FUSION CENTERS

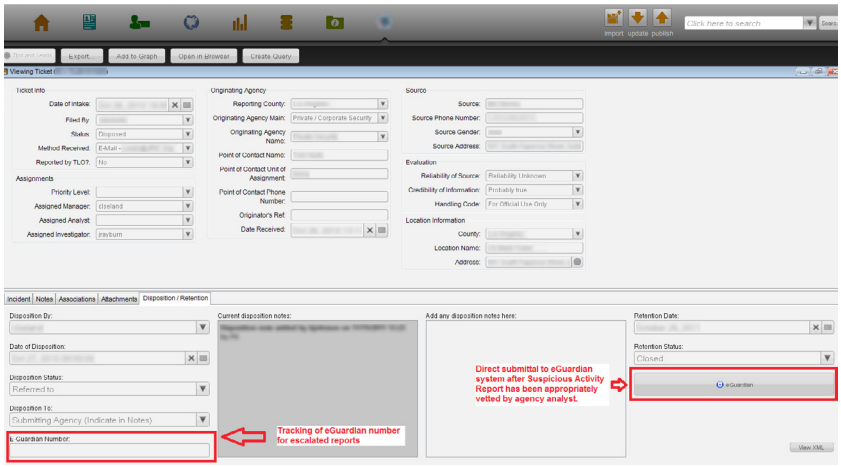
Fusion Centers are staffed by representatives of federal, state, tribal, and local organizations and are situated at the nexus of information systems associated with each of the contributing agencies. Created after the tragic events of September 11, 2001 to address the challenge of multijurisdictional data sharing and collaboration for counter-terrorism analysis, many Fusion Centers have gradually shifted to a broader mission of providing general criminal intelligence and all-crimes, all-hazards analysis support for constituent agencies. With their complicated organizational structures, Fusion Centers and the information management systems they employ face significant data integration challenges. Equally important, they must also satisfy a number of privacy and civil liberties legal and regulatory compliance requirements in order to ensure proper, responsible handling of sensitive data.

The Palantir Platform can be used to address the complexities of the fusion center data sharing environment. State, local, and federal laws and regulations (e.g., 28 CFR Part 23) are often cited in Fusion Center privacy policies as prevailing guidelines for Fusion Centers' intelligence system requirements, but such guidelines have failed, in many cases, to keep up with advances in information management and analysis technologies such as Palantir. To assist Fusion Centers in complying with these requirements while adapting them to the Palantir Platform's unique capabilities, we have invested significant resources in researching requirements and adapting capabilities to address the unique regulatory and privacy protection challenges faced by Fusion Centers.

Working closely with our fusion center clients, their policy and legal staffs, privacy and civil liberties advocates, and our own advisors, Palantir has tailored the platform's capabilities to empower Fusion Centers to better satisfy regulatory requirements and protect privacy and civil liberties, including by:

- Enforcing granular access controls and data discovery principles to ensure that access to contributing agencies' information sources adhere to need-to-know and right-to-know protocols;
- Rigorously controlling the development and sharing of analytic/intelligence work products;
- Implementing purpose specification and case number entry requirements for certain types of sensitive data querying to ensure that predicate-based search standards protect legitimate use of data;
- Generating verbose audit logs that can be analyzed in Palantir's own graphical user interface, greatly facilitating supervisory oversight of information and intelligence usage.

Additionally, Palantir's Workflow application provides a fully-integrated entry, vetting, supervisory review, and submittal tool for controlling new data inputs such as anonymous tips or Suspicious Activity Reports. As with other Platform components, the Workflow application incorporates rigorous access controls, real-time and immutable auditing, and other privacy and civil liberties protective capabilities. Particularly given the unsubstantiated nature of such information, the Workflow application can enable the oversight necessary to ensure that only appropriate information is shared within the system and that retention and purging guidelines, intended to protect the privacy and civil liberties of citizens implicated in such tips and reports, are strictly observed.



Palantir's Workflow application seamlessly enables analyst and supervisory tracking, review, and ultimately submittal of Suspicious Activity Reports to national ISE and eGuardian portals.