EXHIBIT 2

Public Safety Data Integration
Peregrine Technologies

City of Antioch Police Department
Dated: October 01, 2020

Prepared for:

Antioch Police Department
ATTN: Chief Tammany Brooks,
Lieutenant John Fortner
300 L Street.
Antioch, CA 94509
(925) 779-6942

Prepared by:

Peregrine Technologies, Inc.
Nick Noone, Co-founder & CEO
130 Bush St.
San Francisco, CA 94104
(650) 619-0046
nick@peregrine.io

Contents

Dear Chief Brooks,

We are pleased to present Peregrine for your review and consideration.

I would like to thank you for taking the time to meet with Peregrine. We appreciate the opportunity to learn about your operations and discuss your needs. Please find enclosed our Proposal for the Peregrine Platform including software, data integration, and professional services for implementation.

Please feel free to contact me with any questions at (650) 619-0046 or nick@peregrine.io.

Once again, I would like to thank you and the Antioch Police Department for your time and consideration.

Respectfully,
Nick Noone
CEO

Proposal Overview

The following document details the proposed software agreement between Peregrine Technologies, Inc. ("Peregrine") and Antioch Police Department ("APD").

Peregrine will provide its platform to APD to access, integrate, and analyze information across the department. This proposal includes an annual software license to operate Peregrine which includes data integration, project support, user onboarding & training, ongoing support, and data storage. Under this proposal, Peregrine will provide:

- **Annual License to Peregrine Platform**
    - Use cases & capabilities as detailed on pages 8 – 10
    - Includes: Unlimited users, unlimited search, unlimited sharing within and outside APD, unlimited data imports, unlimited investigations, and unlimited storage of media
- **Data Integration**
    - Data integrations as detailed on page 11
- **Project Support**
    - User group onboarding and training with a focus on use cases enumerated on pages 8 - 10
    - Electronic filing workflow development and support
    - Interagency sharing workflow development and support
    - Other workflow development as agreed on with project team
- **User Onboarding & Training**
    - Peregrine will provide secure login credentials & onboarding to all new users of the Peregrine Platform
    - Training: Peregrine will provide training on-site at APD as well as refresher sessions and desk sides
- **Ongoing Support**
    - Peregrine will provide on-site support as needed and mutually agreed by the Project Sponsors as detailed on page 14
    - Peregrine will provide remote technical & analytic support with service levels as detailed on page 15
- **Data Storage & Retention**
    - Peregrine has designed all data handling, storage, & retention policies in full compliance with California DOJ CJIS requirements.

About Peregrine Technologies

Peregrine is a web based CJIS compliant Platform-as-a-Service (PaaS) that provides a single point of access to view and analyze large-scale real-time data from various data sources. The software performs several critical functionalities, including data integration, search and information retrieval, advanced analytics, data management, reporting, collaboration, access control, and security.

Peregrine was developed to provide a common operations and intelligence picture to facilitate real-time operational decision-making, enhance investigatory capabilities, streamline criminal analysis, and generate intelligence products for Law Enforcement. The software creates an extremely efficient method for turning large amounts of raw data into useful decision-support and analysis products, quickly and with significant reduction in manual manpower processing needs. Peregrine will be made available to any and all law enforcement personnel within Antioch, through the Antioch Police Department.

Peregrine was designed for complete system interoperability and supports existing record management systems (RMS), computer aided dispatch systems (CAD), video management systems (VMS), body worn camera (BWC) systems, automated license plate reader (ALPR) data, real-time sensor data, case management systems, evidence management systems, arrest records, subpoenaed data, gang intelligence data, suspicious activity reports, cell and social media data from Search Warrants, and unstructured data such as document, imagery, and video repositories. Peregrine delivers:

- Technology to integrate and secure data of any type or scale

- Intuitive methods for people to search and access all data from one place

- Applications that empower entire agencies to answer complex questions

- A platform for teams to securely collaborate on operations, investigations, and projects

Company Background

Peregrine Technologies, Inc. is a California-based software engineering company founded in 2017, financed by leading Silicon Valley investors, and dedicated to supporting Law Enforcement agencies on their most complex and critical challenges. Our organization is led by Stanford-educated computer scientists who have created and deployed software for some of the most important and security-conscious government and commercial institutions. We are passionate about partnering directly with our customers to solve problems together and strive to provide the greatest level of service. All current employees of Peregrine have successfully passed Department of Justice and Criminal History background checks to support the Law Enforcement mission.

Peregrine provides Law Enforcement Agencies with a platform to search, manage, analyze and collaborate on all law enforcement data sources in one place
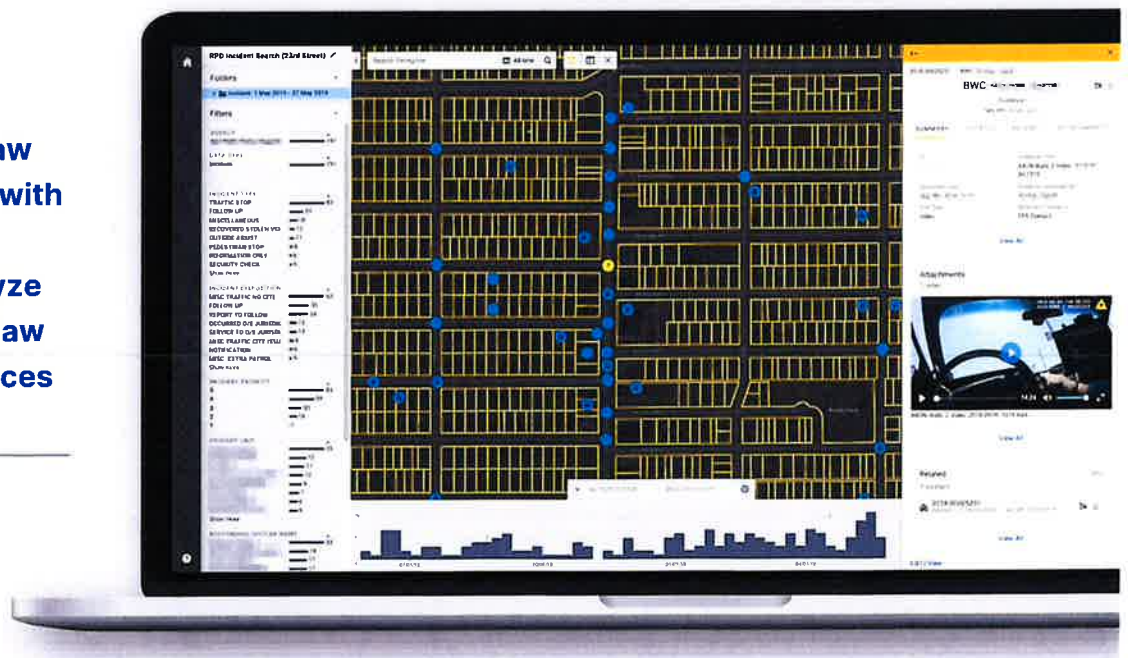
Experience in Contra Costa County & New Mexico

Peregrine's software platform was developed and deployed after 18 months of research and development in partnership with law enforcement personnel in Contra Costa County, CA.

During this research and development period, Peregrine founders were embedded in a full-time capacity studying and integrating key data sources used by law enforcement agencies in and around Contra Costa County, including but not limited to CAD/RMS data, gunshot detection data, body camera video, interview room video, police reports, search warrant data, video data, various sensors, and other unstructured data sources. Peregrine has active engineering projects with the city of San Pablo, CA and Pittsburg, CA, that involve the integration of several law enforcement data sources into a single web-based Software as a Service (SaaS) analytics and reporting platform in full compliance with California DOJ CJIS requirements.

In addition, Peregrine's software platform is deployed at the Crime Analysis Unit of the Real Time Crime Center for the Albuquerque Police Department in New Mexico.

A Peregrine deployment team integrated key data sources used by Albuquerque PD, including but not limited to CAD/RMS data, gunshot detection data, body camera video, interview room video, police reports, search warrant data, traffic citations, crash reports, arrest warrant data, GIS map layers, booking photos, and various unstructured media data sources. Peregrine has active engineering projects with the City of Albuquerque, NM that involve the integration of several law enforcement data sources into a single web-based Software as a Service (SaaS) analytics and reporting platform in full compliance with California DOJ CJIS requirements.

Please direct initial reference checks to:

Captain Brian Bubar	Lieutenant Brian Mathews	Commander Leonard
San Pablo Police	Pittsburg Police	Nerbetski
Department	Department	Albuquerque Police
brianb@sanpabloca.gov	bmathews@ci.pittsburg.ca.	Department
(707) 301-6032	us	lnerbetski@cabq.gov
	(925) 786-3762	(505) 235-9068

Peregrine Use Cases

Peregrine empowers law enforcement officers and personnel across the entire agency. Use cases include:

- **Global Search & Discovery**

    - Law enforcement officers and personnel across every team leverage Peregrine to access and review all available information from one secure location, saving hours of time otherwise spent logging into and navigating through multiple disconnected systems.

- **Secure Collaboration Across Teams & Partner Agencies; Electronic Filing**

    - Granular security and access controls allow teams and agencies to securely collaborate, with peace of mind knowing that security requirements are reinforced and adhered to. Rather than physically transport sensitive data, rely on phone calls, fax, or miss a piece of critical information, personnel seamlessly share information via CJIS and FIPS 140-2 compliant cloud infrastructure, with controls that ensure each person sees only what they are authorized to see.

- **Investigations**

    - Detectives use Peregrine to find leads that were previously undiscoverable, manage cases, synthesize results, and securely collaborate with internal and external teams. All available law enforcement data sources are available to investigators in one location, empowering detectives to ask questions, find answers, and make faster, more accurate decisions.

    - Investigative staff can overlay and correlate multiple information sources simultaneously to find connections. Raw data is cleaned and enriched automatically so that investigators spend more time on analysis and decision-making, and significantly less time on manual data processing.

- **Decision Support for Executive Leadership**

  - Peregrine empowers executive leaders with tools to ask questions, review critical information, and make decisions based upon reliable data that previously took their staff days or weeks to create. Reports, dashboards, intelligence briefings, critical media and documents are accessible through intuitive interfaces that otherwise require significant manual labor to retrieve and synthesize.

  - With investigators, analysts, and operations staff utilizing the same interoperable platform, executive leaders can maintain full situational awareness of their organization's activity and utilization of resources to the necessary levels of granularity.

- **Real-Time Operations**

  - Operational staff maximize real-time situational awareness with all available information accessible in a single view. Operators react to sensor activations, alerts, events, and patterns by immediately reviewing myriad data feeds in a single system including live video, CAD incidents, arrests, cases, individuals, and various real-time and historical sensor feeds.

  - Multiple internal and external collaborators can access and monitor information feeds in real-time, with security controls to ensure each participant can access only what they are permitted to view.

  - Actionable intelligence can be transferred to command staff and field operations for real-time review, and after-action-reviews can be conducted to review steps that were taken by staff in response to critical events.

- **Report Automation**
    - Analysts leverage Peregrine to automate reporting that would otherwise be created manually over the course of multiple hours or days and re-created manually any time new questions are asked or changes are required.

    - Peregrine removes the need for importing, exporting, cleaning, and merging of raw data across multiple systems. All available data is integrated, enriched, and accessible in one powerful report building interface, empowering analysts to spend more time answering questions and less time on manual work.

    - Peregrine also provides significantly improved methods to audit information, which means analysts and those reviewing critical data can trust and verify their results. Leaders can review reports, ask new questions on-the-fly, and get answers in real-time rather than waiting days or weeks for information.

Peregrine Capabilities Summary

Data Integration

- Flexible integrations accommodate data of any type or scale

- Automated tagging of unstructured data

- Link detection across disparate data sources

- Duplicate detection and record resolution/merge suggestions

- Automated data transformations, including time-zone conversion

- Automated linking of imported data from search warrants (such as mobile

Search

- One place to perform global search across all data sources

- Full-text querying across all data in the system, both structured and unstructured

- Advanced geospatial search filtering within specific addresses, areas, and transportation routes

- Store search results and save complex queries for repeat search

- Configurable monitors & alerts

Advanced Analytics

- Geospatial, temporal, and network analysis across multiple data sources

- Drill-down analysis on specific activities, persons, or events

- Link-exploration across data that was previously locked in siloed databases

- Advanced filtering of any data type or data value

- Live dashboards connected to analytics platform for exploration of underlying data

Secure Collaboration

- Rich presentation tools to share analyses or narrate a criminal story

- Real-time collaboration between officers and investigators inside a shared web application

- Automated & saved reporting

- Granular data security and permission model to configure access controls according to regulatory and agency needs

- Secure data export with audit logging

Access Control & Security

- Full data lineage including when it was created or modified and the data source from which it was derived
- Granular security and access restrictions associated with specific data types and data sources

Enable law enforcement to seamlessly access, investigate, and collaborate on data across the organization.

11
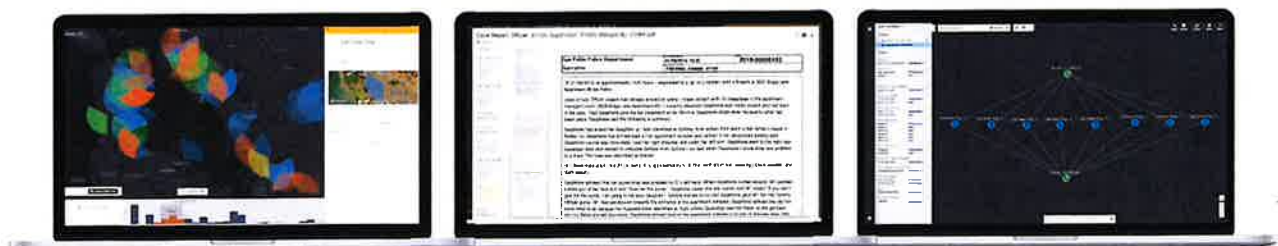
APD Data Sources

Agency Wide Data Integration

Peregrine proposes to integrate APD's key data sources, including:

APD Data Sources

- Records Management Systems (Data 911, Mark43)
  - All records including incidents, arrests, citations, cases, subjects, vehicles, property, & personnel
  - All associated media and case reports
  - Links between systems and records
- Computer Aided Dispatch Systems (Data 911, Mark 43)
- Automated Vehicle Location (AVL)
- Milestone VMS
- Shotspotter via Freeway Security Network (contingent on third party API fee)
- Vigilant commercial, fixed camera, mobile patrol car data (contingent on third party API fee)
- Body-worn camera & video database
- Eagle Eye Contract Vault
- BlueTeam (IAPRO)
- Booking photographs when available
- ESRI

Cell and Social Media data from Search Warrants

In addition, Peregrine has created and continually expands a suite of integrations for automatic import and analysis of search warrant returns. Detectives and administrators can drag & drop data into Peregrine, which immediately detects the type of search warrant return, extracts data for analysis, and links search warrant data with other APD data sources.

Search warrant data integrations include:

- Historical call data records for 4 major wireless communications service providers
- Mobile phone historical and live GPS ping data
- Physical phone extraction data

Proposal Logistics & Implementation

Initial Milestones & Project Deliverables

Peregrine intends to complete the integration of APD's proposed data sources no later than 12 weeks following initial data access. Timeline initiates upon access to all proposed data sources.

TIME

Pre-Work: Scoping & Kick Off (2 weeks)

- Get access to identified data sources and introduction to users
- Set up project team and governance

KICK-OFF

Month 1: Data Integration, Modeling, & User Discovery

- Standup Peregrine
- Setup proper permissions controls
- Ingest, transform and model data sources
- Validate data quality with APD team
- Onboard first set of users
- Start work on scoped projects (e – filing, interagency sharing)

STEERING COMMITTEE

Month 2: Data Integration, Modeling, & User Discovery

- Continue data integrations and data quality validation
- Train users to use the whole suite of Peregrine applications for real-time search, analytics, reporting, investigations, and other workflows
- Continue to implement projects and identify additional areas of interest

STEERING COMMITTEE

Month 3: Operationalization & Next Steps

- Finalize remaining data integrations
- Collect feedback and iterate on workflows
- Validate implementation of data integration and projects based on actionable results

STEERING COMMITTEE

Key Team Members

- **Antioch Police Department**
    - **Project Sponsor Description of Role:**
        - Responsible for strategic vision, day to day logistics & interactions, and user access
    - **Technical Sponsor Description of Role:**
        - Responsible for IT management and day to day technical / data source access requirements
- **Peregrine Technologies**
    - **Executive Sponsor:** Nick Noone, CEO
    - **Project Lead:** Toki Sherbakov, Deployment Strategist
    - **Implementation Team:** Dana Ford, Forward Deployed Engineer; Sarah Hollingsworth, Deployment Strategist
    - **Central Infrastructure Team:** Ben Rudolph, CTO

Data Sources & Access Controls

- **Data Sources**: Peregrine proposes to integrate Data911 CAD/RMS, Mark43 CAD/RMS; Milestone VMS; Search warrant data sources; Automated Vehicle Location (AVL); Shotspotter through Freeway Security Network [excluding API fees] ; Vigilant commercial data, Vigilant fixed cameras, Vigilant mobile patrol car camera [excluding API fees]; Eagle Eye Contract Vault, BlueTeam (IAPRO), Booking photographs when available, ESRI, and other identified internal data sources

- **Additional Integrations**: All additional data integrations shall be at the mutual agreement between the Project Sponsor & Project Lead

    - After Project Sponsor & Project Lead agree on additional data integrations, Project Lead & Technical Lead will coordinate the data modeling & technical requirements, respectively, with APD's Technical Sponsor

    - Peregrine will model, ingest, and make available new data sources to users in real-time and shall work out data inconsistency & proper representation case by case

User Access, Onboarding & Training

- **Current User Access**

  - Peregrine Platform access can be configured for on-premise as well as off-premise access via APD desktop and mobile machines

    - All users are assigned individual, two-factor authentication credentials

    - Mobile device management to be determined with Technical Sponsor as-needed

- **Adding & Removing Users**: APD may add an unlimited number of additional APD users to Peregrine Platform & Peregrine Mobile

    - APD's Project or Technical Sponsor retain specific approval rights to new users

    - Once a written request for a new Peregrine user is submitted, Peregrine shall then supply the new user with secure, two-factor authentication credentials and schedule an introductory training session

    - In the event of the need to remove users from Peregrine, within 24 hours of a request to remove user by APD's Project or Technical Sponsor, Peregrine shall revoke all access rights

    - Peregrine can support an Active Directory integration to enable automatic user addition & removal

- **Onboarding & Training**: Each new user shall have Basics and Intermediate training sessions to provide 1) Overview of the Peregrine application(s), 2) Background on currently accessible data sources, and 3) Introduction to analytic capabilities. Additional training will be carried out based on need

Support

- **On-site Support**: Peregrine shall support APD users on-site with in-person trainings, analytical support, user feedback, modeling/understanding of additional data sources or automated data imports, and new product features

    - Peregrine employees performing on-site support shall receive prior approval by Project Sponsor in order to access APD premises & interact with users

- **Offsite Support**: Peregrine provides 24/7 critical tech support via support@peregrine.io and support line (630) 946-4273. Peregrine's Project Lead and Technical Lead are also available and make best efforts to address user or administrative concerns.

## Service Levels & Issue Resolution

- **System Availability:** During any calendar month, the Peregrine system shall be available to users no less than 99.9% of the time on a 24x7 basis, excluding scheduled maintenance of the system, provided that Peregrine is not responsible for any downtime of the applications or software caused by third party data services (e.g. Evidence.com or Mark43 database). Peregrine shall provide APD with prompt notification as soon as it becomes aware of any actual or potential unscheduled downtime of the system, as well as periodic updates during the unscheduled downtime regarding Peregrine's progress in remedying the unavailability and the estimated time at which the system shall be available.

- **Issue Response and Resolution**:
  - "Severity level 1 error" means any system error that renders the system or any material portion of the system inoperative, or materially impairs use of the system in a production environment.
  - "Severity level 2 error" means any system error that substantially impairs use of one or more features or functions of the system.
  - "Severity level 3 error" means any system error that has a minimal impact on the performance or operation of the system.

Severity Level	Level of Effort	Initial Response	Work Around	Permanent Fix	Status Updates
1	Continuous best efforts, 24/7	Immediate, but in no event to exceed 30 minutes	8 hours	3 calendar days	Every 2 hours prior to work around and every calendar day until permanent correction
2	Commercially reasonable efforts, 24/7	1 hour	24 hours	5 calendar days	Every 6 hours prior to work around and every calendar day until permanent correction
3	Commercially reasonable efforts, during normal business hours	1 business day	10 business days	20 business days	Every 2 business days prior to work around and every calendar day until permanent correction

APD Technical Details

- **Software Architecture, Hosting, & Security:** Peregrine has implemented procedures to adhere to the FBI CJIS Security Policy. In addition, the hosting facility for Peregrine software utilizes state-of-the-art access control technologies that meet or exceed CJIS requirements

- **Application Requirements**: The Peregrine Platform runs on the following applications:

  - Browser requirements for Peregrine Platform – Google Chrome Version 69 and above, Mozilla Firefox Version 62 and above, or Microsoft Edge Version 17 and above

  - Mobile device requirements for Peregrine Mobile – iPhone OS version 12.0 and above

- **3rd Party Data Access:** In order to model & ingest 3rd party data sources, Peregrine requires explicit Project Sponsor approval & grant of access rights

- **Upgrades:** Peregrine continuously invests and upgrades the current software platform on a daily to weekly basis. All upgrades are included in the APD annual license and as the platform evolves, Peregrine shall give 48 hour advance notice of any "major upgrades" (i.e., affect application availability for more than 60 minutes)
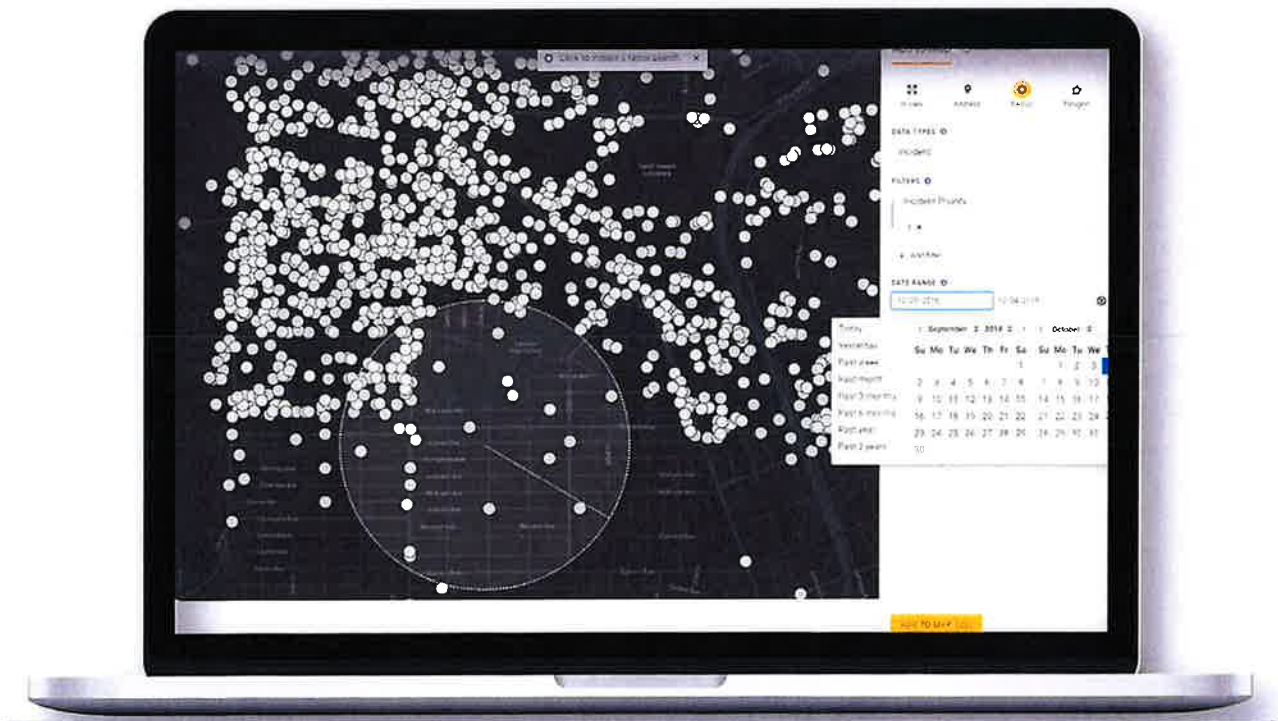
Pricing

The below contemplates a package price and includes an unlimited, site wide, subscription license package. Peregrine looks forward to partnering with APD to ensure the user experience & platform achieves APD's objectives.

The license includes the Peregrine platform as it stands today, including use cases & capabilities as detailed on pages 8–10, professional services, training, and all future software improvements. Peregrine will honor the proposed annual subscription price for years 1-3 of the subscription agreement.

City of Antioch Peregrine Platform Pricing Estimates	
Pricing Estimates, Hosted / Software-as-a- Service	
1. Software Licensing – Other than or in addition to annual subscription.	Not applicable
2. Third-Party Licensing (if applicable) – Discuss pricing for any recommended third-party solutions.	Third Party API or data fees may apply*
3. **Vigilant API**	~~$5,000~~ *waived***
3.Implementation – Training, user adoption, travel expenses, initial installation, scoped data conversion, scoped integration, etc.	~~$60,000~~ *waived***
4. Annual Subscription, 3 Years – Includes operating and maintenance, support, data conversion, data integrations to meet project objectives	
Year One	$127,000
Year Two	$127,000
Year Three	$127,000
5. Total Year One	~~$192,000~~ ** $127,000
6. Total Three Years	$381,000

*Third Party API or data fees may include: Vigilant partner agency and/or commercial Data, Clear, TLO, etc.
**Waived with multi-year agreement

Package Details (1/2)

Peregrine Technologies Annual License – 1 Year Term	**$127,000.00**
Enterprise Data Integrations	Included
Data911 records management system database	Included
Data911 computer aided dispatch system database	Included
Mark43 records management system database	Included
Mark43 computer aided dispatch system database	Included
Automated Vehicle Location (AVL)	Included
Milestone VMS	Included
Vigilant commercial, fixed camera, mobile patrol car	Included
Eagle Eye Contract Vault	Included
BlueTeam (IAPRO)	Included
Booking photographs when available	Included
Shotspotter via Freeway Security Network [excluding third-party API fee]	Included
Body-worn camera data source if/when applicable	Included
National Integrated Ballistic Information Network (NIBIN) database	Included
ESRI	Included
External API	Included

Package Details (2/2)

User Training & Support	Included
Peregrine platform introductory user training	Included
Peregrine platform advanced user training	Included
User-specific workflow development and support	Included
24-hour troubleshooting	Included
Software deployment, upgrades, and feature enhancements	Included
Peregrine Platform Tools	Included
Unlimited users	Included
Unlimited search queries	Included
Unlimited saved search queries	Included
Unlimited investigations	Included
Unlimited alert configurations	Included
Unlimited exports and downloads of data	Included
Unlimited report templates	Included
Unlimited dashboard configurations	Included
Unlimited sharing between internal users	Included
Unlimited sharing with external organizations	Included
Unlimited interagency searches	Included
Generic file storage	Included
Search warrant data import & processing	Included
Generic tabular data import & processing	Included
Entity resolution capability	Included
Permission controls, including location-based, user groups, and cell-level ACLs	Included
Within-agency permission controls	Included
External organization permission controls	Included
Full audit capability	Included
Automatic record deletion detection & expungement	Included