

# Intelligence software for the district.

Location requests, published FIRs, vehicles named in those FIRs, and call records the unit has lawfully obtained — on one case, with an audit entry.

📍 Location

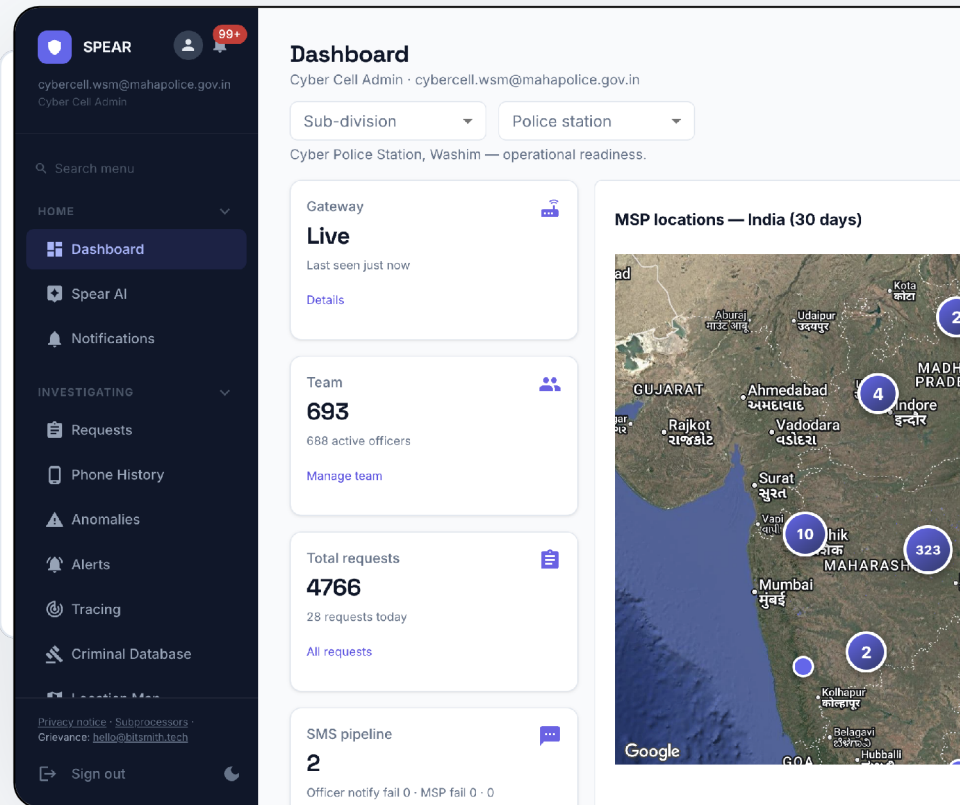
📄 FIR & vehicles

📞 Call records

🚶 Patrol

🕒 Audit

SPEAR · BitSmith Technologies



# From manual operator calls to a recorded, automated location pipeline.

## EXISTING PROCESS

-  Officer sends an SMS to the cyber cell
-  Operator (MSP) is looked up manually
-  Request is routed to the MSP, which replies later
-  Reply is manually forwarded back to the officer

---

 Slower lookups, no reliable audit trail, and no way to confirm the request came from a legitimate investigating officer.

## WITH SPEAR

-  Officer sends the request
-  Spear sends the operator lookup and records the reply automatically
-  The requesting officer receives the reply directly
-  Location is added to the case record with an audit entry

---

 Runs around the clock on authorised, case-linked requests — no manual retyping of operator replies.

# Every operator reply becomes part of the case.



1

## The reply becomes a case.

Map with the nearest police station, a PDF for the case file, and a searchable history for every number. Replies reach the officer by SMS or WhatsApp.



2

## The number can be watched.

Scheduled checks on a number, with an alert when a fix enters a watched district.



3

## A changed handset is flagged.

SIM and device indicators when the SIM or handset under the same number changes. They are indicators, not proof of a swap.

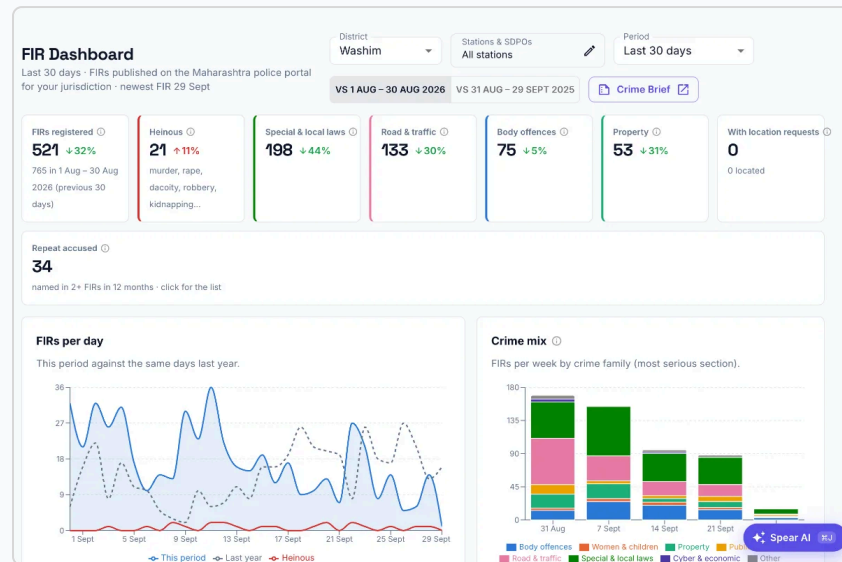


**Spear Assistant.** Officers ask in plain language about the record on screen. Any action, such as starting a trace or opening a case, waits for the officer to press the button. Nothing is sent without approval.

# The FIRs your stations already published, readable by the officers who supervise them.

## WHAT COMMAND SEES

-  FIRs registered in the period, for every station the login covers
-  Crime matrix by type of crime, station by station
-  Heinous offences called out
-  Which FIRs already have a Spear location request, and which do not
-  Names appearing as accused in more than one FIR within twelve months
-  Vehicle registrations appearing in more than one FIR



 These views cover published FIRs for the unit's own jurisdiction. Spear does not replace CCTNS. It places the published register next to the location request.

# One FIR, read into fields the case can use.

## KEPT FROM THE PUBLISHED FIR

# FIR number and police station

Sections

Complainant

Accused

With father's name where the form prints it

Mobile numbers

Vehicles

Registration, and chassis or engine number where printed

## WHAT THE OFFICER CAN DO FROM IT

 **Trace a number printed in the FIR**

Send a location request for the complainant's or accused's mobile.

 **See the accused in other FIRs**

Other FIRs where the same name appears as accused.  
Name-only matches are marked possible.

 **See the vehicle in other FIRs**

Other FIRs where the same registration is printed.

 **Check the numbers everywhere**

Each mobile checked against location traces, criminal records and investigation cases.

# Find cases that happened the same way.

Describe the modus operandi in plain words. Spear finds FIRs that read alike, even when the words differ.

## THE OFFICER TYPES

 Two men on a motorcycle snatch a gold chain from a woman on her morning walk

## SEARCH ACROSS

District

Range

State

## WHAT COMES BACK

-  FIRs with a similar method, ranked by how closely they match
-  Where and when each one was registered
-  Search by any detail in the FIR: what was taken, the place, the time, a vehicle or weapon described
-  Each result opens the full FIR

 A similar method is a lead for the investigating officer. It does not mean the same accused.

# The same vehicle, in more than one FIR.



## Identified from the FIR

Registration number, and chassis or engine number when the FIR prints them.



## Role on each FIR

Stolen, used, or seized, as the FIR form records it.



## Seen again

Other FIRs in the jurisdiction where the same registration appears.



## Duty vehicles left out

Government and police-duty vehicles are excluded from the seen-again list, so a patrol vehicle never shows up as a suspect car.

The screenshot displays the SPEAR interface for a vehicle with registration number **MH 37 A 2472**, identified as an **Auto-rickshaw** (Commercial). It is registered at Washim RTO, Maharashtra. A status badge indicates it was **Used in an offence**.

**Summary Statistics:**

- FIRs: 5
- Police stations: 3
- Stolen: 0
- Recovered / seized: 0
- Used in offence: 3
- Location requests: 0
- First seen: 9 Jan 2020
- Last seen: 22 Sept 2026

**History:**

- 22 Sept 2026** (Mentioned) **FIR**  
 FIR 0613/2026 - Rash driving / hurt in accident  
 Karanja City, Karanja SDPO - Sawakar Chavla Karanja, Karanja  
 A police constable reported that a driver named Wasimuddin Najamuddin Sodagar was driving vehicle MH-37-AB-2472 recklessly and at high speed on a public road in Karanja, creating danger to life and property.  
 Accused: Wasimuddin Najamuddin Sodagar
- 11 Oct 2025** (Used in offence) **FIR**  
 FIR 0498/2025 - Public nuisance / obstruction  
 Karanja Rural, Karanja SDPO - Kheda Fatz Village, Karanja Lad  
 A vehicle was parked in the middle of a public road causing danger to traffic and pedestrians; the driver was questioned by police and identified for an offence under section 285 BNS.  
 Accused: Wasimuddin Naimoodin
- 18 Sept 2025** (Mentioned) **FIR**  
 FIR 0239/2025 - Public nuisance / obstruction  
 Dhanaaj, Karanja SDPO - (N): वाशीम नजामुद्दीन सोदगार  
 Accused: वाशीम नजामुद्दीन सोदगार
- 5 May 2020** (Used in offence) **FIR**  
 FIR 0357/2020 - Disobeying public order  
 Karanja City, Karanja SDPO - (N): वाशीम नजामुद्दीन सोदगार  
 Accused: वाशीम नजामुद्दीन सोदगार

**Possibly the same vehicle:** MH 37 AE 2472 Car 1 FIR

**Seen with these vehicles:** MH 37 AE 2472 Car 1 FIR

**People in these FIRs:**

- वासिम नजामुद्दीन सोदगार
- वासिम नजामुद्दीन सोदगार
- वासिम नजामुद्दीन सोदगार
- Wasimuddin Naimoodin
- Wasimuddin Najamuddin Sodagar

**Police stations:**

- Dhanaaj 2 FIRs
- Karanja City 2 FIRs
- Karanja Rural 1 FIR

**Sources for this vehicle:** [Spear AI](#) [QR](#)



**A repeated plate is a lead for the investigating officer. It is not a finding that the vehicle was used in both offences.**

Vehicle details come from the FIR text only. Spear does not look up RC owners or Vahan records.

## The CDR the operator already sent, read inside the case — not in a separate desktop tool.

### EXISTING PROCESS

-  Excel and a separate CDR desktop tool
-  One file, one number at a time
-  Every operator sends a different layout
-  No link back to the FIR

### WITH SPEAR

-  An investigation case inside Spear
-  Several target numbers on one case
-  Layout recognised; the officer confirms the columns
-  Each number checked against FIRs, location traces, criminal records, and other cases

 **Stored records only.** This is the CDR the unit lawfully obtained from the operator. Spear does not intercept calls.

# How a call-record file gets into a case.

The upload is locked until the case carries a legal order.



STEP 1

## Open the case

FIR or case reference, investigating team, target numbers, and a retention date.



STEP 2

## Record the legal order

Court or SP order reference under BNSS §94. Without it, upload stays blocked. The reference is printed on every report.



STEP 3

## Upload the operator file

Vi, Jio, Airtel and BSNL layouts are recognised, including Vi's subscriber block. Unknown layouts are read from the header and the values.



STEP 4

## Confirm the columns

The officer confirms which columns hold mobile, IMEI, IMSI, date and cell ID. The confirmed layout is reused next time.



The original file stays on the unit's Spear host. It is never a public upload.

## Six views of one file, each answering one question.



### Contacts

Who this number called or messaged, and how often.



### Places

Towers used most, by night and by day. Home and work are estimates from towers, not addresses.



### Devices

Handsets (IMEI) and SIMs (IMSI) used with this number.



### Time

The usual day, late nights, silent gaps, and bursts of new contacts.



### Footprint

Banks, lenders, wallets and apps that sent SMS to the number, so the officer knows which records to request next.



### Links

Numbers shared by two targets, one handset on two SIMs, and two targets on the same tower within 30 minutes.



**Every flag opens the rows behind it:** silence, several handsets, call forwarding, roaming, and a call received and passed on within five minutes, seen at least three times.

❗ Same tower within 30 minutes means both were near that tower. It does not prove they met.

❗ For a Wi-Fi call the file shows a public IP. The internet provider can be asked for that subscriber.

## The same number should not be investigated three times in three windows.

WHEN ONE OF THESE APPEARS

**Mobile number**

**IMEI**

**IMSI**

Spear shows where the district has already seen it.

ALREADY SEEN



Named in a published FIR



Traced on a location request



On a criminal record



Under a scheduled trace



A target in another investigation case in the district



### **Name-only matches stay “possible”**

Records are never merged into one identity on a name alone.



### **No cross-district links**

Links stay inside the district until a data-sharing arrangement exists.

# Every rank gets its own dashboard.

Role-based access, set up to match your district hierarchy.



SUPER ADMIN

## Cyber Police Station

Complete system access and control.



READ-ONLY

## SP & Additional SP

Dedicated login to monitor all activity across the jurisdiction.



SUB-DIVISION

## SDPO

Supervision of every police station in the sub-division.



STATION

## Station In-Charge

Location request history and all active officers under their command.



**Hierarchy setup:** create sub-divisions, then attach police stations under them.

# Digital proof of officer presence during patrols.



## Simple Mode

Ready for station pilot

The station in-charge pins real places on the map or puts QR codes on the wall. On arrival, the officer scans the QR or takes an in-radius selfie.



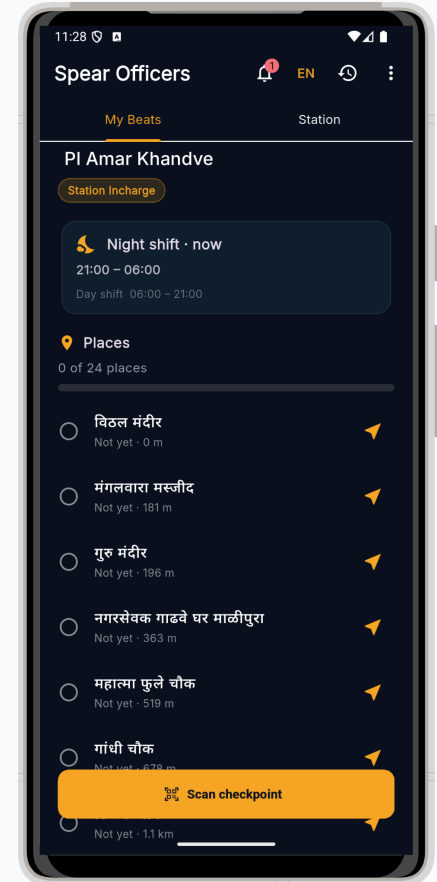
## Custom Beats

For structured jurisdictions

Named routes and dated duty rosters. Map custom beats for the jurisdiction and schedule beat duties.



Role-based access for the Station In-Charge, Beat Marshals, SDPO, and SP.



# The check-in path

Four steps from arrival to a verified attendance record.



STEP 1

## Scan

Officer scans the QR code at the location, or opens the app within range of it.



STEP 2

## Selfie

An in-radius selfie confirms physical presence.



STEP 3

## Submit

Attendance is recorded and synced with the command center.



STEP 4

## Verify

The station in-charge reviews check-ins and can reject a selfie; the officer is notified.

## Built for lawful operator enquiries under BNSS, DPDP data roles, and CERT-In operational duties.



### BNSS §94 — stored records

The unit's written authority travels with every request to the telecom nodal officer. Spear is the recorded pipeline. It does not create a new police power.



### Not interception

Spear does not tap calls or messages. Telecom Act §20 (intercept) is out of scope. Location enquiries go to the operator on the unit's written authority.



### DPDP Act 2023

Bitsmith is Data Processor for case and location data, and Data Fiduciary for officer accounts. A DPA is signed for every new unit.



### Data Security

India hosting (AWS Mumbai), encryption in transit, private evidence storage, incident process operated in line with CERT-In Directions. Not CERT-In certified — no such product certificate exists.

## Where the data comes from, who can see it, and when it is deleted.

### Where do FIRs come from?

Published FIRs. Dashboards cover the unit's own jurisdiction; similar-case search can look across the range and the state.

### Where do CDRs come from?

The file the operator gave the unit. Upload is blocked until the legal order reference is on the case.

### Are patterns proof?

No. Silence, meetings, home towers and repeat plates are leads, shown with the rows they come from.

### Who sees a case?

The case team, their supervisors in the same jurisdiction, and admins. Every open, upload and export is recorded in the activity log.

### When is call-record data deleted?

When the case retention date passes, the call-record rows and the uploaded file are deleted. The case can still show that a CDR existed.

# Three deployment options

Cloud-first deployment, transparent annual licensing, and enterprise support. On-premises on request.



DEFAULT

## 1. BitSmith Cloud

Built for continuous district operations on BitSmith India Cloud (AWS Mumbai). Requires a PO and a cyber-cell gateway phone.



## 2. Your Cloud

The cyber police or district provides its cloud project and Spear is installed there. Requires cloud account access for installation.



ON REQUEST

## 3. On-Premises

Servers inside your building when the unit requires it. Needs 24/7 power and network. Scoped and scheduled after PO — not the default path.

↔ **Moving later?** Cloud → on-premises is supported on request. Timeline and scope are agreed after PO.

# Frequently asked questions



## Can Spear tap a phone?

No. Location replies and CDRs are stored records the unit requests from the operator. Live interception is out of scope.



## Does a repeated vehicle mean the same accused?

No. It means the registration is printed on more than one FIR in the jurisdiction. Government and police-duty vehicles are excluded.



## Can Spear identify the owner of a Wi-Fi connection?

No. When a Wi-Fi call shows a public IP instead of a tower, the officer can ask the internet provider for that subscriber.



## Can we upload a CDR received on WhatsApp?

Only after the case carries the legal order reference. Until then, upload stays blocked.



## Will another district see our FIRs or CDRs?

No. Your cases, call records and links stay inside your jurisdiction. Cross-district links are off.



## Does Spear replace CCTNS?

No. It reads the FIRs your stations already published and shows them next to the location request.

# Frequently asked questions



## Can one officer SMS list several mobile numbers?

Yes. Spear reads the numbers in the investigating officer's SMS and schedules a request for each.



## What if the cyber cell's phone is dual-SIM?

Set a SIM for each MSP and the Spear Gateway app routes each request to the right one.



## Does the data stay in India?

Yes. Hosted in AWS Mumbai (ap-south-1). Architected so case and location data stay in India.



## Can officers check in from home or another location?

No. Check-ins outside the required radius (default 20 m) are rejected and logged for the station in-charge.



## Can a mock-location app fake a check-in?

No. The app detects mock-location and developer tools, so officers must be at the real location.



## Who can access the data?

Case data is for your provisioned logins. BitSmith has no standing access; any break-glass support access is logged.

 [SCHEDULE A LIVE DEMO](#)

# See Spear on your own authority model: location requests, the FIR register, call records, and the audit trail.



PHONE

**+91 7744953400**



EMAIL

**hello@bitsmith.tech**



WEBSITE

**<https://bitsmith.tech>**

 Training at installation, video-conference sessions for field staff, and ongoing technical support.

# Thank you.

Partnering with law enforcement to build safer, data-empowered communities.

## CORPORATE HEADQUARTERS

### **Bitsmith Technologies Private Limited**

18A Ujjwal Nagar 2, Darwaha Road, Yavatmal, Maharashtra

+91 7744953400 · hello@bitsmith.tech

## REGISTRATION

GSTIN

**27AAJCB1429N1ZE**

CIN

**U80904MH2020PTC342801**

Startup India (DIPP)

**DIPP88374**