Bastille

EXECUTIVE SOLUTION BRIEF

# Corrections

# Corrections Challenges

For most of us, a cell phone is a lifeline to the worldsomething we can't do without. However, a cell phone is more than a convenient gadget in a corrections facility—it can be a dangerous weapon.

Contraband cellular phones have long been a security and public safety concern for correctional facilities worldwide, and successfully detecting, locating, and confiscating them before they do damage is one of the biggest challenges these facilities face.

While other types of contraband create issues inside the prison, the damage that an inmate can do with a cell phone can extend far beyond prison walls. Reported cases of contraband cell phone use include:

- A Texas death row inmate used a contraband phone to threaten a state senator and his family.
- An inmate escaped from a Kansas prison with the aid of a cell phone smuggled in by an accomplice.
- A South Carolina prison official was ambushed and assaulted at his home in an attack coordinated from the inside using a cell phone.
- Inmates extorted an Alabama family by threatening to harm an incarcerated relative
- Prison officials even caught Charles Manson communicating to his followers with a contraband cellphone when he was still alive.

# Nature and Scope of the Threat

The scale of the problem is staggering. Large state systems can confiscate 10,000-15,000 contraband phones every year. Cell phones have become the most popular contraband item in correctional facilities, ahead of drugs and tobacco.

One purpose of incarceration is to remove people from the environment that led to their criminal actions. A cell phone allows inmates to maintain their prior connections and reduces the effectiveness of behavior corrections and programs.

Using a cell phone bypasses the in-house telephone system, evading call monitoring and recording systems and reducing the revenue generated by inmates using the in-house pay phone.

The problem goes beyond cellular, as inmates may illicitly use today's smartphone Wi-Fi and Bluetooth capabilities to establish or maintain connections outside the corrections facility.

# Creative Smuggling

With nothing but time on their hands, methods of smuggling phones into a facility are varied and creative. Visitors can sneak them in, or drones can fly and drop them in. Trained cats and carrier pigeons have been used to deliver phones, and with inmates willing to pay well over $1000 per phone, there have been many corruption cases of Corrections staff and officers.

# Issues Faced By The Corrections Industry

Corrections departments face limited or shrinking budgets and need more staff, especially in recruiting and retaining corrections officers. These issues drive the need to make optimal use of all available resources, especially personnel resources. Finding ways to increase monitoring and protection with less staffing is the standard budget model for today's prison facilities.

# Previous Efforts to Mitigate the Problem

Several types of mitigation to the cellphone problem have been deployed over the years, with little success, based on the persistence of the problem.
Pat downs and using wands at entry points are spot checks, are labor intensive, and may miss devices that are deactivated or turned off. California DCR estimated that continuous wanding of all inmates would cost $20M in personnel costs yearly at their facilities.

Cellular phone blockers or jammers are discouraged by the FCC and can cause unwanted blocking of resources needed by facility staff. Additionally, managed access systems are costly to install, operate, and maintain and may miss Bluetooth and Wi-Fi communications. Random cellular device sweeps can be hit or miss, cause disruption in the housing unit, are resource intensive, require multiple officers, and consistently increase the risk of violence among inmate populations.

None of the approaches above is adequate, integrates with existing security and video management systems, or provides an audit trail of RF activity.

## A Systems Approach is Needed

Corrections facilities need a proper systems approach that can monitor spaces for Cellular, Wi-Fi, and Bluetooth activity 24/7, alert when activity is detected, direct officers to the location of the activity, and integrate with existing security systems and policies.

## Intelligent Wireless Airspace Defense

Corrections facilities require an improved approach to wireless airspace defense to detect these threats and enable a modern security policy. This refined approach is:

- Intelligent
- Comprehensive
- Integrated
- Future Focused

Bastille Networks makes this refined approach available.

## Bastille Solution

Bastille provides intelligent, comprehensive, continuous cellular phone monitoring within corrections facilities. The Bastille solution combines Sensor Arrays deployed throughout your facility, Concentrators to aggregate and process sensor data, and the Fusion Center platform, which analyzes and augments the wireless data and enables integrations with your existing security systems. This tiered architecture allows the Bastille solution to scale from monitoring a single common room to many Corrections locations with a single management interface.

## Sensors

Bastille achieves comprehensive monitoring by deploying its sensor arrays throughout the monitored facility. Bastille sensor arrays detect wireless emitter activity from 25 MHz to 6 GHz, and Bastille decodes, processes, and sends this RF metadata traffic to the Concentrator for further event correlation. The sensor arrays are 100% passive, which means they never transmit, are plenum-rated, are available for indoor and outdoor use, and are manufactured in the United States. The sensors capture all available attributes of the wireless devices, including dozens of identifiers such as vendor name, Bluetooth network definitions, Wi-Fi device characteristics, and Cellular network information

Bastille's Sensor Arrays use Software-Defined Radio (SDR) technology, which allows them to receive in-place upgrades and ensures future protocol support and decoding.

Bastille's Sensor Arrays are nondescript and can be concealed above false ceilings or left in the open and labeled with harmless designations to reduce suspicion or inspection.

**Figure 1:** Sensor Array

# Concentrator

The Bastille Concentrator receives data from a facility's sensor arrays, refines and consolidates the data into events, and sends them to the Fusion Center. The Premium Concentrator gathers additional data from cellular device transmissions.

# Fusion Center

Bastille's Fusion Center platform is the only NIAP-certified product in this market and provides additional assurances on the quality and security of the Bastille solution. Fusion Center receives wireless data from the Concentrator(s), compiles and analyzes the data, and displays all data on current and historical wireless device activity. The Fusion Center overlays any detected wireless device clearly on your facility floor plan, including the current device location to within 3m accuracy and a playback capability to show the historical position of each wireless device as it moves through your space. This playback functionality allows correlation with other systems to determine who brought the device in and when and where they traveled within the facility.

Bastille's Fusion Center automatically detects known wireless threats from its curated database of threats discovered by Bastille's Threat Research team and industry-disclosed vulnerabilities. The Fusion Center platform offers highly customizable reports, provides rich API capabilities for integration with SIEM/SOAR systems, and is fully maintained and supported by Bastille along with the sensor arrays for the life of the subscription.

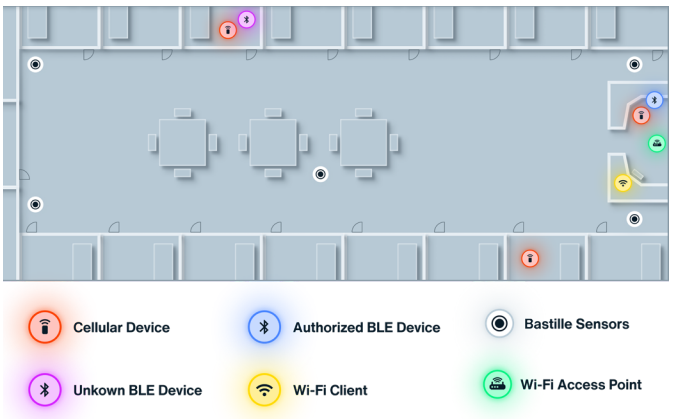


**Figure 2:** Device Location plotted on your floor plan

# Bastille's Differentiation

Bastille has 30 patents in the wireless detection space and maintains a significant advantage in detecting wireless threats.

**EXAMPLE**

## Individual Cellular Device Detection

Bastille can uniquely provide precise location information on cellular phones in your facility and differentiate individual devices—much more than a heat map. With Bastille's technology, you can track each cellular device's location, carrier, and specific attributes as it moves through the monitored facility while adhering to data privacy concerns. Bastille's device history shows you exactly when and where the device entered the facility and every place it's been within the monitored space.

**EXAMPLE**

## Threat Signatures & Event Intelligence

Bastille's Threat Signatures filter through all detected devices and categorize them so you can focus your resources on critical threats. Bastille's solution brings wireless data to your security policy, enabling you to evolve your policy to match the reality of your environment.

Bastille's comprehensive categorization capabilities allow you to rapidly detect new devices and assess their threat posture while maintaining visibility to approved devices used by your personnel.

EXAMPLE

# Advanced Bluetooth Device Detection

Bastille's unique approach simultaneously monitors all 79 Bluetooth and 40 Bluetooth Low Energy channels. This approach identifies Bluetooth-paired devices, explicitly noting the paired network endpoints, attributes of both ends of the pairing, and Bluetooth devices performing inquiries or scans. Other vendors only show when Bluetooth devices are looking to pair; after they've paired, they become invisible. After a device has paired, it can exfiltrate data and cause disruption; you need this visibility to protect against Bluetooth surveillance threats.

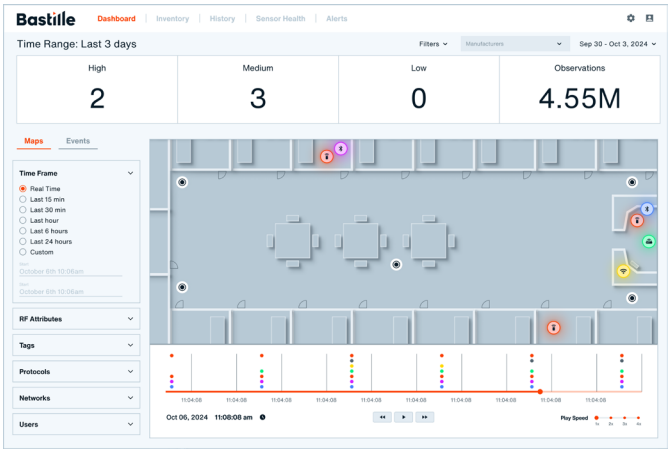


**Figure 3:** Bastille Fusion center

Bastille

## About us

Bastille specializes in providing security solutions for wireless environments. Bastille uses a network of Software-Defined Radios (SDRs) to continuously monitor a facility's entire wireless environment, including cellular, Bluetooth Classic, Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, and other protocols. Our sensors detect, analyze, and localize transmissions in real time, providing a comprehensive view of wireless activity.

Bastille's system goes beyond just identifying signals; it analyzes data to uncover real-time and long-term threats. By capturing the entire wireless spectrum, Bastille offers unparalleled visibility into potential security risks, empowering organizations to proactively safeguard their wireless infrastructure.

## Learn more

To find out how Bastille can detect cellular phones in your Corrections facility, visit us at [bastille.net](bastille.net)