**Bastille Networks**

*Discover, Analyze, Act*

Bastille detects and locates unauthorized Cellular, Bluetooth, Bluetooth Low Energy, Wi-Fi and IoT devices to produce a dots-on-the-map floor plan of your facility, with geofencing, hotspot detection, integrations include Aruba, Cisco, and others, plus DVR forensics.

For more information, visit [www.bastille.net](http://www.bastille.net/) and follow us on Twitter [@bastillenet](https://twitter.com/bastillenet) and [LinkedIn](https://www.linkedin.com/company/bastille-networks).

**Key Contacts & Contracts (if applicable):**

**Company Overview**

* Vendor was founded in 2014
* Startup funding from DHS has been expanded through Phase 5 (commercialization)
* Rich customer base (commercial and Government)
* Government customers include: DHS, USAF, JSOC, NGA, ODNI, NSA and others

**Brief Summary:**

## CELLULAR, BLUETOOTH, BLE & WI-FI INTRUSION DETECTION

Bastille’s real-time Cellular, Bluetooth, BLE and Wi-Fi detection and location system locates all authorized and unauthorized devices within a campus or forward deployed location, accurately places dots on a floor-plan map for device location and sends alerts when a device is found where it should not be or doing what it should not do.

**Deploy and GEOFENCE (in/out) for SCIF and Open Secret Environments:** Bastille is **100% passive** and can be deployed where no transmitters are permitted. Bastille can set geo-fences to include or exclude areas where devices are/not allowed and send real-time alerts when devices are located and/or policies are violated.

**Authorized vs Unauthorized Devices:** Commands want to permit only certain authorized devices in SCIF/Open Secret areas, and Bastille makes this possible. Bastille takes feeds from any other system e.g. Aruba where a device has been authorized, and/or gives the ability to tag specific devices as authorized for a given location and/or time.

**Device Pairing Red Alerts:** Bastille detects and Red Alerts if device pairing ever happens e.g. a Garmin Fenix pairs with a phone in a locker or car outside the Open Secret area.