal and well-established relationships to identify who within a foreign law enforcement agency has the mandate and willingness to act.

Legal and ethical considerations

When collecting information related to environmental crime, CSOs must adhere to ethical and legal standards. This may include obtaining informed consent when interviewing individuals, protecting the confidentiality and safety of sources—particularly in high-risk contexts—and ensuring the secure handling of sensitive data. CSOs should also take care not to interfere with ongoing investigations or actions by law enforcement, nor compromise potential evidence.

Many CSOs involved in environmental crime investigations, for example, engage in undercover work, which raises particularly complex legal and ethical challenges. In many jurisdictions, there is legal ambiguity surrounding such investigative methods. CSOs are neither formally recognised as law enforcement agents nor consistently protected under laws governing journalism. As a result, field operatives and source networks face considerable personal and legal risk, particularly when exposing high-level corruption or organised criminal activity. To mitigate these risks, CSOs undertaking such investigations may wish to consider registering as media or journalism organisations. While this does not guarantee immunity, it can provide an additional layer of legal protection, especially in cases of arrest, detention, or threats of prosecution.

CSOs should also be aware that some jurisdictions impose legal restrictions on the collection or dissemination of certain types of information. These may include prohibitions on reporting about specific individuals—such as members of a royal family or political leadership—or on publishing material that could be considered defamatory, politically sensitive, or seditious. These restrictions may apply even where the information collected is accurate. It is strongly recommended that CSOs seek legal advice to ensure compliance with applicable national laws and regulations governing information collection, publication, and sharing.

It is also important to recognise that, in many jurisdictions, law enforcement agencies operate under strict legal frameworks that govern how information can be obtained, stored, and used—particularly in relation to evidentiary standards. These requirements often do not apply to CSOs or other non-state actors. As a result, information collected by a CSO, while potentially valuable for intelligence purposes, may not meet the evidentiary standards or legal threshold for use in court. In such cases, the information may inform investigations but could be inadmissible during prosecution.

2. Helping CSOs meet quality standards for the information they share

This chapter provides civil society with an overview of how law enforcement assesses the value of information they receive. By understanding this assessment process, CSOs can ensure that the information they provide meets the necessary quality standards.

Assessing the value of information

For information to support meaningful law enforcement action, it must meet certain standards of quality that align with operational and intelligence-led policing requirements. High-quality information is more likely to be prioritised, verified, and acted upon, making it a more effective tool for investigations and enforcement efforts.

Information is generally considered high value when it meets the following criteria:

- **Relevant to policing purposes**: It directly relates to a recognised policing function, such as detecting, preventing, or investigating environmental crime.
- **Detailed**: It precisely identifies the issues and presents a coherent picture.
- **Comprehensive**: It includes sufficient facts or supporting material to enable analysis or operational follow-up, or clearly identifies any gaps, uncertainties, or limitations.
- **Reliable**: It is supported by credible evidence and comes from sources assessed as trustworthy or previously validated.
- **Time-sensitive**: It is submitted promptly, allowing law enforcement to respond, preserve evidence, or prevent harm in a timely manner.
- **Legally obtained**: It is collected in compliance with applicable laws and ethical standards, ensuring its admissibility and integrity.

By aligning submissions with these criteria, CSOs can greatly increase the utility of the information they provide and strengthen their role as trusted partners in the enforcement of environmental law.

Ensuring information is relevant for policing purposes

When sharing information with law enforcement, it is essential that CSOs ensure the information relates to a legitimate policing purpose. While many environmental issues may be morally or ethically troubling, not all cases of environmental degradation constitute a breach of the law. In some instances, law enforcement agencies may lack the legal mandate to act, even where there is significant harm to the environment.

Law enforcement can only act upon information that relates to one or more of the following policing purposes:

- An actual or alleged breach of the law.
- The protection of life and property.
- The preservation of public order.
- The prevention of criminal offences.
- The apprehension or prosecution of offenders.
- Any legal duty or responsibility imposed by law.

Information falling outside these categories—such as concerns about poor environmental practices that are not prohibited by law—may not be actionable by police or enforcement authorities.

If necessary, CSOs should consider obtaining legal advice in the relevant jurisdiction to ensure the information they share with law enforcement clearly aligns with at least one of the above areas.

Evaluating reliability and credibility of information

All information received by law enforcement, including that provided by civil society organisations, is subject to an evaluation process to determine its reliability and potential operational value. To manage this process consistently, law enforcement agencies commonly use grading systems that assess two key aspects:

(i) the reliability of the source, and
(ii) the accuracy of the information itself.

This evaluation process recognises that a trustworthy source may provide false information, and an untrustworthy source may provide accurate information. Each element is assigned a grade—often using letter and number codes (e.g., A1, B2)—which helps law enforcement personnel determine how the information can be used, whether further verification is required, and the level of confidence they can place in it. This structured approach ensures that investigative decisions are based on sound judgment and that unreliable or unverified information is handled with appropriate caution.

To maximise the usefulness of the information provided to law enforcement, civil society organisations are encouraged to establish their own internal review mechanisms that evaluates both the source of the information and its content. All information collected to civil society should be corroborated and subject to evaluation by trained investigators within the CSO.

Establishing internal review mechanisms helps safeguard against errors, false claims, or manipulation by malicious actors. Sources should be subject to the "How/Why Test" each time they pass information to the CSO. This approach is designed to uncover the motive of the source ("why" they are providing the information) and assess the means by which the information was obtained ("how" they came to know it). Applying this test consistently assists in determining both the veracity of the source and the reliability of the information. Aligning information collection and evaluation practices with the grading systems used by law enforcement agencies enhances the credibility of the submission and improves its potential operational value.

Assessing the reliability of the source

The first step used by law enforcement in evaluating information is to assess the reliability of the source. This involves determining whether the person or organisation that provided the information is trustworthy, competent, and in a position to know the facts they are reporting. It also requires consideration of any potential bias or ulterior motives that may affect the credibility of the information. This assessment gives law enforcement a clear understanding of how much confidence can be placed in the origin of the information before it is used to guide investigative or operational decisions.

This step helps ensure that action is not taken based on unverified or misleading intelligence, and promotes a responsible, consistent approach to information management. Where possible, the **original source** of the information should be identified and evaluated. Sources are typically classified into one of three categories:

- **Reliable**: a source with a proven track record of providing accurate and credible information, with no reason to doubt their integrity or trustworthiness.
- **Unreliable**: a source known to have provided false or misleading information in the past, or whose motivations are questionable.
- **Untested**: a source who is new or unknown, and whose reliability cannot yet be confirmed due to a lack of previous engagement or corroborated reporting.

To assist in evaluating the reliability of the source, careful consideration should be given to the following questions:

- Is the source clearly identified, or have they remained anonymous?
- Has this source provided information previously, and if so, was it found to be accurate and reliable?
- Is the source technical (such as CCTV footage, biometric data, or forensic evidence), or human (such as a witness or informant)?
- What is the known or presumed motivation of the source in providing the information? Could any bias or self-interest be influencing the report?
- Was the information obtained lawfully and in accordance with applicable ethical and legal standards?

Law enforcement should conduct due diligence on the CSO providing the information

When information is provided by a civil society organisation, it may be necessary to assess the reliability of both:

(i) The CSO acting as the intermediary; and
(ii) The original source(s) from whom the organisation obtained the information (e.g. community members, informants, or investigative staff).

This dual assessment is important because either the intermediary (the CSO) or the original source may have biases, vested interests, or ulterior motives that could influence how the information was collected, interpreted, or reported. For example, if a CSO submits a report based on interviews with local community members, the recipient law enforcement agency must consider the credibility and objectivity of both the CSO and the individuals providing the information, as either may have incentives that unintentionally or deliberately distort the facts.

From the survey responses, law enforcement agencies were asked to identify challenges that impact the effective use of information provided by CSOs. A recurring concern was the potential for bias, with some respondents noting that CSOs may present information in ways that reflect their advocacy goals or organisational agendas, rather than strict evidentiary standards. This includes instances where information may be overstated, emotionally driven, or based on incomplete or non-standardised methods.

Law enforcement agencies that receive information from a civil society organisation have a responsibility to conduct due diligence to determine whether the CSO is a trustworthy and competent source. This assessment may involve reviewing several key factors, including:

- **Track record of reliable reporting**: Law enforcement should assess whether the CSO has a history of submitting accurate, credible, and actionable information. Consistency in prior reporting and alignment between current and previous submissions can help build confidence in the organisation's reliability. Agencies are more likely to act on information from CSOs that have demonstrated professionalism and integrity in previous information-sharing engagements.
- **Trusted references:** Law enforcement may also seek endorsements or references from other reputable organisations—such as international bodies, enforcement agencies, or vetted CSOs—that have prior experience working with the CSO in question.
- **Reputation and credibility review**: Law enforcement should conduct open-source research to assess the CSO's public standing, independence, professionalism, and to confirm that it adheres to recognised investigative, ethical, and data protection standards. It is important that the CSO appears to be an impartial actor with no political, financial, or reputational motives to provide misleading or manipulated information.
- **Formal information-sharing agreements**: In some cases, law enforcement may insist on a formal arrangement such as a Memorandum of Understanding (MoU) or data-sharing agreement that clearly define the protocols for communication, confidentiality, and data handling. Importantly, these agreements establish that a CSO may be held legally accountable—and in breach of the agreement—if it fails to comply with these protocols.
- **Familiarity through past cooperation**: Law enforcement will also consider any prior engagement it has had with the CSO, including in other professional contexts such as participation in joint training initiatives, multi-stakeholder forums, or capacity-building programmes. While these may not have involved direct information exchange, such experience can still provide law enforcement with insight into the CSO's professionalism, values, and operational culture.

If there are concerns about the CSO's credibility—or if previously submitted information has proven incomplete, inaccurate, speculative, or unverifiable—law enforcement may decide to disregard current or future submissions. This is particularly likely when information contradicts existing intelligence or lacks adequate supporting evidence.

Assessing the information

Once the reliability of the source has been evaluated, the next step is to assess the information itself, focusing on its credibility, reliability, and potential operational value. This involves grading the information according to the degree of confidence that can be placed in its accuracy, based on how it came to be known by the source. Information may fall into several categories depending on its origin:

- It is first-hand information, directly observed or experienced by the source.
- It has been relayed through one or more intermediaries, reducing the certainty of its accuracy.
- It is considered unreliable, such as information based on rumour, speculation, or unverified opinion.

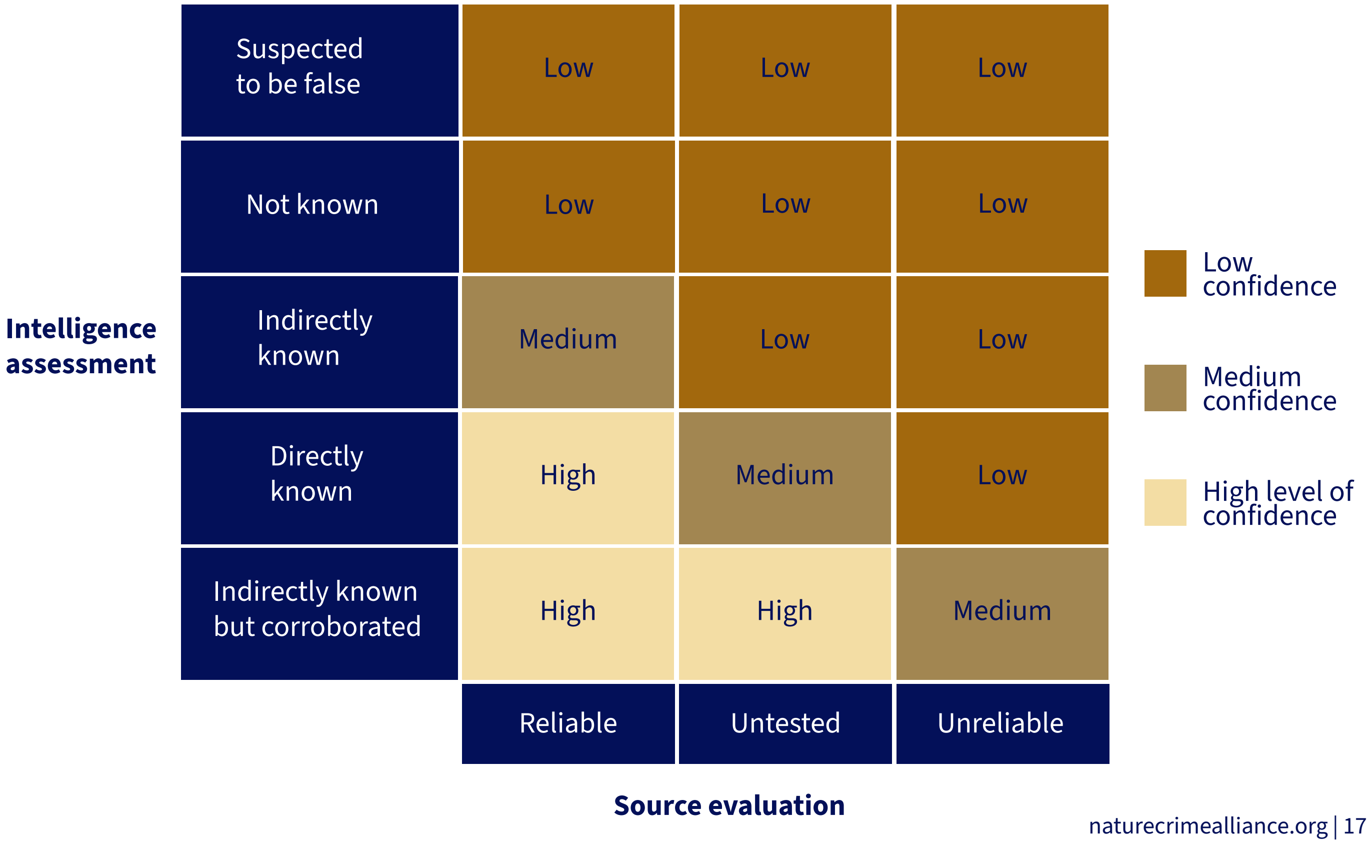
This grading helps law enforcement and intelligence personnel assess how likely the information is to be true. The more direct and verifiable the information, the greater its potential value.

The following questions are likely to be used by law enforcement to evaluate the reliability of information received from civil society:

- Is the information known personally to both the source and the CSO reporting it?
- Is it known personally to the source, but not the CSO reporting it?
- Is the information based on rumour, personal opinion, or hearsay?
- Has the information been corroborated by other independent or official sources?
- How specific, detailed, and complete is the information provided?
- Under what circumstances was the information collected (e.g. firsthand observation, undercover work, or second-hand report)?
- Is there any reason to question the reliability, objectivity, or accuracy of the information?

Examples of evaluation frameworks

The UK-based NGO, the Environmental Investigation Agency, uses an internal framework modelled on the UK National Intelligence Model to assess and document the reliability of its information before sharing it with authorities. This evaluation framework uses a 3x5 standardised system for evaluating and grading intelligence information. The overall level of confidence that can be placed in the information is determined based on the combination of both the reliability of the source and the validity of the intelligence.



Intelligence assessment	Reliable	Untested	Unreliable
Suspected to be false	Low	Low	Low
Not known	Low	Low	Low
Indirectly known	Medium	Low	Low
Directly known	High	Medium	Low
Indirectly known but corroborated	High	High	Medium

Source evaluation

■ Low confidence

■ Medium confidence

□ High level of confidence

Similarly, the Wildlife Conservation Society and the Wildlife Investigators Training Alliance (WITA), both headquartered in the United States, use the NATO Intelligence Source and Information Reliability System—commonly referred to as the Admiralty Code—to evaluate the credibility of sources and the reliability of the information they provide. WITA has adapted the Admiralty Code with the addition of a colour code scheme to indicate the overall level of confidence that can be placed on the information.

Source reliability			Information credibility
Reliable	A	1	Confirmed
Usually reliable	B	2	Probably true
Fairly reliable	C	3	Possibly true
Not usually reliable	D	4	Doubtful
Unreliable	E	5	Improbable
Unknown	F	6	Unknown

By adopting similar models, CSOs can strengthen their position as credible, professional partners in the fight against environmental crime.

Handling and sharing of information

In addition to evaluating the source reliability and the credibility of the information, many law enforcement agencies apply a third element in the grading process: the handling code. This classification determines how information may be used, stored, or shared, based on legal obligations, operational sensitivity, and the need to protect the source.

Handling codes are a critical part of responsible intelligence management. They ensure that sensitive information, particularly where it involves personal data, confidential sources, or material collected under legal or ethical constraints, is used and disseminated in a way that upholds investigative integrity, complies with national and international legal standards, and protects individuals from harm.

A key consideration in applying a handling code is whether disclosing the information could expose the source to risk of identification or retaliation. For example, if only one person could have plausibly accessed or known the reported information, and law enforcement acts on it, it may become obvious who provided the tip, potentially placing that individual at serious personal risk.

In the context of environmental crime, which often crosses national boundaries, it is also important to assess whether the information is of national or transnational concern:

- Information relevant only to the country where the offence occurred should be retained and managed by the local or national law enforcement agencies.
- Information with a transnational element—such as the cross-border movement of illegal commodities, suspects, or financial flows—may also need to be shared with an appropriate regional or international law enforcement body, such as INTERPOL.

It is important to note that only information shared through authorised national law enforcement channels can be entered into INTERPOL's global databases. Civil society organisations cannot necessarily submit data directly to these systems, but may contribute valuable information that, once validated and shared through proper channels, supports international law enforcement efforts.

Covert and undercover investigations

Any CSO that deploys covert tactics must be aware that, in many jurisdictions, law enforcement operations are bound by legal standards designed to ensure procedural fairness. These include the need to avoid entrapment or other forms of inducement that could jeopardise the legal admissibility of evidence or undermine prosecutions. As a matter of best practice, any organisation engaging in undercover activity should ensure that their personnel receive training in lawful covert operations. This training should align with standards accepted by law enforcement (rather than military or intelligence frameworks), with a focus on both the integrity of any resulting investigation and the safety of operatives.

For CSOs involved in undercover operations or covert recording of illicit activity, the CSOs must take great care not to engage in activities that could be construed as entrapment, particularly when interacting with individuals suspected of environmental crime. Entrapment occurs when a person is induced or encouraged to commit a crime they would not have otherwise committed. To avoid this, investigators should always act as passive observers—never initiating illegal transactions or suggesting prices for contraband. Instead, they should aim to document the clear, voluntary intent of the suspect, allowing the offender to take all active steps in any illegal arrangement.

It is also essential to emphasise that CSOs are not law enforcement agencies and do not have the same legal mandates or protections. Activities such as surveillance, wiretapping, covert recording in private spaces, and controlled deliveries typically require judicial authorisation or statutory powers not available to CSOs. Attempting to conduct such operations without appropriate authorisation can result in legal consequences for the CSO. CSOs must, therefore, be cautious not to cross the boundary between lawful observation and unlawful surveillance or interference, and they are strongly advised to seek legal counsel before engaging in sensitive or high-risk activities.

In particular, CSO investigators should avoid physically handling or transporting illicit goods, such as wildlife products or toxic materials, to prevent compromising their neutrality and to reduce legal exposure. Wherever possible, conversations should be covertly recorded in public spaces, where there is no reasonable expectation of privacy—both to protect the legality of the recording and to ensure the safety of the investigative team.

Disclosure, chain of custody, and data management

Law enforcement agencies in many jurisdictions are subject to legal obligations to disclose to the accused all information relevant to a criminal case, including both used and unused material. This legal requirement is designed to ensure fairness and uphold the rights of the accused. To support this, any information submitted by CSOs must be properly documented and stored to allow authorities to maintain a ledger of received material, including any information that is ultimately not used in the case.

CSOs should keep clear records of the source, time, method of collection, and any handling of the information. This obligation applies to original files (e.g., recordings, transcripts, notes) as well as analysis or summary documents. Law enforcement may also require the original copies to verify authenticity and integrity.

In addition, law enforcement agencies may need assurances that all materials shared with them has been securely stored and managed in accordance with data protection laws and sovereignty considerations, particularly where the information relates to cross-border offences or is stored on cloud servers outside the jurisdiction.

To assist with this, CSOs are encouraged to implement a basic chain-of-custody log and to clarify the storage location and access controls for any sensitive material. Where possible, CSOs should avoid sharing sensitive data through unsecured channels and follow best practice guidelines for digital data transfer.

3. Recommendations for CSOs to improve their contributions

This chapter provides guidance for CSOs to ensure that the information they share is of value to law enforcement.

When providing information to law enforcement, CSOs should consider the following best practices to assist in the evaluation process:

1. Share their internal assessment of reliability and credibility

When submitting material to law enforcement, CSOs are encouraged to include their own internal evaluation of the source and the information. This helps law enforcement understand the context in which the information was gathered, how it was evaluated, and provides a valuable foundation for further verification. This allows law enforcement to make informed decisions about how the information should be used and whether additional validation is needed before taking action.

2. Provide supporting evidence

Where available, submit corroborating material such as photographs, copies of communications (e.g. emails, social media messages), transaction records, or other documentation. This strengthens the credibility of the report and aids law enforcement in determining its evidentiary value.

3. Include contextual background

Especially in the case of raw data or indirect observations, provide context explaining how the information was obtained, under what circumstances, and whether any specific methods (e.g. undercover work, open-source analysis) were used.

4. Detail the credibility of the source

Include relevant background about the source, such as their prior reliability, knowledge of the subject, and any relevant motivations or biases.

5. Facilitate direct communication

Whenever possible, provide contact details for a representative of the CSO who can respond to follow-up questions, clarify aspects of the information provided, or supply additional documentation. Open and responsive communication enhances trust and operational effectiveness.

By adopting these practices, CSOs can strengthen their role as credible partners to law enforcement.

Formatting and structuring information for law enforcement use

CSOs should consult with relevant law enforcement contacts to determine the preferred format and structure for submitting information. Survey feedback highlighted that while law enforcement agencies are generally able to receive information in a variety of formats, the most suitable format will depend on the nature of the information and the intended recipient within law enforcement. For instance, investigators may prefer narrative-style case files with documented evidence and witness testimonies provided in Word documents or PDFs. In contrast, intelligence analysts may favour structured raw data in spreadsheets, which can be sorted, cross-referenced, or integrated into analytical tools.

Law enforcement agencies are encouraged to develop standardised templates for CSOs to use when submitting information. Standardised formats help ensure that submissions are complete, consistent, and easy to review across multiple law enforcement functions. Clear formatting also facilitates better documentation of sources, dates, and locations.

Law enforcement have noted that poor formatting or inconsistent documentation can significantly reduce the usefulness of CSO-submitted information. The absence of uniform reporting protocols or structured forms was identified as a barrier to efficient cooperation.

CSOs should not withhold information

Even if a CSO assesses certain information as potentially unreliable or seemingly insignificant, it is still important to share it with law enforcement. CSOs should avoid editing out details they consider unimportant, as what may appear irrelevant to them could be critical to an ongoing investigation. Law enforcement agencies often possess additional intelligence or context that allows them to identify patterns, validate leads, or corroborate facts that could otherwise be overlooked.

The role of the CSO is to provide information, not to determine its final value or operational use. By providing all information, law enforcement agencies are able to make their own informed decisions based on the full scope of available data.

4. Recommendations for law enforcement in verifying information received from CSOs

While civil society organisations can provide valuable intelligence, law enforcement should also independently verify the information before acting on it. This chapter shares guidelines to support verification.

The following steps can help law enforcement agencies assess the reliability, relevance, and integrity of the information received:

1. Assess alignment with internal intelligence

Evaluate whether the CSO-provided information is consistent with existing intelligence or criminal analysis.

2. Cross-reference with official databases

Verify the information against internal law enforcement databases, government records, or other authorised data sources. Cross-referencing can reveal corroboration or identify discrepancies that warrant further investigation.

3. Re-interview key witnesses if necessary

Where practical and appropriate, law enforcement should consider re-interviewing witnesses or sources cited by the CSO to verify the statements and clarify any uncertainties.

4. Assess the authenticity of any media content

Law enforcement should be aware of the increasing risk of manipulated media, including deepfake video or audio content. Where recordings are provided, forensic image and audio analysis should be considered to confirm authenticity and detect signs of tampering.

5. Strengthening the relationship between CSOs and law enforcement

This chapter explores the importance of building trusted relationships between CSOs and law enforcement.

Unfortunately, in many jurisdictions where environmental degradation and natural resource exploitation are most severe, law enforcement agencies may be compromised by corruption, or may lack the capacity, technical expertise, or institutional commitment required to take effective action.

To mitigate these challenges, CSOs are encouraged to invest in building trusted and reliable relationships with law enforcement agencies and establish professional connections with individual officers who are competent, ethical, and genuinely committed to environmental enforcement significantly increases the likelihood that shared information will be acted upon effectively.

The following strategies can be used by CSOs to develop trusted law enforcement contacts:

1. Support training and capacity building

When CSOs provide or participate in environmental crime training and other capacity building initiatives with law enforcement personnel, this offers a practical opportunity to also assess their professionalism, knowledge, and commitment to environmental enforcement.

2. Build trust through outreach and relationship-building trips

One effective way to identify trustworthy law enforcement contacts is through in-person outreach visits. CSOs can organise trips to meet with law enforcement officials directly, creating an opportunity to explore shared interests, discuss collaboration frameworks, and assess the professionalism and openness of potential contacts. These initial engagements should focus on relationship building rather than the sharing of sensitive information.

It is strongly recommended that CSOs withhold operational or source-sensitive data until a strong level of trust has been established—something that often requires repeated interaction and may take years to develop. CSOs must also recognise that trust, once established, is not permanent. Even a previously reliable contact may come under pressure or be compromised.

In jurisdictions where corruption is widespread, any officer, regardless of integrity, may be approached with a bribe or face coercion. In some cases, high-ranking government or senior officials may intervene, instructing a trusted officer to abandon an investigation or suppress information.

These dynamics make it essential for CSOs to remain vigilant, document interactions, and regularly reassess the reliability of their contacts over time. Contingency planning should be in place, even when a relationship appears strong.

6. Risks and operational challenges

This chapter explores some of the challenges that can arise when CSOs and law enforcement collaborate, and provides guidance on how to overcome them and avoid associated risks.

Unreliable CSO information

It is important for civil society organisations to understand that providing unreliable information to law enforcement can create significant risks and operational challenges, including:

- **Wasted resources**: Law enforcement agencies have limited staff and operational capacity. Pursuing inaccurate, misleading, or poorly substantiated information diverts valuable resources away from legitimate investigations and undermines trust between CSOs and enforcement partners.
- **Compromised intelligence**: Unreliable CSO information may cast doubt on existing intelligence holdings, potentially disrupting ongoing investigations or undermining operational planning.
- **Reputational damage**: Acting on flawed CSO information could result in public criticism, loss of public confidence, or reputational harm to the law enforcement agency.
- **Legal exposure**: Agencies may face legal challenges or litigation from individuals or entities affected by enforcement actions based on inaccurate information.

Given these risks, it is essential that law enforcement treat CSO-submitted information with the same level of scrutiny as other forms of intelligence, applying structured evaluation and establishing clear protocols for ongoing collaboration.

Handling information from anonymous or confidential sources

In some cases, individuals who provide information about environmental crime may request to remain anonymous. They may fear retaliation, social stigma, or other risks to their safety. Where possible and appropriate, CSOs should encourage witnesses to provide contact details to enable law enforcement follow-up. However, if anonymity is requested, it is recommended that the CSO still collect and securely record the source's identifying details, but access to this information should be limited to a small number of trusted and vetted CSO staff. This ensures that the information can later be verified by the CSO if needed, while still protecting the identity of the source.

When sharing information with law enforcement, CSOs may sanitize reports—removing or redacting details that could reveal the identity of the source. However, in such cases, it is crucial that the CSO includes its own evaluation of the source's reliability, including any known history, motivation, or prior engagement that may inform an assessment of credibility. The CSO should share its own internal evaluation to allow law enforcement to assess the credibility of the source, and the information provided.

To ensure the protection of whistleblowers and other confidential sources, CSOs are strongly encouraged to adopt robust security protocols, including:

- Anonymising or redacting sensitive details prior to information sharing.
- Using encrypted communication channels and secure digital storage for all sensitive data.
- Limiting access to source-identifying information on a strict need-to-know basis within the organisation.
- In high-risk situations, where there is concern for the safety of a witness or whistleblower, it may be necessary to arrange temporary accommodation in an undisclosed location to prevent exposure or retaliation.

7. Guidance to help CSOs manage corruption risks

CSOs should recognise the risk posed by corruption when engaging with law enforcement. This chapter outlines the different forms such corruption can take, and provides guidelines to mitigate this risk.

One of the most serious risks faced by CSOs when sharing information with law enforcement is the potential for corruption within the law enforcement agency itself. Corrupt officers may leak sensitive information to criminal networks, sabotage investigations, or exploit the information for personal or financial gain. In some reported cases, law enforcement officials have used CSO-provided intelligence to extort suspects, shield high-level offenders, or even retaliate against whistleblowers and witnesses.

This threat poses a significant operational and ethical dilemma for CSOs. It not only affects the criminal investigation, but also poses real danger to CSO staff, field operatives, and community informants. Ensuring the privacy, security, and well-being of these individuals must remain a top priority for any civil society organisation engaged in sensitive investigative work.

CSOs have a duty of care to protect their personnel and local contacts. This includes strict internal protocols for handling source identities and sensitive data. Information should only be shared with law enforcement when it can be done securely, and when there is reasonable confidence that it will be handled appropriately and not released into the public domain. In particularly egregious cases, information provided in good faith has been misused to harass, intimidate, or criminalise witnesses, undermining both justice and public trust.

In addition to overt corruption, CSOs should also be alert to more subtle forms of misconduct, where incompetence is used to disguise corrupt intent. In some cases, corrupt officers deliberately undermine investigations not through obvious sabotage, but by appearing to make procedural errors or mishandling of evidence. For example, they may fail to follow proper arrest protocols, neglect to secure crime scenes, or intentionally disrupt the chain of custody of key evidence. While these acts may be dismissed as negligence or lack of training, they can in fact be calculated moves to weaken the prosecution’s case and ensure suspects avoid conviction. This type of covert corruption is particularly difficult to detect and places additional pressure on CSOs to monitor how their information is used and to document all interactions carefully.

Survey responses from civil society organisations underscore the scale of this concern. All CSOs surveyed reported having experienced instances where the information they submitted to law enforcement was ignored, without explanation or follow-up.

More troubling, half of the CSO respondents indicated that law enforcement agencies had, at some point, leaked sensitive information they had provided, either intentionally or through carelessness, which subsequently reached the criminal networks being investigated. In this context, it is understandable that many CSOs view the failure to act on credible information as a strong indicator of potential corruption within the relevant agency. Whether due to active collusion with criminals or deliberate neglect masked as procedural incompetence, such inaction erodes trust and discourages future cooperation.

Establishing relationships with credible law enforcement contacts takes time and may not always be possible before an investigation needs to be launched. In such cases, CSOs should adopt a cautious and strategic approach to engagement, seeking to identify and support honest, capable officers while limiting exposure to those who may compromise investigations.

These best practice steps are recommended to mitigate any corruption risks:

1. Share information only with trusted law enforcement contacts

Only share information with trusted contacts, preferably those with whom the CSO has an established, professional relationship.

2. Conduct discreet background checks

Validate law enforcement contacts through background checks, reputational vetting, or endorsements from other reliable institutions. CSOs may look to gather information about individual officers, including their track record, involvement in prior cases, and any public or internal allegations of misconduct.

3. Seek peer recommendations

CSOs should consider requesting references from other credible CSOs, inter-governmental bodies, or international law enforcement agencies who have worked with the officers or units in question.

4. Leverage partnerships to share the information

Where possible, CSOs should consider working through other organisations and networks that already have vetted law enforcement partnerships and standard operating procedures for secure engagement. Sharing information with other credible CSOs can also increase external oversight and provide an added layer of accountability.

5. Engage multiple agencies

To reduce risk when sharing sensitive information, CSOs may consider reporting the case to more than one law enforcement agency, where appropriate. Doing so can help mitigate the risk of a single corrupt or negligent actor derailing the investigation.

6. Use formal channels where possible

Formal information sharing channels, including national task forces, vetted inter-agency platforms, or through international organisations such as INTERPOL, have internal accountability mechanisms.

7. Document all exchanges of information

Keep notes of all information shared, including dates, recipients, and content shared, to establish a record in case of future disputes or breaches.

8. Test with low-risk information

CSOs should consider sharing only the minimum information necessary to trigger an investigation. The CSO should then evaluate how responsibly it is handled, and whether it is followed up appropriately. CSOs should avoid disclosing the identity-related information (such as names, contact details, or photos of sources), or sensitive details about investigative methods, unless strictly necessary and only where the recipient law enforcement agency has demonstrated the capacity to protect such information.

9. Monitor the investigation and case outcomes

After sharing information with law enforcement, CSOs should remain actively engaged to track the results of the investigations led by specific officers or units, focusing on transparency, successful prosecutions, and signs of procedural integrity. Where feasible, CSOs should implement oversight measures to ensure the investigation is proceeding lawfully and effectively. This may include regularly visiting police detention facilities to confirm suspects have not been unlawfully released and attending all court appearances to monitor legal proceedings. CSOs should, where possible, request regular updates from their law enforcement contacts. Regular follow-up demonstrates continued interest in the outcome and can deter misconduct or procedural failures.

10. Use public accountability measures

As a last resort—and only after internal escalation efforts have failed—it may be appropriate to engage the media or other public channels. This can raise awareness, apply external pressure, and help ensure a level of public scrutiny over the investigation process.

8. The importance of law enforcement providing feedback

This chapter notes that CSOs often do not receive a response from law enforcement after sharing information. Providing feedback can help law enforcement organisations build trust and strengthen relationships with CSOs that could lead to future successes.

A recurring concern raised by civil society organisations is the lack of feedback following the submission of information to law enforcement. When no acknowledgment or follow-up is provided, CSOs may assume that the information was ignored or dismissed, undermining trust and discouraging future collaboration. In some cases, this lack of feedback may prompt CSOs to publicly publish their findings in an effort to pressure authorities into action.

From a law enforcement perspective, providing feedback—where appropriate and operationally feasible—is a critical tool to strengthen partnerships with civil society organisations. It encourages the ongoing flow of high-quality information, reinforces mutual trust, and positions the CSO as a reliable contributor to the intelligence cycle.

In the survey conducted by the Nature Crime Alliance, civil society organisations were asked what kind of feedback they would find most valuable after submitting information to law enforcement. CSOs overwhelmingly indicated that they would most appreciate guidance on how to improve the quality, presentation, or relevance of the information they provide. However, only 25% of respondents reported having ever received such feedback. Without it, CSOs noted that it becomes difficult to allocate resources effectively or refine their methods for collecting and submitting environmental crime information.

Given the high workload and other operational constraints experienced by law enforcement, CSOs stressed that even minimal feedback will still be valuable. They suggested that short, non-sensitive updates, particularly after an investigation concludes, could help CSOs evaluate whether their submissions were useful and how to improve them in the future. Some CSOs also expressed interest in two-way dialogue, including opportunities to respond to follow-up questions or requests for clarification, which would enable them to strengthen their original submissions and foster more responsive cooperation.

At a minimum, law enforcement agencies should formally acknowledge receipt of any information submitted by a CSO. A simple confirmation that the information has been received and is under review can go a long way in demonstrating professionalism and respect for the CSO's efforts. For law enforcement officers seeking to build long-term, cooperative relationships with CSOs, the following feedback practices are recommended:

1. Provide status updates

Where possible, offer general updates on the relevance or usefulness of the information provided, without disclosing sensitive operational details.

2. Maintain ongoing engagement

If the information proves useful, law enforcement should consider re-engaging the CSO to request clarification, context, or additional data that may support further investigation.

3. Communicate outcomes

At the conclusion of an investigation or case, law enforcement agencies should—subject to legal and operational constraints—inform the CSO of the result. This may include whether enforcement action was taken, charges were filed, or the case was closed.

4. Offer constructive feedback

Whenever possible, provide guidance on how future submissions can be improved, such as increasing specificity, including corroborating material, or aligning reports with legal standards of evidence.

The constraints on law enforcement when providing feedback to CSOs

CSOs should understand that feedback from law enforcement may be delayed due to the operational nature of investigations, particularly if a matter proceeds to court. Furthermore, no feedback will be provided where doing so may:

- Compromise ongoing or future law enforcement operations.
- Reveal confidential sources, surveillance methods, or investigative techniques.
- Breach national security protocols or privacy laws.

CSOs should also not expect feedback relating to how their information fits within broader intelligence frameworks, or whether it links to other ongoing investigations. Such intelligence holdings are classified and governed by legal safeguards that prohibit disclosure to external parties. Law enforcement agencies have a duty of care to the communities they serve, including the protection of operational information, informants, and affected individuals.

Additionally, law enforcement agencies are less likely to share feedback with organisations known to publicise sensitive content without appropriate safeguards. CSOs with a history of publishing internal communications or revealing details to the media may be excluded from future information-sharing dialogues, as this introduces risk and undermines operational security.

It is also important to recognise that feedback practices vary across jurisdictions and agencies. Some law enforcement bodies may be structured to provide regular updates and engage with civil society partners; others may be restricted by legal frameworks or internal policy from offering any feedback at all. While feedback is encouraged as a good practice, it is not always possible, and in many countries, law enforcement is under no obligation to provide it.

Nonetheless, where circumstances allow, feedback should be seen not as a privilege but as an investment in building credible, effective partnerships that support the shared objectives of protecting the environment and the pursuit of justice.

9. Things CSOs should consider before making information public

This chapter highlights the reasons that CSOs may choose to publish information without first sharing it with law enforcement, but notes the risks this could pose - including to potential investigations.

In many cases, CSOs that have not established secure mechanisms for engaging with law enforcement may resort to publishing their findings through the media. This is often done with the intention of raising public awareness or pressuring authorities into taking action. However, while well-intentioned, the premature release of operationally sensitive information can have serious consequences. Public disclosure may alert offenders, giving them the opportunity to destroy evidence, evade capture, or shift operations.

In addition to jeopardising legal proceedings, CSOs should be aware that publishing information about an investigation—particularly before it concludes—may inadvertently reveal investigative techniques, surveillance tactics, or other operational details. This could compromise future investigations or expose vulnerabilities in how operations are conducted.

Avoiding premature publication also serves to protect the safety and security of the CSO's own personnel and sources, who may be exposed to retaliation or legal risk if their involvement becomes public. Caution should be exercised to ensure that public disclosure does not unintentionally endanger those involved in the investigative process.

Where the information collected is potentially actionable, law enforcement should be the first point of contact. When law enforcement is willing and able to investigate, CSOs should prioritise sharing information with law enforcement through secure, confidential channels. That said, there may be instances where CSOs have reasonable grounds to believe that law enforcement will be unwilling or unable to act. In such cases, public exposure may be seen as the only viable strategy to achieve accountability. Law enforcement agencies should understand that the following factors are likely to influence a CSO's decision to publish its findings rather than share them confidentially:

- Perceived or demonstrated inaction by law enforcement in relation to environmental crimes.
- Lack of access to trusted, professional, or secure law enforcement contacts.
- Concerns about corruption, which may place sources at risk or compromise the integrity of the investigation.

In situations where publication is deemed necessary, CSOs should take precautions to ensure that their actions do not inadvertently compromise future law enforcement efforts. Recommended measures include:

1. Redacting or anonymising sensitive operational details

This includes names, locations, or evidence that could identify suspects or informants.

2. Consulting legal or law enforcement experts

Consult legal experts or law enforcement professionals before releasing any material that may have criminal justice implications.

3. Carefully timing the release

This is to avoid interfering with active investigations or judicial proceedings.

4. Limiting public disclosure of investigative methods or source identities

It is important to avoid revealing tactics or exposing individuals to risk.

5. Using controlled dissemination

This includes restricted-access reports or embargoed press briefings.

While CSOs may have legitimate reasons for wanting to publish their findings—such as building public support or attracting donor attention—this should never come at the expense of operational security or individual safety. Responsible communication strategies must balance the need for transparency with the imperative to protect ongoing investigations and those involved in them.

CSOs should also recognise that allowing law enforcement agencies to take public credit for enforcement actions serves broader strategic objectives. When law enforcement is seen to be taking decisive action against environmental crime, this can raise public awareness of the issue, foster goodwill toward enforcement agencies, and increase political and institutional support for environmental crime units. In the long term, this contributes to stronger enforcement capacity and accountability. Therefore, CSOs are encouraged to delay their own media releases until after an official law enforcement announcement, and to ensure that their messaging publicly acknowledges and praises the role of law enforcement. Media statements should make clear that arrests, seizures, and prosecutions are the result of official action, and that credit belongs to the responsible agency—not the CSO.

Any planned public awareness campaigns, media engagements, or social media disclosures that involve references to law enforcement activity should, wherever possible, be discussed in advance with the relevant law enforcement agency. A timely, targeted, and coordinated communications approach can support operational objectives and public interest. However, premature or uncoordinated disclosures risk undermining months or even years of investigative work.

CONCLUSIONS

Effective responses to environmental crime depend on trusted, two-way collaboration between civil society organisations and law enforcement agencies. These guidelines outline the types of information CSOs may collect, how to assess and share it responsibly, and the operational and legal standards that govern its use by law enforcement.

CSOs can provide critical insights into environmental crime through local access, open-source analysis, and investigative expertise. However, for this information to be useful, it must be accurate, relevant, lawfully obtained, and clearly documented. Law enforcement, in turn, must establish mechanisms to evaluate, act on, and provide feedback regarding information received. This will build trust and improve law enforcement outcomes over time.

Both sectors face risks. CSOs must navigate threats to source safety, legal uncertainty, and potential retaliation; law enforcement must guard against misinformation. These risks can be managed through structured communication, verified partnerships, and mutual accountability.

CSOs should also remain mindful that their role is to support, not replace, law enforcement. Wherever possible, they should empower the competent authorities to take the lead in enforcement actions and criminal proceedings. This includes stepping back once a case has been referred and ensuring that law enforcement has the space and resources to act effectively. Taking a collaborative approach not only respects institutional mandates but also strengthens state ownership, builds long-term enforcement capacity, and reinforces public confidence in the justice system. CSOs that are seen to overstep or dominate enforcement narratives may inadvertently damage their credibility and hinder future cooperation.

It is intended that these guidelines promote mutual understanding between CSOs and law enforcement agencies. For law enforcement, this means gaining deeper insight into the operational challenges CSOs face when collecting and sharing information—particularly the risks to their staff, sources, and community partners. For CSOs, the guidelines offer clarity on how submitted information is handled, what level of feedback can reasonably be expected, and how to enhance the quality and usefulness of the data collected and shared.

Building effective mechanisms for information sharing is a shared responsibility. It requires CSOs to improve the credibility, completeness, and evidentiary value of the information they provide, and law enforcement to demonstrate professionalism in acting on that information.

NOTES

1. INTERPOL presented its Global Threat Assessment of Wildlife Crime, at the INTERPOL Wildlife Crime Working Group meeting in November 2024 at Cape Town, South Africa.

2. See International Fund for Animal Welfare, ‘Digital markets: wildlife trafficking hidden in plain sight’, 2021, available at https://d1jyxxz9imt9yb.cloudfront.net/resource/1000/attachment/original/ifaw-uscybercrimereport-digital-1921.pdf

IMAGE CREDITS

Cover image: Wikimedia Commons. Original image available at:
https://commons.wikimedia.org/wiki/File:Ivory_Seize_Cambodia.jpg.
P4: Pixabay / ibrahimpoonawala553
P6: Pixabay / JacquesTiberi
P8: Rawpixel / USGW
P11: NCA
P13: Flickr / USG
P16: Icons8 / Geran de Klerk
P21: Pexels / Harvey Sapir
P22: Pexels / Pok Rie
P28: Wikimedia Commons / Ibama. Original image available at:
https://commons.wikimedia.org/wiki/File:Terra_Ind%C3%ADgena_Munduruku,_Par%C3%A1_(28160721237).jpg

NATURE CRIME ALLIANCE

people. planet. justice.

naturecrimealliance.org