Revere Action Toolkit

HOW TO HELP BUILD THE REVERE MAP

ABOUT THIS GUIDE

The Revere Map and the other content we publish is a public resource intended to provide situational awareness, and pertinent information, data and analysis on an accurate, reliable, and timely basis for map users. To ensure its usefulness, we rely on several sources of publicly available information and data sources, as well as privately sourced information that is provided and verified by trusted individuals. We invite you to join in these efforts.

This guide covers:

- The data and information we need (types of content, formats, types of information)
- How to provide it to us — in person, or through the contact us page
- Our methods and approach (privacy and anonymity)
- Roles: independently collecting and providing information; receiving and vetting information; verifying the accuracy, reliability and importance of information, data, and claims

USE THE SALUTE METHOD

Use the SALUTE method to report accurate, actionable information that helps protect communities and guide response efforts. This standardized format ensures clarity and reduces fear from unverified claims.

(See: https://www.traverseindivisible.org/resources/see-something-salute)

S — Size	Note the number of individuals, vehicles, or assets observed (e.g., 5 agents, 2 vans).
A — Activity	Describe what they are doing — e.g., conducting a raid, questioning individuals, using force, or searching a building.
L — Location	Provide a precise address, intersection, or landmark (e.g., "123 Main St, near the gas station"). Include boroughs in NYC or specific street names.
U — Unit	Identify the group or affiliation — e.g., ICE, CBP, HSI, or DHS. Note visible patches, insignias, or vehicle markings (e.g., "ICE ERO," "DHS," "CBP Field Operations").
T — Time	Record the exact date and time of the observation (e.g., "June 7, 2025, at 10:15 AM").
E — Equipment	List tools or weapons observed — e.g., flexicuffs, dogs, batons, sound cannons (LRAD), door breachers, or armored vehicles.

Use this method when reporting to local organizations' rapid response networks.

Do not post unverified reports on social media — this can spread panic. If you document the event, record video horizontally, capture officer details (faces, badges, license plates), and only intervene if safe. Always remain calm, know your rights, and avoid signing anything or discussing your immigration status.

DOCUMENTATION BEST PRACTICES: BACK IT UP AND WRITE IT DOWN

- Back up footage immediately to cloud storage before any potential device seizure.
- Write a contemporaneous written account as soon as possible — memory degrades fast.
- Use the 5 W's: Who, What, Where, When, and What was said — verbatim as much as possible.
- Note whether agents identified their agency (ICE, CBP, FBI, etc.) and showed credentials.
- Document any absence of a warrant — agents are required to have a judicial warrant to enter any premises.

Key Red Flags to Document

- Agents refusing to identify their agency.
- Stops with no apparent probable cause (e.g., someone simply walking or shopping).
- Agents questioning or detaining U.S. citizens or people who clearly have documentation.
- Threats or intimidation of observers or bystanders.
- Stops that appear to target people based on appearance in non-border areas.

DATA SOURCES WE NEED FOR REAL-TIME MAPPING

If you have access to and observe any of the following, you can help keep us informed and equipped with the latest.

TIER 1: PUBLICLY AVAILABLE & ACCESSIBLE

Citizen & Community Reporting

- Crowdsourced incident reports (your own app/form — the most scalable real-time source)
- Existing rapid response networks: United We Dream, RAICES, local coalitions
- Social media monitoring: Twitter/X, Nextdoor, Facebook community groups, WhatsApp broadcast channels
- Waze and Google Maps user reports (indirect signal — unusual traffic stops, road activity)

Government & Court Records (Public)

- PACER (federal court filing system) — tracks ICE detention filings, immigration court cases, warrant applications by district
- Federal court dockets — surge in filings in a district signals enforcement surge
- ICE's own published detention/removal statistics (updated periodically, not real-time)
- DHS Office of Inspector General public reports
- CBP checkpoint locations (many are publicly listed)
- FOIA request databases — organizations like MuckRock aggregate previously released ICE operational documents

Flight & Aircraft Tracking

- ADS-B Exchange (adsbexchange.com) — unfiltered aircraft transponder data; ICE and CBP operate surveillance planes and helicopters with known tail numbers
- FlightAware / FlightRadar24 — broader coverage, some federal aircraft visible
- Known ICE Air tail numbers are publicly documented by journalists and researchers
- CBP's fleet includes P-3 Orions, Cessna Citations, and drones — tail numbers are catalogued by watchdog groups

Vehicle & Radio Monitoring

- Broadcastify.com — live police/federal scanner feeds by region
- OpenMHz — archived scanner audio
- Known ICE vehicle descriptions circulate through advocacy networks
- License plate reader (LPR) data — some jurisdictions publish aggregate data; private networks like DRN (Digital Recognition Network) aggregate sightings

TIER 2: SEMI-PUBLIC / OBTAINABLE VIA FOIA OR ADVOCACY NETWORKS

Detention & Transfer Data

- ICE detention facility population data — published with lag, obtainable via FOIA
- Vera Institute's TRAC Immigration (trac.syr.edu) — aggregates ICE enforcement data with geographic detail; publicly accessible but lagged
- ICE 287(g) program participants — list of local law enforcement agencies with ICE agreements is public; their activity is partially reportable
- Detainer requests to county jails — many counties now publish these; others require FOIA

Federal Procurement & Contracts

- USASpending.gov — shows ICE/CBP contract awards including surveillance technology, vehicle fleets, detention contractors, and operational support vendors by region
- SAM.gov — federal contract solicitations can reveal planned operational expansions before they happen
- These can signal where resources are being deployed geographically

Legal & Advocacy Organization Data

- ACLU state affiliates track incidents and share data with partners
- National Immigration Law Center
- Human Rights Watch field reports

– Local legal aid societies — often first to know about detention surges

TIER 3: KNOWN TO LOCAL/STATE GOVERNMENT — NOT ROUTINELY PUBLIC

These sources exist and are accessible to state/local agencies, but require relationships, legal process, or leaks to access:

Law Enforcement Information Sharing Networks

– HIDTA (High Intensity Drug Trafficking Areas) fusion centers — federal/local intelligence sharing hubs; ICE often coordinates through these
– Regional Information Sharing Systems (RISS) — law enforcement-only network
– FBI JTTF (Joint Terrorism Task Force) coordination logs — ICE sometimes embedded
– LEO (Law Enforcement Online) — federal officer-only portal

Jail & Detention Coordination

– County sheriffs with 287(g) agreements receive ICE detainer requests in real time — not public but known to sheriff's offices
– Secure Communities program data — when someone is booked into jail, their fingerprints are run against DHS databases; this triggers ICE notification; local jails know when ICE has been notified
– State corrections departments track federal holds

State DMV & Infrastructure

– Some states share DMV data with DHS under existing agreements — state transportation agencies know this
– Toll and traffic camera systems — some have been accessed by federal agencies; state DOTs have records of access requests

Emergency Services Coordination

– Local 911 dispatch records — federal operations sometimes generate calls; accessible via public records requests with varying lag
– Fire/EMS dispatch — federal facilities and enforcement operations occasionally generate emergency responses
– Local emergency management agencies are sometimes notified of large-scale operations in advance

Notification to "Sanctuary" Jurisdictions

– In cities/counties with sanctuary policies, local police chiefs and city attorneys are sometimes formally notified of federal operations — these communications may be obtainable via state public records laws

TIER 4: SIGNALS & CORRELATIONS (INDIRECT BUT POWERFUL)

These don't directly report activity but correlate strongly with enforcement surges:

Signal	What It Indicates
Surge in immigration court filings (PACER)	Recent arrests in that district

Increase in federal detention bed contracts (USASpending)	Planned operational expansion
ICE Air flight activity to a region	Transfer operations underway
Spike in 211/legal aid calls in a community	Community under active enforcement pressure
School absence spikes in immigrant-dense zip codes	Community has gone into hiding — known enforcement nearby
Decreased ER utilization in immigrant communities	Fear-driven avoidance — known enforcement signal
Rental vacancy spikes in certain zip codes	Displacement following enforcement
Social media language analysis in specific zip codes	Community fear signaling
Unusual hotel/motel bookings near detention facilities	Families gathering near detained relatives

Existing Systems to Study or Build On

System	What It Does
Deportation Machine (The Intercept)	Investigative mapping of ICE operations
TRAC Immigration (Syracuse)	Best public data aggregator for ICE enforcement
Mijente's #NoTechForICE tracker	Vendor/contract mapping
ACLU Mobile Justice	Incident reporting infrastructure
Ushahidi platform	Open-source crisis mapping used globally for exactly this type of work
Rapid Response Network maps	Community-built, city-specific versions exist in LA, Chicago, NYC

GUIDANCE ON BEST PRACTICES AND PERSONAL SAFETY

These important activities sit at the intersection of civic journalism, whistleblowing, and source protection. But your personal safety should come first, and that depends heavily on who you are and what kind of access you have.

FOR EVERYONE — Universal Baseline

1. Digital Security First

- Never use a personal phone, work phone, or work computer to research how to share information
- Use a separate device — ideally a cheap prepaid phone or a public library computer — for anything related to sharing sensitive data
- Use Tor Browser (torproject.org) for researching options anonymously — it routes your traffic through multiple servers and strips identifying information
- Never use your home or work WiFi for any of this — use public WiFi accessed from a location you don't regularly visit, or a prepaid mobile hotspot paid for in cash
- Assume every digital action on work systems is logged — keystrokes, screenshots, file access, print jobs, USB connections

2. Identity Protection

- Never tell anyone — including close friends or family — what you are doing
- Do not discuss this on any platform connected to your real identity
- Do not search for secure communication tools on any device connected to you

CATEGORY A: Private Citizens with Access to Public-Adjacent Sources

For social media monitors, scanner listeners, flight trackers, court watchers — this activity faces the least legal risk, as you are aggregating lawfully public information.

Best Practices

- Contribute through an established organization's reporting portal rather than directly to an individual — this adds legal buffer
- Use a pseudonymous email (ProtonMail or Tutanota, created over Tor, never accessed from personal devices) for all coordination
- If submitting to a map or database, do not include details that could identify you as the observer (e.g., your exact vantage point, unique personal details)
- Understand that metadata — the when, where, and how of your submission — can be as identifying as the content itself

CATEGORY B: Local or State Government Employees

Activities gathering data from 911 dispatchers, DMV staff, county jail employees, city attorneys, emergency management occupy a middle-risk zone — they may have policy protections but also confidentiality obligations.

Legal Grounding First

- Consult a whistleblower attorney before sharing anything — many offer free initial consultations and can advise on whether your disclosure is protected
- Key federal protections: Whistleblower Protection Act, and for state employees, most states have parallel statutes
- Sharing information that reveals illegal federal activity or constitutional violations generally has stronger protection than sharing routine operational data

Operational Security

- Never access, copy, or transmit the information from a work device or work network
- If the information is something you observed or were told verbally, you can relay it from memory on a personal secure device — this is categorically safer than copying files
- If documents are involved, consult your attorney first — physical documents (printed at work on a work printer) carry forensic risk (printer tracking dots, access logs)
- Use Signal (with disappearing messages enabled) on a device not connected to your identity
- Consider reaching out through a news organization's secure tip line rather than directly to a database project — journalists have additional legal protections for their sources

CATEGORY C: Federal Employees or Contractors

Gathering information involving ICE, CBP, DHS, DOJ, or contractors with operational visibility carries the highest risk and the highest value. The calculus here is serious.

Legal Framework

- Federal whistleblower protections exist but are weaker and more complicated for national security and law enforcement agencies
- The Whistleblower Protection Enhancement Act covers many federal employees but has carve-outs for intelligence and some law enforcement

- An attorney specializing in federal whistleblower law is not optional here — it is essential
- Key organizations that can connect you with attorneys at no cost: Government Accountability Project (whistleblower.org); National Whistleblower Center; Whistleblower Aid (whistleblowersaid.org) — specifically set up for federal employees

If You Proceed

- The SecureDrop network (securedrop.org) was built specifically for this — it is used by The New York Times, Washington Post, The Intercept, and dozens of other outlets; it operates over Tor and is designed to strip all metadata
- Never use government systems to identify, research, or contact any outlet or database
- The physical gap matters: there should be zero connection between your work identity/access and any communication about sharing — different device, different network, different location, different identity
- Consider whether the information you have documents illegal conduct specifically — this is the strongest legal and moral ground, and the strongest protection

What to Share vs. Not Share

- Information documenting patterns of illegal targeting, constitutional violations, or abuse of authority — strong public interest basis
- Operational details that could endanger individuals being sought for violent crimes — avoid
- Information that could identify specific undocumented individuals to bad actors — avoid; this could harm the very people you're trying to protect

SECURE COMMUNICATION TOOLS — RANKED BY SECURITY LEVEL

Tool	Best For	Risk Level
SecureDrop	Federal/high-risk leaks to journalists	Lowest — built for this
Signal (disappearing messages)	Ongoing coordination	Very low if device is clean
ProtonMail over Tor	Initial contact	Low
Tutanota	Email to organizations	Low
Standard email (Gmail, etc.)	Anything sensitive	⚠ **Do not use**
Phone call on personal phone	Anything sensitive	⚠ **Do not use**
Text message	Anything sensitive	⚠ **Do not use**

THE JOURNALIST LAYER — WHY IT MATTERS

Routing information through an established news organization rather than directly to a database provides several advantages:

- Journalists have reporter's privilege in most states — they can resist subpoenas for source identity.
- News organizations have legal teams that actively defend source protection.
- Publication creates a public interest record that is harder to suppress.
- Established outlets have security infrastructure (SecureDrop, encrypted intake) already in place.

Relevant outlets with strong source protection infrastructure and demonstrated commitment to this coverage: The Intercept, ProPublica, The Guardian US, Washington Post, New York Times, Documented NY, The Marshall Project.

THE SINGLE MOST IMPORTANT PRINCIPLE: COMPARTMENTALIZATION

The person with access should know as little as possible about you, your project, and your infrastructure. You should know as little as possible about them. The information should travel through the fewest possible hands between origin and use. Every additional person who knows anything is an additional point of failure.

A source who follows all the right security practices can still be exposed by a recipient who doesn't. Your own operational security is just as important as theirs.