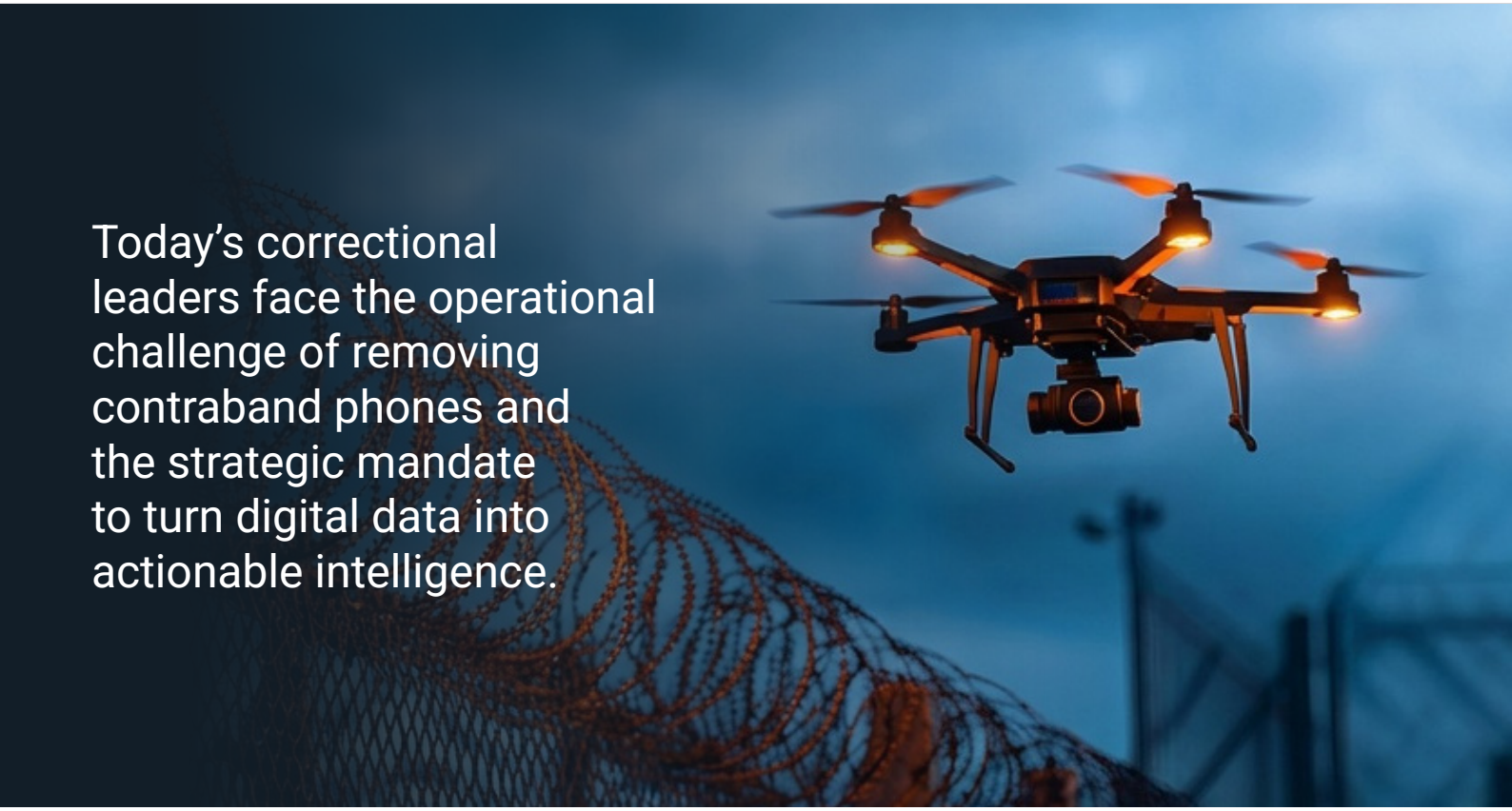
Cellebrite

WHITEPAPER

5 Best Practices

for Investigating Contraband Phones and Drones in Jail



Today's correctional leaders face the operational challenge of removing contraband phones and the strategic mandate to turn digital data into actionable intelligence.

Overview

Contraband phones and drones are two of the most urgent and escalating threats facing jails and correctional facilities today. Phones give inmates the ability to coordinate organized crime, intimidate witnesses, traffic narcotics and orchestrate violence from behind bars. Drones have made the problem worse—jails are now inundated with contraband of all kinds delivered over the walls, from drugs and weapons to devices that land and disappear before officers can respond. Despite intensive interdiction efforts these threats continue to grow, fueling hidden criminal networks that erode staff safety, undermine public trust and strain investigative resources.

Today's correctional leaders face the operational challenge of removing contraband phones and the strategic mandate to turn digital data into actionable intelligence. By adopting modern digital investigation practices, correctional agencies can expose hidden behaviors, disrupt criminal networks and dramatically improve safety outcomes for staff, inmates and surrounding communities.

Below are five modern best practices—including dedicated drone forensics guidance—to transform the contraband crisis into an opportunity for stronger security, faster and intelligence and measurable impact.

TIP #1

Establish a Clear Contraband Phone Strategy Rooted in Intelligence Not Just Interdiction

Most facilities still approach contraband phones reactively, confiscating devices without a consistent data driven strategy. But modern correctional threats demand a proactive intelligence posture.

A strong contraband strategy begins with clear goals and outcomes such as:

- Reducing violent incidents and staff assaults
- Dismantling inmate run criminal networks
- Speeding investigative response times
- Strengthening transparency and public trust

Leaders should define how digital evidence will be collected, reviewed, secured and shared, establishing standards that reinforce chain of custody and ensure defensible auditable evidence handling.

Why it matters:

Public safety leaders and wardens must demonstrate measurable improvements in community protection and institutional security. A well defined strategy shows stakeholders from legislators to prosecutors that the facility is operating with accountability, transparency and modern investigative rigor.

TIP #2

Put Seized Device Data to Work to Accelerate Intelligence & Disrupt Networks

Historically, many facilities seized contraband phones but lacked the capacity to extract and analyze the digital evidence inside them. This leads to lost intelligence, missing opportunities to uncover threats, prevents violence or exposes connections beyond the prison walls.

Modern digital intelligence solutions like Cellebrite Inseyets and Pathfinder allow agencies to:

- Access, extract and decode data from sanctioned or contraband inmate devices
- Surface hidden connections between inmates, external associates, gangs and criminal networks
- Analyze encrypted, deleted or fragmented data
- Detect high risk patterns such as extortion, trafficking, contraband, smuggling and coordinated violence
- Quickly triage large volumes of messages, images, locations and media

Forensic examiners and gang investigators gain immediate insight into communications that previously sat dormant. Investigators, wardens and public safety leaders get faster time to evidence, enabling earlier interventions that prevent escalation.

Outcome impact:

Facilities using these approaches have reported 5× faster case resolution, reduced backlogs and strengthened legal outcomes through clearer, defensible digital evidence.

TIP #3

Act Fast on Recovered Drones - Trace Operators Before the Trail Goes Cold

Drones are now a primary delivery mechanism for contraband at jails -- and they present a forensic challenge unlike phones or any other seized device. In jail environments, contraband drones often disappear quickly after an incident, leaving little opportunity for follow-up. Investigators need to quickly trace drones back to their operators before evidence is lost, or another delivery occurs. Traditional digital forensic tools were not designed for this reality.

UAV data extraction has become significantly more challenging in recent years as manufacturers have hardened device protections. Corrections officers require a fast, on-site method to extract flight logs, operator identifiers and device pairings from recovered drones -- before the window to apprehend a suspect closes. Cellebrite Inseyets.CFID is purpose-built for exactly this: enabling agencies to extract and analyze data from UAVs quickly, without waiting on external labs that can cost investigations days or weeks.

Correctional agencies should prioritize drone forensics capability when:

- A drone is recovered at or near the facility
- A spike in contraband deliveries over jail walls is detected
- Leadership recognizes that waiting on external labs costs investigations days or weeks

Why it matters:

Drone-delivered contraband is a time-sensitive threat. Every hour after a drone is recovered is an hour the operator has to disappear. Agencies with on-site UAV forensic capability can identify operators, interrupt supply networks and prevent the next delivery -- rather than sending evidence to a lab and waiting while the investigation stalls.

TIP #4

Break Down Information Silos and Enable Secure Real-Time Collaboration

Contraband phone intelligence often becomes trapped in isolated systems, slowing investigations, delaying decisions and weakening coordination with prosecutors or outside agencies.

A modern approach requires centralized secure evidence collaboration, ensuring stakeholders can access relevant insights in real time.

Solutions like Guardian enable:

- A single secure workspace for evidence review
- Controlled access and full audit logs to protect chain of custody
- Rapid sharing with prosecutors, partner agencies and internal teams
- AI-powered summarization of lengthy chats and complex data
- Cross case analysis that exposes multi-facility or multi-agency patterns

For correctional environments where multiple agencies may touch a single case, this level of visibility is critical. It ensures defensible evidence handling, strengthens interagency coordination and eliminates manual risky sharing methods such as USBs or DVDs.

Why it matters:

Public safety leaders gain transparency, prosecutors make charging decisions faster and examiners spend far less time on manual admin allowing them to focus on mission-critical analysis.

TIP #5

Partner Strategically with Outside Agencies to Dismantle Criminal Operations

The criminal activity enabled by contraband phones almost always extends beyond prison walls into narcotics trafficking fraud schemes, weapons distribution, human trafficking and violent gang coordination.

Correctional agencies must treat contraband phones as security violations and as windows into broader criminal ecosystems.

By partnering with local law enforcement, state partners, federal agencies and community stakeholders, correctional facilities can:

- Share intelligence that helps dismantle external networks
- Build stronger cases based on combined digital, physical and field insights
- Improve community safety and strengthen public trust
- Demonstrate measurable impact beyond facility boundaries

Solutions like Inseyets, Pathfinder and Guardian support cross jurisdiction investigations ensuring safe, compliant and defensible sharing of digital intelligence.

The result:

Faster case closures, stronger prosecutions, reduced recidivism and a more unified ecosystem for public safety, all while decreasing the operational burden on correctional staff.

A More Secure Future Inside and Outside Facility Walls

Contraband phones and drones will continue to evolve -- and so must the strategies correctional agencies use to combat them. By shifting from reactive confiscation to proactive digital intelligence that encompasses both phone and UAV forensics, facilities can transform a growing contraband crisis into a strategic advantage.

Modernizing with a unified digital investigation approach allows agencies to:

- Uncover hidden behaviors and networks
- Accelerate investigations and improve case outcomes
- Strengthen institutional safety
- Build community trust through transparency and measurable results
- Preserve chain of custody while collaborating securely

Correctional facilities that adopt these best practices are better equipped to protect their staff, inmates and surrounding communities and to stay ahead of the criminal networks using contraband phones and drones to do harm.

REQUEST A DEMO →

About Cellebrite

Cellebrite's (Nasdaq: CLBT) mission is to enable its customers to protect and save lives, accelerate justice and preserve privacy in communities around the world. We are a global leader in Digital Investigative solutions for the public and private sectors, empowering organizations in mastering the complexities of legally sanctioned digital investigations by streamlining intelligence and investigative processes. Trusted by thousands of leading agencies and companies worldwide, Cellebrite's Digital Investigative platform and solutions transform how customers collect, review, analyze and manage data in legally sanctioned investigations.

LEARN MORE:

WWW.CELLEBRITE.COM | WWW.CELLEBRITE.COM/EN/BLOG | WWW.CELLEBRITE.COM/EN/NEWSROOM