**E.T.S.**

(Evidence Tracking Solution)

CNT4182

RVC1198

SG-09

Randy Van

Yosselyn Andino

Juan Carlos Gonzalez

Manny Garcia

**Table of Contents**

[Overview 3](#_Toc25409152)

[Data 10](#_Toc25409153)

[Technology 17](#_Toc25409154)

[Business 22](#_Toc25409155)

[Security 27](#_Toc25409156)

[Standards and Regulations 33](#_Toc25409157)

[Appendix A](#_Toc25409158) - [Incident Response Plan: 35](#_Toc25409159)

[Appendix B](#_Toc25409160) - [Privacy Impact Assessment 39](#_Toc25409161)

IoT High Value Evidence Product Development

# Overview

**Context:**

The Drug Enforcement Administration (DEA) has recently come across major drug in the past few months. They have acknowledged the possibility of some of the evidence being inadmissible in court because there could have been some tampering of evidence or discrepancies in the chain of custody. This could lead to powerful drug lords either getting away with the crime or facing a significantly lighter sentence. The cartel has major widespread influence in the area due to corruption, intimidation and power. Important evidence could seemingly vanish and there could be odd gaps in the trail of records. Often these drugs bust happen in remote areas like the middle of the desert and communication and connectivity is limited.

The DEA wants an efficient, secure and reliable way that takes detailed accounts of who has handled the evidence and a detailed account of the movement of the evidence. Our company aims to solve this issue by developing a smart sensor-based application which will be employed by law enforcement agencies to account for the location of evidence items required for prosecution. This information would also be used by the law enforcement evidence custodian, forensic lab personnel, and lawyers from both sides of a criminal case. Considerations like environment, type of user, location and policies will be considered. Its primary aim is to establish a continuous chain of custody as well as simplify the location, retrieval and overview of all evidence on a per-case basis.

**Problem Statement/Ask:**

To develop a new application based on smart sensors that will be employed by law enforcement agencies to account for where evidence items required for prosecution are located. This solution will solve the need to use paper records, misplacement, delay in processing, and/or loss of key evidence, ensuring a continuous chain of custody, or, at the very least accountability as per the evidence last known location.

**Product Vision:**

The solution is proposed to be a cloud-based application, which will ensure its accessibility from a variety of permitted devices and various locations (i.e. evidence room, forensic testing lab, or court room) to the exact location of an evidence item. This way access will be regulated, and risk is reduced for intrusion or leaked information due to misconfiguration. Evidence will be stocked and accounted for by means of sensors. Each level will have an associated method of tracking which will report to the solution and provide information like Timestamps, User, and Location. Upon receiving the requirement from primary users, the solution should be intuitive, accessible, efficient and effective at rapidly locating a desired item from a large collection. Regardless of the initial requirements the solution should be secured given the type of information it will handle and the consequences an attempt against C.I.A (Confidentiality, Integrity and Availability) would have in the cases being prosecuted and the final resolution. Sensors used to track evidence will be reliant to cold/hot environment as well as humidity, magnetic interference, and loss of signal if stored below ground, also any type of over-the-air connection will be encrypted.

**User Groups:**

**Administrator Level:** Users with complete access to the solution back-end does not necessarily need to be able to see the confidential information but it’s cleared to do so in case of an outage or trouble ticket is issued. Motivation for accessing solution is for troubleshooting, monitoring correct functioning and implement changes the customers have requested. The admin would not be able to see the details of the case, only be able to see that it exists and its metadata. A process like a “fire call” could be implemented if the administrator needed to see the details of a case.

**Primary Users:** Evidence Collectors, Lab Technician, Police Department Officers (with clearance), this user can add, remove (once it has been cleared for return to owner), alter, evidence and description. Primary users will be able to access historical data logs.

**Guest Users:** Court Room Users, Client Facing Users (Lawyer, DA)this is a case by case user with very restricted access which is revoked after case has been completed with the ability to re-open stored data should the need arise, user is only able to query cleared evidence and request it with approval from higher entity.

**Benefits:**

The customer base will enjoy a robust and dynamic system that will locate the evidence in the shortest number of steps possible, a secure platform that can be shared between departments to boost collaboration, prioritization of processing and storage of evidence, as well as continuous accountability for the item’s location. The intuitive solution will make it easy for an user of any level to input a serial number, label, or case number related information and retrieve all associated evidence to which they are authorized to access and its current location, multiple actions and features like requesting delivery, accessing chain of custody and report of analysis made to the evidence can be implemented at customer’s request.

The organization will be benefited from faster processing times in cases and evidence analysis, collaboration between alienated departments as well as enjoying the peace of mind of being able to locate an item from a hand-held device or workstation. Higher accountability will ensure correct handling and storage of evidence that could be key to a case that is being prosecuted as well as recollecting old evidence if a case is re-opened will be an easier process. Additionally, the process of purging and destruction of unneeded evidence will be faster for the business and will reduce costs, as evidence that is deemed to not needed can be disposed of faster.

**Primary Users (Supports User Groups)**

* **Law Enforcement Evidence Custodian** – Keeps a detailed log of all the contents, as well as detailed chain of custody logs, of the items that have been added to the evidence inventory system. Mainly, they oversee evidence held by law enforcement agencies. Their main duty is to preserve the integrity of the evidence collected and allow the required parties to have controlled access to the evidence. It also falls under the purview of the Evidence Custodian to fulfill any FOI requests made from civilians. Additionally, it is their duty to purge and destroy evidence once it is deemed to not be needed anymore. Using or acquiring this application would allow an evidence custodian to efficiently account for evidence items required for prosecution and where they are located at all times. in a secure manner that does not affect the integrity of the evidence collected in any way. It would also allow the custodian to fulfill his aforementioned duties in an easier way.
* **Forensic Lab Personnel** – Personnel who works at crime laboratories to examine evidence from criminal cases. They run tests on the evidence brought to the labs, analyze the data, and provide a detailed report on the information gathered from the pieces of evidence. The personnel include forensic scientists, fingerprint analysts, crime scene investigators, and the Scene of Crime Officer (SOCO). The forensic lab personnel would find it useful to have an application that can track the location of physical evidence so it can be quickly accessed and accounted for prosecution. When law enforcement officials come to pick up the analyzed evidence and reports, the forensic technicians can use the application to locate all the needed evidence. The application would assist the forensic labs to keep a detailed log of all evidence, which would help in preventing any evidence to go missing.
* **Prosecution lawyers (DA)** - it’s a prosecutor’s job to prosecute accused criminals and seek conviction through concrete analysis and evidence through various methods. They must determine what charges to bring about and what punishments to seek, interview witnesses and explain the process and reasons behind their decisions. The motivation for the use of the application is that it gives the prosecutor assurance that the integrity of the evidence presented in court has been preserved through tracking and logging. The application assures that no evidence has been tampered with.
* **Defense Lawyers** – Similar to prosecution attorneys, however, they defend the individuals being accused by the state or a third party. Defense lawyers require access to evidence pertaining to their cases in order to provide adequate counsel to their clients, therefore they must have access to evidence. This system will help defense lawyers by ensuring that evidence has not been tampered with or incorrectly attributed to their client, for example. Defense lawyers would have restricted access to the application, however, so the prosecution and evidence is not compromised.
* **Law Enforcement Officials (L.E.O.)**: The role of a law enforcement official is to deter crime and assure community in their jurisdiction. They investigate crime and apprehends suspected criminals. They maintain law and order and protect the members of the public and their properties. The motivation for the use of the application for law enforcement officials is that it ensures proper chain of custody and gives the location of the evidence gathered and provides accountability.
* **Crime Scene Technicians**: Individuals that gather evidence requested by Investigators. This evidence usually requires specialized equipment, collecting procedures and/or special handling. Along with LEO, these are the primary users who add evidence to the inventory system. Crime Scene Technicians would benefit this application as it would allow them to enter information in the system with less likelihood of errors (like inputting a wrong date or time) which could otherwise make evidence unusable in court.
* **Dept. Of Justice Officials**: D.O.J. officers typically oversee transporting and safeguarding the evidence while its being transported to court, and back to the evidence inventory. Their main duty is to liaison with court officials and produce the evidence the day it is needed in court for each case/suspect, and transport it with security agents/etc. This application would be beneficial to these users as it will make the logistics of collecting and preparing the evidence that needs to be transported much simpler. In case something is misplaced, it would allow for the evidence to be tracked.
* **Internal Affairs Audit Officers:** This user’s duty is mainly to oversee all LEO with regards to any activities related to evidence, ensuring the Law Enforcement Evidence Custodian is following all regulations and procedures. Since this application uses smart sensors, it will reduce the amount of monitoring that needs to be done. It will also allow the monitoring the integrity of the evidence and its chain of custody to be monitored more reliably by the IA Audit officers.

**Features:**

Customer based Requirements

* Submit items into evidence by trusted individuals
* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Provide event-based alerts
* Tracking Chain of custody
* Dispose of items of evidence, as well as manage the database holding the information.

Back-end Requirements

* Administrative features:
* Admin users can create and control security groups
* Designate functional roles
* Restrict access and capabilities within the system
* Backup data
* Access to historical data logs of chain of custody and retrieval

**Features per User Category:**

Administrators

* Create and control security groups
* Designate functional roles
* Restrict access and capabilities within the system
* Backup data and configuration files

Law Enforcement Evidence Custodian

* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Provide event-based alerts
* Tracking Chain of Custody
* Dispose of items of evidence, as well as manage the database holding the information

Forensic Lab Personnel

* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Provide event-based alerts
* Tracking Chain of Custody

Law Enforcement Officials

* Submit items into evidence by trusted individuals
* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Provide event-based alerts
* Tracking Chain of Custody

Crime Scene Technicians

* Submit items into evidence by trusted individuals
* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Tracking Chain of Custody

Dept. Of Justice Officials

* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Provide event-based alerts
* Tracking Chain of Custody

Internal Affairs Audit Officers

* Tracking and logging of evidence movement
* Provide event-based alerts
* Tracking Chain of Custody

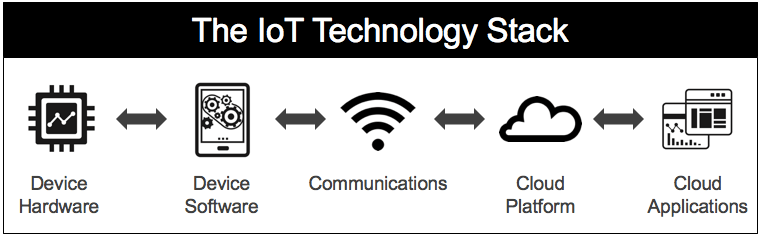
Prosecution Lawyers (DA)

* Present evidence when and where it’s needed
* Tracking and logging of evidence movement

Defense Lawyers

* Present evidence when and where it’s needed
* Tracking and logging of evidence movement

**IoT Stack Reference:**



**IoT Stack:** the interconnectivity of technologies, standards and applications

Device Hardware: Smart sensors would be used to track and log the activity associated with all evidence gathered. Activity is comprised of tagging, logging, provide location data, as well as details on current user in possession of the item.

Tags/NFC/RFID chips: These would be used to uniquely identify each item in the evidence application. Considerations must be taken as to the nature of the evidence collected and the specific identifier that should be used (dimensions, type of adhesive, etc.)

Device Software: Software with the purpose to send and receive data from cloud platform hosting solution, connection secured via Virtual Private Network (VPN) and Mobile Device Manager.

Data: All data will be encrypted before being transferred.

Communications: All forms of communication will be encrypted.

Cloud platform: Software as a service (SaaS) is the platform being used. It takes away the installation and configuration portion on the user’s side, it’s lower cost, is scalable. easily integrated and it’s easier to perform upgrades on.

Cloud Applications: The benefits of the application being a cloud-based application is that is reliable, flexible and cost effective. With cloud-based applications it is easy to both scale applications for growth.

# Data

Identification of data elements:

* Location Data – sensors would track the locations of all the items using GPS.
* Status Data – users would know the status of the items being tracked in real time. Users would know where the items are, whether it made it to the destination and when, etc.
* Automation Data – whenever certain events occur like an item reaching one of its destination checkpoints, an item arriving late to a particular location or a sensor beginning to fail. The application would send automated alerts and log these events. When a sensor begins to show signs of failure, it would begin to back up its data to the cloud.

Data collected for tracking purposes:

* Unique Identifier of the piece of evidence being tracked (from the FRID/Barcode/Tag issued to the piece of evidence)
* Unique identifier of the user inputting or accessing the evidence tracking system (username used to log in into the application interface via HTML5 compliant web browser)
* Location (Global Positioning System (GPS) coordinates)
* Time (Coordinated Universal Time, UTC)
* Date (Gregorian Calendar format)
* Unique Identifier of the specific sensor that collected the data (MAC Address used to send the data)

The smart alerts feature which is an event based alert system that logs and automates alerts whenever certain conditions are met like an item arriving on time or when anomalies occur like a blizzard occurs. The smart alerts feature is enhanced by the combination of the automation and the status data being collected. In addition, the more environmental data that is being collected, the more data the sensors can use and analyze what temperature it should sustain to maintain optimal performance.

**Data Required by Features**

Unique Evidence Identifier:

* Submit items into evidence by trusted individuals
* Handle the evidence by the pertinent individuals
* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Dispose of items of evidence

Unique User Identifier:

* Admin users can create and control security groups
* Designate functional roles
* Restrict access and capabilities within the system
* Submit items into evidence by trusted individuals
* Handle the evidence by the pertinent individuals
* Tracking Chain of Custody

Location Tracking:

* Present evidence when and where it’s needed
* Tracking and logging of evidence movement

Date & Time:

* Present evidence when and where it’s needed
* Tracking and logging of evidence movement
* Tracking Chain of Custody

**Data Collection**

* The sensors will collect data and send it securely. Data should be processed, at least encrypted, before being sent over the VPN. In the case the sensor has no connectivity, perhaps some more processing might be needed, as the data should stay encrypted on the sensor until it is sent over the VPN. A solution that allows the user to enter data even when this occurs, perhaps an app that provides same front-end as the website, collects and stores the data and metadata, encrypts it, and sends it to a main secure server that integrates it to the main database once connectivity is found may require more processing as well by the sensors
* Any required data will be supplied by authorized users. All stakeholders from all user groups will provide their user credentials such as the unique user identifier. The administrator group will input the user data gathered in order to create security groups and assign roles.
* From the primary users’ group, law enforcement officials and crime scene technicians will input the evidence data, with each piece of evidence receiving a unique evidence identifier. This data will also include the date, time, and location pertaining to evidence for tracking and logging.

**Data Accessibility**

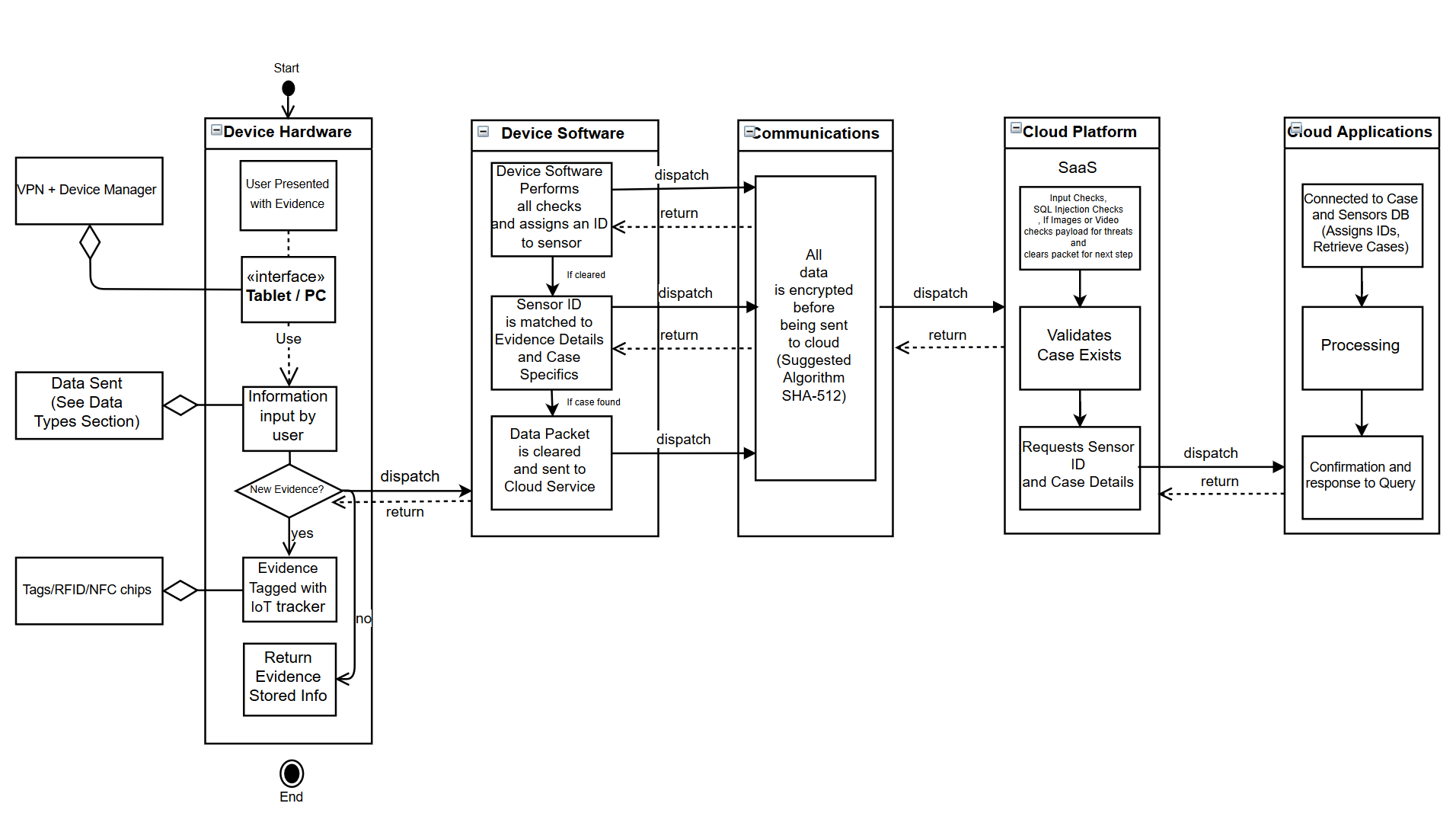
* Access to the data during its use would be permitted to authorized users. Primary users such as the law enforcement evidence custodian, will have access to data for tracking purposes and to ensure evidence integrity. Dept. Of Justice officials will need access to the date, time, and location of court cases to efficiently transport the evidence to its respective court room.
* Guest users, which include prosecutor lawyers and defense lawyers, will have access to evidence data during trial. This access to data will give guest users the assurance that the integrity of the evidence presented in court has been preserved, and that the evidence has not been compromised.
* Access to the data after its use will depend on the final ruling of the court case. After the trial, evidence from resolved cases must be stored and preserved in the evidence storage vault. Evidence from unresolved cases may be stored for an indefinite time. Law enforcement officials leading the investigation of a case will need access to data after its use, in the event of a case reopening or a correction to a case ruling.
* The presiding judge has the power to make judicial proceedings and the trial record (where evidence would eventually become public) closed doors and not available to the public, at his/her discretion, as well as to comply with federal/state laws.

**Real Time:**

* Access to this data should be restricted only to the relevant parties involved in the case, following relevant state and federal law. Case evidence gathered and tracked will be tied to a Court Case Number (which is a unique identifier). Only relevant users that are party to a case, which would be the DA or Assistant DA handling the case, the defense lawyer, and judge will have access to all the data during the pretrial and trial proceedings. The Law Enforcement Evidence Custodian may also have access, in order to corroborate the evidence’s integrity.
* Dept. Of Justice Officials would only need the tracking information of the evidence record, but not full access to the data itself, in order to transport the evidence and secure the evidence in court.
* Similarly, Internal Affairs Audit Officers should also similarly access in to ensure no foul play has taken place by state/federal agencies and to give them the ability to analyze the tracking information, to verify the Evidence Custodian’s lawful handling and safeguarding of evidence. Additionally, there should be a process that allows this user to see all evidence data lawfully, while being audited as they do so.

**Historical Access:**

* At the end of trial, access to the evidence is decided according to the type of charge, type of physical evidence (DNA, hair, footprint impressions, fingerprints, etc.), the verdict, among other factors, by the judge presiding over the case in accordance to federal, state and county laws and guidelines. Additionally, evidence collected from unsolved cases could be stored indefinitely in some jurisdictions and made available to other agencies upon request, or individuals associated with government agencies upon request.

**Data Flow Diagram IoT Stack:**

**Data Flow (Explained):**

Successful understanding of the above diagram relies in following the concept of any arrow labeled ‘dispatch’ overrides any action from top to bottom until the arrow labeled ‘return’ completes the cycle from left to right. The above diagram is an attempt to visualize the data exchange, deemed “dataflow” from beginning to end when users interact with our solution. Diagram has been created following the IoT Stack basics represented above. Starting from Device hardware it is expected the user to be presented with search query or new evidence, the user will interact with an interface (deemed Tablet/PC) which will be secured via Virtual Private Network (VPN) and Device Manager. By using the interface an input will be dispatched to Device Software, where a series of checks will be requested through Communications Section, Cloud Platform subsequentially returning a desired response before moving down to the next step. Once all ‘checks’ have been completed one last data packet containing the query will be sent through Communications Section to our Cloud Platform to be validated and make the final request to Cloud Applications which interacts with Evidence and Sensor Database to fulfill query. Lastly returning a desired response to the device hardware where a decision was initially made for new evidence or existing evidence.

Our thought process while working in the Diagram allowed us to come up with multiple scenarios however as a rough draft, it is understandable this is an iterative process and new test cases will apply, our application is designed with modularity in mind, making sure ETS can always incorporate new features the consumer requests. For this test case based on customer requirements, ETS has implemented an interface that allows for two basic functions to be performed, to add new evidence, to retrieve information about stored evidence. The user will query our solution platform from their allowed device which will do all the analysis on the cloud allowing for faster, safer processing, ultimately saving costs and incrementing accessibility. The above example applies to most of the customers interacting with the solution, a platform will be provided for those with administrator duties for monitoring and supporting the solution.

**Analytics**

The processing power needed to perform all analytics should be at the cloud. Given that do not know how many sensors a law enforcement organization would need, nor how many clients would need these sensors, it would be cheaper for the sensors themselves to have enough hardware required to only process the gathering, temporarily store it and transfer the gathered data. This would lessen the cost of the individual sensors when considering the power requirements of each. Additionally, the processing power needed to perform the analytics over time will increase. Once this happens, it would be a cheaper and easier to upgrade the processing power in the cloud (I.e. upgrading the servers in the SaaS backend) than to upgrading all the deployed sensors across the U.S.A.

Law Enforcement Evidence Custodian and D.O.J Officials:

Predictive:

Smart alerts based on the location of evidence and events occurred is a type of analytics that would be required. Additionally, this data could be correlated with real time traffic data from Google Maps API to accurately predict loading, pickup, and drop off times, making the process safer.

If evidence takes longer than expected to reach its destination, the application could automatically flag this evidence and give the receiving individual and the Evidence custodian a log event which would allow them to scrutinize the evidence more carefully upon taking possession of it.

Prescriptive:

By cross-referencing the time and location when each piece of evidence is needed in court, automated reports will be issued to these users detailing transportation needs required to transport the needed evidence to and from the courts.

By cross-referencing where a piece of evidence should be against an established perimeter set by the devices, the Evidence custodian and DOJ officials would receive immediate alerts the moment an evidence item is not found within this established perimeter it should be on.

LEO/Crime Scene Technicians:

Descriptive:

By cross-referencing the time and location when each piece of evidence is needed in court and which user added the evidence into the system, notifications can be issued to these individuals when evidence they have gathered is scheduled to appear in court, as they can be called during pretrial motions, to server as witnesses during the trial.

Predictive:

Crime scene technicians and law enforcement officials can benefit from predictive analytics by the application giving information like estimated time of arrival to ensure that the evidence gathered reaches its destination in a timely manner.

Prescriptive:

Prescriptive analytics can be used to optimize scheduling. With all the data gathered, the application would use algorithms to find the most optimal time to send items and the efficient routes to get the items to the destination as soon as possible.

Forensic Lab Personnel:

Descriptive:

The analysis of descriptive evidence data will benefit forensic lab personnel by easing the process of identification of evidence. Every piece of evidence belongs to a respective case. With this type of data, the lab personnel can track and log the activities related to a group of evidence from a specific case.

Prescriptive:

The personnel of forensic labs are constantly handling evidence from different cases. The notification system can help the forensic personnel to prepare an effective schedule in order to have evidence ready for testing, analysis, and collection from law officials.

Prosecutor Lawyers & Defense Lawyers:

Descriptive:

Prosecutor and defense lawyers can be notified when evidence has been readied for trial. By monitoring the location of the evidence, and tracking a chain of custody, the DA, assistant DA, and defense lawyer can corroborate the integrity of the evidence and that no evidence has been tampered with.

Predictive:

The use of predictive analytics can help determine the time of arrival of the evidence. Depending on whether evidence arrives on time or not, a trial can start on the scheduled time or be delayed. By gathering data related to distance travelled, weather conditions during transport, and chosen routes, a proper analysis can lead to better time estimates for the arrival of evidence.

Internal Affairs Audit Officers:

Descriptive:

The internal affairs audit officers would use descriptive analytics to compare the item and its times stamps from departure to arrival. This would give the auditor information of any potential anomalies that might have occurred.

Predictive:

The application would give the auditor the estimated time of arrival. If the actual delivery time is over the estimated delivery time, the auditor can investigate further on the causes and if it can lead to possible tampering.

Administrators:

Descriptive:

With all the information gathered the administrators can store the data in a database and keep track of the events that occurred, time and distance traveled, quantity, etc.

Predictive:

From previous data, administrators can use predictive analysis to anticipate how long an item would arrive based on their location and what challenges each route can potentially face during travel. Administrators can also use predictive analytics to predict weather future weather conditions that might cause a delay in delivery.

Prescriptive:

Administrators can use prescriptive data to extend and optimize the life of the sensors. By gathering information from the network of sensors, predictive data can use algorithms to know the best times to deploy updates and patches. The sensors would use a finite amount of power depending on different conditions.

# Technology

**Client-Facing Hardware:**

Sensor devices

Abeeway Micro Tracker – is a multimode tracker with sensors that combine technologies such as GPS, low-power GPS, WI-FI sniffer, Bluetooth Low Energy (BLE) and Long Range (LoRA) Time Difference of Arrival (TDoA) geolocation technologies.

https://www.abeeway.com/micro-tracker/

* Battery Life - Its long battery life allows it to function up to a year on a single charge.
* Durability - has an IP64 water resistant rating and is ATEX zone 2 and 22 certified which makes it resistant to explosive atmospheres. Has embedded temperature, motion and pressure sensors.
* Tracking - can monitor in real-time and give position alerts during anytime. It can check activity through its motion sensors and gives notifications at a scheduled time or on demand.

Gateway devices

Dell Edge Gateway 3002– specifically aimed towards the Internet of Things and offers cost effective security and management tools.

https://www.dell.com/tc/business/p/dell-edge-gateway-3002/pd

* Reliability - The Gateway 3002 embeds itself with countless types of endpoints and multiple sensors for precise analytics.
* Availability - The device enables analytics even during periods of lost connectivity
* Tracking - The device has integrated GPS, accelerometer and atmospheric pressure sensors that informs you where things are and where they are going.

Communication protocols used for interconnectivity

Data Distribution Service (DDS) will be used in between the sensors and the cloud servers because of its high performance and efficiency in real time data exchange. DDS communication is peer-to-peer which simplifies deployment, provides low latency, maximizes scalability and increases reliability.

* + - Performance and Efficiency– DDS can achieve data connectivity latencies that are as low as 30 microseconds and can output several million messages a second. DDS automatically discovers endpoints through dynamic discovery and doesn’t need to configure endpoints for communication.
    - Security – DDS provides authentication, encryption, access control and logging capabilities to enable secure data connectivity.

OpenVPN will be used for our VPN connections in between the user’s device and the gateway device. OpenVPN uses up to a 256-bit OpenSSL encryption library and SSLv3/TLS v1 protocols. It can be configured to run on any port and is configurable. It also uses AES which one of the strongest forms of encryption. OpenVPN can also compatible across all platforms.

**Cloud:**

Pivotal Cloud Foundry (PCF or simply CF) represents the next step in the evolution of IT, enabling us to focus exclusively on our system and data without worrying about underlying infrastructure.

* The Cloud Controller provides REST API endpoints for clients to access the system. The Cloud Controller maintains a database with tables for organizations, spaces, services, user roles, and more. Commands include staging applications, starting or stopping applications, collecting health information, and querying that all desired applications are running.
* PCF’s portfolio of modern runtimes allows us to deliver ETS system features faster. It is design with zero-downtime deployment as a priority.
* Systems are protected from attackers using Pivotal security model: Repair, Repave, and Rotate.
  + Repair vulnerable operating systems and application stacks consistently within minutes/hours of patch availability.
  + Repave every virtual machine (VMs) from a baseline state every few hours without application downtime.
  + Rotate credentials continuously (from every few minutes to a few hours)
* Rely on built-in high availability to keep front end customer systems online under even the peak traffic hours.
* Application life cycle management: BOSH can provision and deploy ETS over thousands of Virtual Machines. With BOSH, PCF provides tools to ease the workflow of several disciplines, including project management, requirements management, development, testing and quality assurance (QA) as well as customer support and IT service delivery.

Centralized platform administration and centralized logging:

* With CF, user accounts can be managed using User Authentication and Authorization (UAA) servers. These support access control as OAuth2 services, which can store user information internally. Alternatively, they can connect to external user stores through LDAP or SAML.
* With PCF, ETS can be deployed and made available to customers in a matter of minutes. The cloud easily scales applications to handle more traffic, simplifying the build-out and migration efforts.
* The git system on GitHub is used by PCF for version control source code. Developers on the platform can also use GitHub for their own custom configurations, as well as other resources.

Deployment Monitoring and Analysis

* Loggregator gathers and streams logs and metrics from user applications in a CF deployment. It also gathers and streams metrics from CF components. Loggregator architecture includes components for collecting, storing, and forwarding logs and metrics.

Dynamic Routing:

* With PCF’s Gorouter, traffic coming into Cloud Foundry is directed to the appropriate component, whether the request comes from an operator addressing the Cloud Controller. With Gorouter, traffic is routed appropriately to live, available instances.

Lastly, PCF will allow Integration with external logging components like Elasticsearch and Logstash.

**Analytic software:**

Data incoming from the hardware and sensors will all be analyzed on cloud software, this guarantees reliability, efficiency and safety when it comes to the resources that will be handled as well as cut down on the response times. For this specific solution adopting a containerization approach, using:

* **Docker**: a software that allows us to place all our code in “containers” or virtual buckets for modularity and organization.
* **Kubernetes**: a platform that orchestrates tasks, functions and networks the containers/clusters that have our code in order achieve the desired behavior.
* **ELK Stack**: a collection of analytic tools used in conjunction to take any type of data and provide a way to visualize it from input to back end. (**E**lasticsearch, **L**ogStash, **K**ibana)

This is a proactive approach for expanding and adding new features in the future as well as making the support/debug task easier. The ideal flow and use of these tools would be as follows; our code will be created and placed into docker containers, preferably categorized by area (consumer requirements, hardware functions, back end functions) this will make support easier in case of troubleshooting Kubernetes, our container orchestration platform will alert which specific container is having an issue cutting down research time. Data extracted from the devices will pass through the ELK Stack (see definition above). ElasticSearch allows us to store, search, and analyze big volumes of data quickly, in near real time it will sift through big datasets and extract information that will be passed to LogStash, a tool for collecting, parsing, and storing logs for future use, which oversees doing the processing of the information received from the hardware, finally ending in Kibana, which provides visualization capabilities on top of the content indexed on an Elasticsearch cluster, its main purpose is to prettify the processed data to make it easily understandable which is a benefit when looking at multiple statistics or large numbers of datasets.

The specific analytics that each group will have access will be as follows:

* **Administrator Level User:** Will have access to charts indicating, request/response times, hardware devices and sensors status, connection details, databases, and any other critical information to ensure the correct functioning of the solution and to make troubleshooting/implementation easier. Management from operational side has access to telemetry regarding sensors in use, cases added, as well as chain of custody records (they are not concerned with the technical telemetry).
* **Primary User:** Does not require access to telemetry, this user group will have access to requested datasets for a specific sensor or case. As a primary user they are concerned with interacting with the solution to add or retrieve case information and sensor location allocated to the given case.
* **Guest User:** Does not require access to telemetry (nor technical or operational) access will be limited and based on clearance from administrator level user group pending order from authorized individual.

**Mobile device software:**

The mobile application version of the solution will follow the architecture of a hybrid mobile application. A hybrid app functions as a native application that can be downloaded to a supported portable device, while running a web application inside. This will allow the web application to run in a mobile device and have access to the device’s features, such as the camera, or GPS.

**Hybrid Mobile Application Development Features**

* Decreased development cost
* Enhanced User Experience due to flexibility and accessibility
* Easy integration of device’s features
* Simple to maintain and sustain

With the implementation of a hybrid application, the development of multiple versions of the app will not be necessary to support different mobile operating systems. Meaning the application will be compatible with Android and iOS devices, effectively cutting the cost and time of development. A hybrid application bypasses versioning, meaning the creation and management of multiple releases of a software, as it makes app upholding as trouble-free as updating a website page.

This mobile application will have two main functionalities. The first function is to allow users the addition of new evidence, the second being the retrieval of information about identified or stored evidence. All users will input their sign in data which includes their unique user identifier or username. Primary users will be able to input new evidence data that will be assigned to a unique evidence identifier. The mobile device software will receive any input from authorized users, which could come from a search query, and then it will send a request to the cloud platform. The request consists of data packages with checks and queries that must be validated by the cloud platform, and then sent to the main cloud application which connects to the evidence databases. A response will then be sent back to the mobile application with the desired information.

The mobile application is expected to be functional on multiple portable devices. The main mobile devices would be tablets and smartphones. The flexibility and accessibility of a hybrid application allows the stakeholders to use any desired operating system from any smartphone or tablet, without worrying about the compatibility of the software and the device.

# Business

**Product Value**

Evidence Tracking Solution (ETS) was designed to ensure the integrity of evidence through the judicial process. ETS provides users with detailed, accurate logs in real time, provides a chain of custody and gives users comfort that the evidence presented in court is applicable. The price of litigation is costly, and the stakes are high; ETS ensures that users are in the best hands and provided with the best technology possible to protect the integrity of the evidence.

To show the value and features of the application to customers, ETS will partner with a Law Enforcement agency to initially deploy and test the system in a real-world setting. This agency will receive compensation in the form of future service discounts. This pilot implementation will be also be used for demonstration purposes. Along with a randomly populated evidence system (for testing purposes), gateway devices, sensors and tags used for demonstration purposes will be taken in person and shown by our vendors to interested agencies, as well as discussing where the sensors should be placed and how these devices function. ETS will provide detailed videos, documentation and functionality testing for each of the application’s features through this pilot implementation.

**Monetization**

Organizations would be charged a one-time variable cost fee for the hardware, depending on their size and needs, as well as a $20 charge per user per month for use of the application. Organizations with more than 100 employees are eligible for discounts. In addition, there will be a monthly service usage charge, to which ETS will add a 5%-8% markup, based on the amount of data storage and CPU usage (AWS Services) the organization incurs.

**Sample Pilot Customer ETS Implementation Costs:**

Organization: Small Police Department in a Suburban County, U.S.A.

Hardware Costs – Gateways and Sensors:

One (1) Main Evidence Storage Building: 2 Gateway Devices, 60 Sensors

Two (2) Court House Buildings: 4 Gateway devices, 40 sensors

Two (2) Forensics Laboratory Buildings: 4 Gateways. 40 sensors

Patrol Cars: 30 Sensors

Criminal Scene Investigation Vehicles: 10 Sensors

Evidence Transportation: 5 Sensors

Backup Sensors: 5% of deployed sensors: 10 sensors

Sub-Totals:

Total Gateways: 10 @ $887.70 = $8,877.00

Total Sensors: 195 @ $80.70 = $15,736.50

Initial RFID Badge Package: 4000 units = $400.00

Initial NFC Badge Package: 2000 units = $500.00

**One Time Hardware Costs: $25,513.50**

Users:

Law Enforcement: 80 Users

Technicians/Experts: 30 Users

DOJ Transportation Officers: 20 Users

Attorneys: 60 Users

IA/Audit: 5 Users

Total Users: 195

**Monthly Recurring Users Cost: 195 @ $20.00 = $3,900.00**

**Monthly Recurring AWS Services – Data Usage/Storage: Variable, estimated ~$2,500.00**

**Monthly Recurring Total Costs: $6400.00**

Installation Fees:

Given the wide area of locations where ETS will be marketed and used, it is expected that most organizations will have their own IT departments and use them to install ETS. Given a scenario where an organization does not have a dedicated IT Department, third-party CJIS compliant IT companies will be recommended by ETS to be used by agencies and organizations, at the cost of the organization.

Support Fees:

Automation and security have been focal points of the development team while creating ETS. Support costs and fees are expected to be minimal. Firmware updates to the sensors are installed remotely and automatically, as well as BIOS upgrades to the gateways. Aside from hardware failure, most issues and tickets can be resolved almost instantly, as ETS is able to access, configure and administer every gateway and sensor remotely. Agencies can change the sensor batteries themselves for minimal costs. If a sensor fails, agencies would disconnect the device, connect a backup sensor, and ship the offending sensor to our headquarters, where it would be inspected and either sent back to the manufacturer for a replacement or redeployed. Customer support and ticketing system will be available to agencies as part of the services provided by ETS.

**End-User Costs**

The end user will not be charged in any way. ETS will work directly with Law Enforcement Agencies and Police Departments. The agencies will be responsible for paying for the costs associated with adopting and implementing ETS within their department.

**Device Cost Estimate**

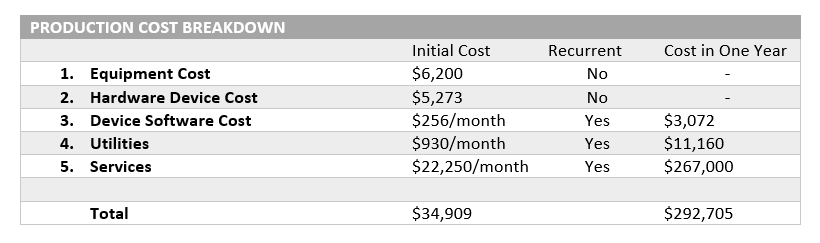
The device cost estimate is the estimate of all the costs and expenses of all hardware devices and device software for the development of ETS. The hardware devices needed include smart sensors, gateway devices, and tags such as NFC/RFID chips. The chosen sensor device, Abeeway Micro Tracker, has an average unit price of $80.70, with the average price for a hundred units being $8,070. The chosen gateway device is Dell Edge Gateway 3002, with a cost of $887.70. The tags to be used for identifying evidence vary in cost depending on the type chosen. NFC chips have an average unit price of $0.25, and the average price for a thousand units being $250. RFID chips have an average unit price of $0.10, with a thousand units costing $100. Both tagging options are affordable for the large numbers of evidence needed to be tracked.

The device software needed include VPN protocols, communication protocols, multi-cloud platforms and analytic software. OpenVPN is the chosen VPN protocol and software with an annual license fee of $15 per connected device. Pivotal Cloud Foundry is a multi-cloud platform provided as a web service by Pivotal which can be accessed for free. Pivotal also offers enterprise support for an average monthly fee of $43.20 or an annual fee of $520. For analytic software, Docker offers different versions at different prices. Docker Community Edition is free to use, while Docker Enterprise Edition is a premium version of the software which includes features that can help enterprises launch, manage, and secure their containers more efficiently with a starting price of $750 a year. Another analytic software, Kubernetes is an open-source container-orchestration system available for free. The ELK Stack of analytic tools include Elasticsearch, Logstash, and Kibana. This stack can be obtained through the Elastic website for free as an open source, a free basic plan, a gold plan, or a platinum plan.

The estimated total cost for hardware devices is $5,273. The estimated total cost for device software is $3072 in a year. The estimated production cost from both hardware and software devices is $8,273 in one year.

**Service Cost Estimate**

The service cost estimate is an estimate of all costs and expenses necessary to provide the services required by the customers and clients which include salaries of employees, specialists directly rendering the service, and the cost of facilities utilized in providing the service such as rental of equipment used and cost of supplies. The average salary of an application developer is $64,329 with a reported salaryrange of $43,530 to $100,303 per year a year. The average salary for an application administrator is $40,000 per year. The average salary of the employees will be around $36,000. Any specialist hired for the development process or for the maintenance process of the application may have an average salary of $51,000 per year. For needed equipment, tools, and services the minimum would be five workstations or computer systems, high-speed Internet access, desks and chairs, mobile devices for testing, office spaces. The estimated cost of technical equipment will be around $6200, a reliable and fast internet access averages at $100 a month, and office space has an average rent of $33.15 per square feet a month. The estimated total service cost is $267,000 in a year.



The estimated cost of production in one year is around $293,000. This total includes the cost of devices and the cost of services. This estimate will serve to determine the total budget needed to produce the application.

**APIs**

An Application Programming Interface (API) refers to an interface designed to receive a set of instructions from other software to which a response or interaction is generated. An API has an endpoint used to connect and request a variety of information. ETS uses its own API. Dependency of another API service might render the solution unusable in the event service is down or that the third-party vendor is compromised. Also considering the Personal Identifiable Information (PII) and confidential information ETS handles, ETS needs to remain secure and within its internal network. Specifically, it is suggested to use RESTful API format or Representational State Transfer which suggest a set of constraints and formats for the request and response to the API. This adds a security layer, formalizes all interactions and by using Swagger Files (files which contain responses from RESTful API) it allows for troubleshooting and building on existing features. Benefits of building our own APIs are, building to our own specifications, building with security as a priority, building to match hardware and solution specifics for optimal functioning and response times. While building APIs may be costly, money can be saved in the long run from not contracting vendors, third party support and securing our solution at the API layer as well. It is strongly advised given the nature of the data in transit that the APIs will handle, that the API is not open sourced. Open sourcing services will contribute to general knowledge and even further the possibilities for new features, in doing so allowing threat actors to analyze deficiencies and entry points to possibly compromise our solution. If a client wishes to comply with Open Source laws, it is recommended to be an Open Core or Partial Open Source. This refers to reviewed source code that does not disclose information essential, or that hints a malicious person on how the internal flow and operational order functions, allowing outsiders to compromise the confidentiality, integrity and availability of our APIs or solution.

Security

Device Hardware:

Abeeway Micro tracker: The Abeeway Micro Tracker uses LoRaWAN technology which uses 128-bit Advanced Encryption Standard (AES) algorithms. The trackers use end-to-end encryption using two keys. One of the keys is used to protect the contents of the payload and the other key is used network authentication security.

Dell Edge Gateway 3002: Uses Trusted Platform Module (TPM) 2.0 which allows support for newer encryption and hashing algorithms, BIOS verification that prompts for a password when accessing the BIOS, secure boot which checks the signature each piece of boot software to ensure no malicious activity and has a chassis intrusion switch that detects and indicates whenever there is unauthorized access when opening the chassis. In addition, the 4G capability of this device provides a redundant source of internet connectivity, which would improve operational availability and allow agencies and organizations to continue using ETS seamlessly in the event of internet connectivity failure.

Device Software:

Mobile Device Manager (MDM): MDM will allow the management of devices to be easier. MDM ensure devices are up to date with the latest updates and patches, devices are configured correctly with the appropriate group policies, allows for devices to be containerized to separate personal and work use and that devices can be remotely wiped or locked to protect all business information.

Virtual Private Network (VPN): a VPN ensures that data is moved in a secure manner. A VPN will encrypt data and send it through the internet, decrypt the data once it reaches the VPN network and then send the data to its destination.

Communications:

Data Distribution Service (DDS): DDS combines 5 Service Plugin Interfaces (SPI) to provide security for its systems.

* Authentication: provides authentication between participants by using a shared secret.
* Access Control: controls operations and the privileges on what users can perform.
* Cryptographic: utilizes encryption, decryption, hashing, digital signature and shared secrets.
* Logging: audits all security related events.
* Data Tagging: provides a means to add tags to sample data to improve search and discovery.

OpenVPN: OpenVPN uses a pre-shared static key between peers or uses SSL/TSL certificates for authentication. OpenVPN also uses up to 256-bit AES encryption using OpenSSL and can run over both TCP and UDP transports.

Cloud Platform:

Amazon Web Service (AWS): AWS provides numerous security features and capabilities, as it is compliant with Criminal Justice Information Systems (CJIS) Security Policy. AWS has built in firewalls that controls access to applications, encrypts data in transit using TSL, uses autoscaling and AWS Shield to mitigate DDoS attacks, monitor and logs activities, gives alert notifications for specific events or when thresholds are over capacity, provides identity and access control using AWS’ Identity and Access Management (IAM) and uses multi-factor authentication. Additionally, Key Storage & Management is handled by AWS CloudHSM, which allows ETS to generate, use and manage our own encryption keys for each client and the organization itself. These are generated using FIPS 140-2 Level 3 validated hardware.

Cloud Applications:

Cloud-based applications are, to an extent, secured by the security controls and mechanisms implemented at the Cloud Platform level. Using AWS Web Application Firewall (WAF), ETS protects its web applications from web exploits, particularly those which affect availability. Custom rules and new rules can be deployed almost instantly, allowing us to respond quickly and effectively to suspicious traffic patterns.

**Vulnerabilities and Threats:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Risk Severity | | | | |
| Risk Probability | Catastrophic | Critical | Moderate | Minor | Negligible |
| 5 - Frequent |  | Phishing |  | Password Attacks |  |
| 4- Likely |  | DDOS | MITM |  |  |
| 3- Occasional |  | Malware | Social Engineering | WIFI Jamming |  |
| 2- Seldom |  | Disgruntled Insider/Insider Threat | Remote Code Injection | Sensor Theft  Human Tampering/Error | Hardware/Connect-ion Failure |
| 1- Improbable | Advanced Persistent Threats |  |  |  |  |

Device Hardware:

Sensor Theft: AES encryption implemented by the sensors would mitigate any significant risk associated with this threat, as all data at rest within the sensor is encrypted. It is recommended that agencies acquire additional replacement sensors and keep them on site (to reduce shipping time delays). Connecting the new sensor to the existing infrastructure would not surpass an hour of downtime.

Gateway Uplink Failure (Damaged equipment, attacks on the agency internet connectivity access as well as WIFI jamming attacks) - 4G connectivity provides failover connectivity, allowing the gateway to continue operating normally.

Human Tampering/error: Damaged involving hardware can be either unintentionally through human error or on purposed by a disgruntled employee. The Abeeway micro trackers are very durable and has an IP64 water resistant rating and is ATEX zone 2 and 22 certified which makes it resistant to explosive atmospheres. Properly training employees on how to handle these devices would also reduce the chances for error.

Device Software:

Device Loss/Theft: With MDM, the affected device can be quickly purged from the authorized inventory device control list, which will not allow any further connections from the device. In addition, MDM allows ETS to quickly block access to the device and erase the device’s data to ensure confidentiality (and can be just as quickly restored if the device is found and was not tampered with).

Malware: Whether its ransomware, virus, worms or trojans; malware is malicious software that can come in numerous forms and runs harmful code that can interfere with the functions of systems.

Communications:

Man-in-the-middle (MITM): A man-in-the-middle attack is a form of eavesdropping and allows for the interception of communication. A MITM attack can come in the form of spoofing, sniffing, packet injections and session hijacking and attackers can capture valuable information by listening between parties. Using communication protocols like DDS that OpenVPN that uses high standard forms of encryption like AES prevents attackers from seeing traffic in plaintext and capturing and deciphering important data.

Social Engineering: the use of social tactics to gain inside and confidential information on an individual or organization. Attack vectors include baiting, pretexting and tailgating.

Phishing Attack/Stolen Credentials: phishing is when an email is used to trick users into entering their personal credentials into a website that is disguised as a legitimate website. Phishing attacks can be mitigated with proper training. Checking the legitimacy of the URL and checking if the website is running over HTTPS are some of the ways to prevent a phishing attack. WAFs can use an access-controlled list (ACL) to only a allow a list of trusted websites to be accessed through whitelisting.

Cloud Platform:

Distributed-Denial-of-Service (DDOS): a DDoS attack is when a targeted host gets flooded with request from a variety of sources which overloads it and makes its services unavailable. AWS has different services available to mitigate a DDoS attack like Amazon Route 53, Amazon CloudFront, Elastic Load Balancing and AWS WAF. These services combined with AWS Shield and use best practices to block unwanted request. AWS uses best practices to mitigate a DDoS like scaling applications based on traffic, decoupling applications to minimize the attack surface area and using constant logging and monitoring to detect anomalies.

Advanced Persistent Threats (APT): Highly advanced attacks that are usually sponsored by nation states. These attacks take advantage of zero-day exploits that have the capabilities to destroy entire infrastructure. Usually these attacks are well thought out, methodical and allows attackers to get unauthorized access to systems and remain in them for long periods of time without ever being detected.

Cloud Applications:

Remote-code Injection and Cross-Site Scripting: With AWS WAF, ETS can control traffic to our deployed web applications by defining specific rules, preventing traffic that could contain SQL injection attacks to our web application. WAF can be used to block common attack patterns

Password Attacks: using techniques like a brute force attack or a dictionary attack can allow attackers to authenticate as the user and gain access to applications. These password attacks can be subdued by salting and hashing passwords. Using salting algorithms like Argon2 and hashing functions like SHA-3 makes it substantially more difficult for attackers to guess passwords using these methods.

**Controls & Preventions**

Sensor Theft: In addition to the implementation of AES encryption by the sensors, an access control system can be implemented to monitor who has access to the sensors and when is this happening. Proper surveillance is recommended, as well as preparing sensor replacements to avoid any delays or disruptions to the working environment.

Gateway Uplink Failure: The 4G connectivity from Dell Edge Gateway 3002 provides a redundant source of internet connectivity which allows agencies and organizations to continue operations in case of an internet connectivity failure. Dell also provides Uplink Failure Detection (UFD) in its products, which detects the loss of upstream connectivity.

Device Software Loss/Theft: With the use of MDM, an access control can be established for the mobile devices that have the ETS application installed. In case of the loss or theft of a device, MDM allows for remote control, data wipe, and device lock. Files, contacts and email must be encrypted on mobile devices in the event of loss or theft.

Human Tampering/Error: Human error and tampering of devices is inevitable. The best way to reduce the chances of those errors occurring is through proper training. Training employees about the hardware, how to handle it and the procedures to take if something goes wrong prepares employees for all situations that might arise when dealing with equipment. Holding repeated training session not only re-enforces the importance of handling the equipment properly but also ensures that employees don’t forget the procedures involved. Ways to mitigate to damage is to have a disaster recovery plan in place for such failures.

Malware: Ways malware can be prevented is to by training users with best security practices like not downloading from non-trusted sites, clicking on suspicious links in emails, connecting to open WIFI networks etc. Additional ways to mitigate malware is to back up files in case they are compromised and to patch systems regularly.

Man-in-the-middle Attack: To prevent MITM attacks it is recommended to use a Virtual Private Network to encrypt web traffic. ETS will implement OpenVPN and DDS to prevent attackers from seeing traffic in plaintext and capturing and deciphering important data. To further prevent MITM attacks, an Intrusion Detection System (IDS) can be used to monitor the network or system for any malicious activity, and issue alerts when these malicious activities are discovered. The installation of an anti-virus software will also help prevent MITM attacks that rely on malware.

Social Engineering: Can be mitigated through proper training. Properly training employees on different social engineering tactics would help them recognize symptoms of an attack, prepare them on how to avoid such attacks and how to react to an attack.

Phishing Attack/Stolen Credentials: To prevent phishing attacks that could lead to the theft of credentials, the organization needs to educate the employees in recognizing suspicious emails, links, and attachments. Email filters can be used to flag any suspicious email.

Distributed-Denial-of-Service Attack: DDOS attacks can be mitigated by the implementation of different practices to block unwanted requests. One practice is to reduce the attack surface area to limit the scale of the attack. This can be achieved by using Content Distribution Networks that restrict direct Internet traffic to certain parts of the infrastructure. Another practice is to configure Firewalls which can be used to control what traffic reaches the applications and networks.

Advanced Persistent Attacks: it’s difficult to stop an APT but there are measures in place to help mitigate the damages. Making sure administrative controls like employee training are frequent and effective, have great quality physical security, implementing best practice security policies like frequent patching, secure coding, designing a secure network and having a good incident response plan can all mitigate the effects of an advanced persistent threat.

Remote Code Injection: ways to prevent remote code injection such as cross site scripting is to practice secure coding. Input validation ensures that data is being checked before entering the system. Validating that the code is in the matches the expected output prevents any malicious code from entering the system. Input sanitation can also be used to make sure that the given data conforms with an acceptable format.

Password Attacks: To mitigate common password attacks, Multi-Factor Authentication (MFA) can be used. In the case of a password being guessed correctly, MFA will ensure the attacker cannot have access to the system by stopping them with another authentication parameter. The practice of strong password requirements will help in making passwords more difficult to guess. Account lockouts are also recommended to prevent password attacks because this type of control will lock an account in the event of multiple failed authentication attempts.

# Standards and Regulations

Device Hardware: Members of Congress are introducing and trying to pass the S.734. Internet of Things Cybersecurity Improvement Act of 2019. Under this act, the National Institute of Standards and Technology (NIST) would develop guidelines that would set security requirements for government agencies to manage security vulnerabilities on devices. Since ETS works directly with government agencies, it is imperative that ETS is compliant with these standards. ETS incorporates IOT technology and voluntarily abides to the Internet of Things Cybersecurity Improvement Act of 2019 to encourage and promote increased security in IOT devices.

Device Software: The Geolocation Privacy and Surveillance Act (GPS Act) limits government surveillance using geolocation. The bill gives guidelines on how geolocation can be accessed and used. It mandates government agencies to obtain a probable cause warrant in order to obtain geolocation information. In addition, it prohibits companies from disclosing geolocation data about their customers without the customers consent. Since ETS incorporates GPS in our technology and is partnered with government agencies, it’s important that ETS is compliant with the rules and regulations of the GPS act.

Communications: The Federal Information Processing Standards (FIPS) is a standard developed by NIST to provide minimum requirements for federal information systems. Some of these standards include Secure Hash Standard (SHS) which specifies the standards of the secure hash algorithms. The Advance Encryption Standard is also a part of FIPS, and outlines approved cryptographic algorithms used to protect the confidentiality of data. All government agencies must be FIPS compliant. ETS uses DDS as one of its main communication protocols. ETS is compliant with FIPS 140-2 or the Security Requirement for Cryptographic Modules. OpenVPN can be FIPS 140-2 compliant if it is implemented with an algorithm that has a FIPS validation certificate, as is the case with our infrastructure provider, AWS. ETS adheres to NIST Federal Information Processing standard and uses the approved standards to ensure the highest level of confidentiality, integrity and availability.

Cloud Platform: The Criminal Justice Information Services and Security Policy (CJIS) was developed by the U.S Department of Justice to protect the life cycle of criminal justice information which includes creation, viewing, modification, transmission, dissemination, storage and destruction. ETS uses AWS and its compliant with all 13 policy areas which are Information exchange agreements, security awareness training, incident response, auditing and accountability, access control, identification and authentication, configuration management, media protection, physical protection, systems and communications protection and information integrity, formal audits, personal security and mobile devices. ETS meets the standards of CJIS.

Cloud Application: The Federal Risk and Authorization Management Program (FedRAMP) is a government wide program that provides standards for assessing, monitoring and authorizing cloud computing products and services. FedRAMP is mandatory for all government agencies and all cloud services. To be FedRAMP compliant an organization must be granted an Agency Authority to Operate (ATO) by a US federal agency or a Provisional Authority to Operate (P-Alto) by the Joint Authorization Board (JAB). In addition, NIST 800-53 compliancy is required which mandates a catalog of security and privacy controls for all federal information systems excluding national security. Also, passing a third-party assessment is also required amongst other things. ETS utilizes AWS which is compliant to all the conditions mentioned above, in doing so ETS adheres to FedRAMP and adopts levels of cloud security.

Communications Protocols:

Sensors D2D communications & Sensor to Gateway: LoRaWAN

Abeeway Micro Tracker Sensors implement 128-bit Advanced Encryption Standard (AES) algorithms, and a globally unique identifier (EUI-64-base DevEU) which are issued by the IEEE Registration Authority, for authentication. These vetted and recommended by the NIST (National Institute of Standards and Technology).

Data Distribution Service (DDS) will be used in between the sensors and the cloud servers.

Gateway to Gateway & Gateway to Cloud:

Gateway to Cloud:

All communications take place using HTTPS and VPN by implementation OpenVPN. OpenVPN uses up to a 256-bit OpenSSL encryption library and SSLv3/TLS v1 protocols to encrypt all data while in transit.

Product Compliance:

ETS sensors, manufactured by Abeeway. comply with California’s Senate Bill 327, which establishes the need for “reasonable” security features to protect collected PII from unauthorized access, use, destruction, modification or disclosure in all IoT devices.

State Laws regarding Data Breach Notification: Each U.S. State, as well as the Federal government have their own breach notification statutes, which ETS will strictly follow in the eventuality that PII is disclosed.

# Appendix A

# Incident Response Plan:

**Email Phishing Attack/Stolen Credentials**

This document discusses course of action upon the discovery of a Phishing Attack / Stolen Credentials. The plan aims for prompt and effective mitigation in the event of the outlined situation. Below departments/individuals will have contact information attached. Company staff will be trained in effective communication procedures. The information below outlines specific course of action organization wide.

1. Upon discovery or suspicion of falling a victim the involved individual will reach out to one of the below described individual/departments. In dependence this process may be faster and accessible. In the event the attack vector has been carried out via email, user will simply need to click a “Report Phishing” button in the suspicious email which will be automatically contained, routed to Cyber Incident Response Team and scanned/mitigated for similar instances received by other staff in the case an enterprise email solution is being used. Authorized individuals/departments to handle the situation highlighted above are:
   1. Helpdesk (Route to correct Department)
   2. Intrusion detection monitoring personnel (CIRT Team)
   3. A system administrator (Will escalate issue, take measures and advice next steps)
   4. A firewall administrator (Will escalate issue, take measures and advice next steps)
   5. A manager (Trained in response of said situation)
   6. The security department or a security person. (Security organization alerted to activate protocols in place to mitigate repercussions)

All the above-mentioned entities will have 24/7 access to respond or route issue to correct individual/departments to assist.

1. If the person discovering the incident is a member of the IT/Technology department or affected department, they will proceed to step 5.
2. If the person discovering the incident is not a member of the IT department or affected department, they will call the 24/7 reachable grounds security department at the provided number.
3. After the reception of an incident call, if deemed the individual’s credentials, system, or adjacent system has been compromised. The on-site security office will use the crafted key individuals contact list for IT/Technology Departments which will alert leadership staff of situation with the following details:
   1. The nature of the incident. (brief technical explanation and suggested steps for mitigation or protection)
   2. What equipment or persons were involved? (Departmental group only, names will only be disclosed to direct report of the involved individual)
   3. Location of equipment or persons involved.
   4. How the incident was detected.
   5. Countermeasure to take in case the contacted person is not sure on next steps.
4. The IT/Technology Staff involved (victim or discoverer) will promptly inform direct report, department leader, or reach security organization with details of event, including the following details:
   1. Email address
   2. Time/Date
   3. Description of how the event happen and any details noticed (script running, watering hole, page crash after login attempt, suspicious URL)
   4. As well as provide a copy of email to a secure inbox for analysis.
5. Leadership/Response Team will meet in person or virtually and discuss the event and determine a response strategy, including amount of possible damage and mitigation steps (system scans, security hardening, users check) other topics to be discussed are:
   1. Is the event a real or perceived threat?
   2. Is the incident a one-time event or affected multiple individuals?
   3. How critical is the affected credential/system?
   4. Impact level to the business operations (Minimal, Serious, Critical)
   5. System or systems affected via the lost credentials (Single Sign On (SSO), zero trust network, adjacent systems?)
   6. Is an urgent response needed?
   7. Will a third-party system owner need to be contacted?
   8. Can the incident be quickly contained?
   9. Can we trace back the origin of the attack, identify individual or group involved?
   10. Is the attack one small step to a bigger plan, or are there possibilities to change the vector? (Rootkit, Active Directory Traversal)
   11. Categorize the event (intrusion, phishing, insider threat).
6. An incident Ticket will be generated. This ticket will categorize and add a priority level:

Category One - A threat to sensitive data (Intellectual property (IP), PII (Personal Identifiable Information), CPNI (Customer Proprietary Network Information), PCI (Personal Card Information))

Category Two - A threat to computer systems (Was the attacker able to gain access to our network and systems)

Category Three - A disruption of services (Was business interrupted)

1. Based on the incident assessment involved teams and individuals in charge of response will respond following the below descriptions:
   1. Compromised credentials will be changed or deactivated following the path of any other system that also uses the same credentials
   2. Email will be analyzed to determine details like sender, intention, involved domain and gather as much intel as possible
   3. Similar emails received by other individuals and departments will be flagged and quarantined
   4. URL contained credential stuffing or phishing site will be blocked from access via Web Application Firewall
   5. Systems will be scanned for unusual activity, users check will take place to account for all users, and network traffic will be analyzed.
   6. Continuous monitoring will take place while investigation is ongoing.
2. If any further repercussions, systems or credentials are found to be compromised the response team will implement countermeasures to mitigate or reduce damage, forensic techniques, intrusion detection log audits, systems check, and employee interviews will be conducted to gather as much information as possible about the incident. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
3. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems. Changes may include credential refresh, forced password rotation and firewall rules hardening to accessing non trusted sites.
4. Upon management approval, the changes will be implemented
5. Documentation—the following shall be documented:

a. How the incident was discovered.

b. The category of the incident.

c. How the incident occurred, whether through email, firewall, etc.

d. Where the attack came from, such as IP addresses and other related information about the attacker.

e. What the response plan was.

f. What was done in response?

g. Whether the response was effective

1. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence if necessary, to complete prosecution and beyond in case of an appeal.
2. Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.
3. Assess cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

1. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
   1. Consider whether an additional policy could have prevented the intrusion.
   2. Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
   3. Was the incident response appropriate? How could it be improved?
   4. Was every appropriate party informed in a timely manner?
   5. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
   6. Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
   7. Have changes been made to prevent a new and similar infection?
   8. Should any security policies be updated?
   9. Lessons learned?

# Appendix B

# Privacy Impact Assessment

**For the**

E.T.S

(Evidence Tracking Solution)

**PIA-0##(x)**

**November 13th, 2019**

**Contact Point**

**Product Leader Contact Info**

**Business Name**

**Contact Information of Business**

**Reviewing Official**

**Acting Chief Privacy Officer**

**Abstract**

ETS (Evidence Tracking Solution) a pilot solution herein after referred to as “project” aims at providing law enforcement agencies a viable solution for tracking evidence in respect to cases by means of using sensors and a software platform to continuously query information in regard to said sensors and the adjunct item herein after referred to as “evidence”. The project is in response to a need for faster locating, processing and analysis of evidence collected by field officers, and presented in court while establishing a chain of custody that prevents tampering, misplacement and damage of evidence. The PIA is required to outline and show our commitment to regulations and the information we collect from users, surrounding environment as well as the information we store from sensors and platform. Given the level of priority and clearance needed to operate our solution we aim at fully complying with industry, federal and governmental guidelines.

**Overview**

The project collects PII information deemed necessary and already subpoena/cleared by a high-level law enforcement official to be in our possession. Other than what has been stated, the solution collects user information already within the internal law enforcement system, credentials needed to authenticate user. The team has taken every possible step to ensure information is contained within the internal flow and cannot be leaked, replicated, purged or modified by any outside agent. Protecting our secrets have been the core mindset during all the phases of the project. Some of the routine information collected can be found in the Data Section but may include date, time, location, user credentials, sensor ID, case ID, etc. The potential of a privacy risk comes when an unauthorized party attempts to disrupt, infiltrate or damage our infrastructure. While countermeasures are in place to deter bad actors, this iterative process is constantly looking at new vectors and actively patching, updating and protecting our data. Our projects, being a cloud-based application collects a vast majority of information which is protected at rest, or in transit by a layered security approach, we understand the importance of the data we handle and therefore have closely followed guidelines outlined in above sections to ensure safety and effectiveness.

**Section 1.0 Authorities and Other Requirements**

**1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?**

The Privacy Act of 1974 establishes guidelines for the collection, maintenance, use and spread of personal identifiable information (PII) about individuals that is maintained by federal agencies. The Privacy Act of 1974 includes 12 exceptions. These exceptions listed below provide the authorization of such information gathering.

* To officers and employees of agencies who have a need for the record for the performance of their duty.
* When a disclosure is made under the Freedom of Information Act.
* For an established routine that is part of the systems of record notice.
* If the Census Bureau is carrying out a survey.
* If advanced notification is made and the information is used for statistical research or reporting.
* To the National Archives and Records Administration for historical value.
* To another agency or governmental jurisdiction within the United States for a civil or criminal law enforcement activity, if the activity is authorized by law.
* To a person under strong circumstances affecting someone’s health or safety.
* To either House of Congress or subcommittee of congress.
* To the General Accountability Office.
* To the order of a court with acceptable jurisdiction.
* To a consumer reporting agency that is in accordance with section 31 U.S.C. &3711(f).

**1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?**

ETS works with government agencies that use their own government wide System of Record Notice (SORN).

* OSC/GOVT-1 - OSC Compliant, Litigation, Political Activity and Disclosure Files – 82 FR 45076:

**1.3 Has a system security plan been completed for the information system(s) supporting the project?**

Upon review of our documentation and demonstration of project we expect the Agreement to Operate (ATO) to be granted on November 21st, 2019. Anticipated date of reception for the Certificate and Accreditation (C&A) is the same as outlined before pending our project is recognized as complaint with DHS Management Directive 4300A and categorized as “moderate” under Federal Information Processing Standards Publication 199.

**1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?**

A record retention schedule is approved and existed by NARA. NARA is tasked with the preservation of government documents and makes such documents accessible to the public. ETS follows the guidelines of NARA’s General Records Schedule on finance, human resources, technology, information management, general operations support and mission support.

**1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

Not applicable, the Paperwork Reduction Act is only used by federal agencies to reduce the amount of paperwork that the government imposes on businesses and individuals. Although, ETS works with government agencies, it is solely the governments agencies responsibility to comply with the Paperwork Reduction Act.

**Section 2.0 Characterization of the Information**

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

**2.1 Identify the information the project collects, uses, disseminates, or maintains.**

Information is collected for two types of users of the project. The first category belongs to primary users, the second category belongs to guest users. Information is collected for two types of users of the project. The first category belongs to primary users, the second category belongs to guest users. Primary Users: Individuals with direct access to the project’s application primary features. These users can input data and start search queries. The information collected and stored from these users by the project include log in credentials such as usernames and passwords, evidence unique identifiers, evidence descriptions, location, name, email, activity logs, date and time of evidence retrieval, date and time of evidence delivery, date and time of evidence storage.

Guest Users: Individuals with restricted access to the project’s application. These users do not input data, they are only able to retrieve information regarding the evidence they need to work with. The information collected from these users include log in credentials, name, email, role in the prosecution process.

The project creates new information in the forms of analysis and reports. With the use of sensors, trackers, and devices’ built-in meters, the ETS application can collect information about the geographic location of every evidence that has been tagged and identified, as well as weather and climate information during the transportation of evidence. The purpose of this information is to be analyzed by an analytics team. The analysis of all this information will help improving delivery times and routes and help prevent any wrong handling of evidence during severe weather conditions. The reports being created consist of activity logs detailing the chain of custody of evidence, date and time of retrieval, delivery, or storage, and notification and alert reports.

**2.2 What are the sources of the information and how is the information collected for the project?**

The individuals providing the specific information are law enforcement officials, law enforcement evidence custodians, and crime scene technicians. Any other type of information not collected by the specified individuals, is being collected by technologies which include sensors, trackers, GPS, and mobile device’s built-in meters. Additional information may be collected from the law enforcement databases to provide information about the court cases for which the evidence is

The individuals providing the specific information are law enforcement officials, law enforcement evidence custodians, and crime scene technicians. Any other type of information not collected by the specified individuals, is being collected by technologies which include sensors, trackers, GPS, and mobile device’s built-in meters. Additional information may be collected from the law enforcement databases to provide information about the court cases for which the evidence is part of.

**2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

Commercial and publicly available data is used to provide analytics for customers, like estimated evidence transit times and location.

**2.4 Discuss how accuracy of the data is ensured.**

To ensure the accuracy of data, the project collects information from the authorized users who have been identified and given access to the project’s data input feature. Data gathered using technologies is checked by the standards of public data.

**2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** Some of the discussed risks for privacy are attributed to a data leak, insider threat, divulgation of information, or malicious actor attempting to disrupt service.

**Mitigation:** Some of the mitigations in place are backups to ensure integrity, authentication, tokenization and access control logs, strong company policy and leadership as well as backup systems, incident response plans and disaster recovery plans.

**Section 3.0 Uses of the Information**

The following questions require a clear description of the project’s use of information.

**3.1 Describe how and why the project uses the information.**

The project collects data that is also collected by legal means during investigation. The project shall be an extension of the ongoing investigation having the same rights as an officer would. Such information is used to relate a sensor to a case and ultimately having constant location on the supporting evidence. For more information on how data is collected and used please see “Data” section above.

**3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.**

Not Applicable, DHS will not be handling information contained within.

**3.3 Are there other components with assigned roles and responsibilities within the system?**

User Groups are defined by a need to know basis within ETS, and each has detailed responsibilities.

**3.4 Privacy Impact Analysis: Related to the Uses of Information**

It is up to the Law Enforcement agencies to enforce the controls implemented within ETS, with the help of consultants, if needed.

**Section 4.0 Notice**

The following questions seek information about the project’s notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

**4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

No notice is provided by the project. All notices all provided by officers and individuals on site who personally interact with victims and those involved in the process. Such notices are covered by investigation laws and procedures.

**4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?**

There is no option or consents to opt out, declining to providing information, given the nature of the issue the project aims to tackle any bit of information is crucial about the cases and sensors. Despite this, case officials ultimately decide what information will circulate our system independent from what the users provide.

**4.3 Privacy Impact Analysis: Related to Notice**

The project does not provide any beforehand notice to those involved or related to the cases. Only those performing duties and assigned to the case will be notified of any changes or modifications necessary for the correct functioning of processes.

**Section 5.0 Data Retention by the project**

**5.1 Explain how long and for what reason the information is retained.**

The retention of information regarding evidence complies to the laws and regulation of evidence followed by law enforcement agencies. The storage of evidence after a case can last for a minimum of one year to an indefinite period of time. The collected information from a piece of evidence will be retained as long as the evidence continues being tracked by the ETS system in case of a correction or reopening of a case.

**5.2 Privacy Impact Analysis: Related to Retention**

**Privacy Risk:** There are many risks that are can come when retaining records for a long period of time. First and foremost, the longer data is held, the more data is being stored. Having data for a long-time duration just opens it as a potential attack target and makes it that much more exposed to possible security breaches. With that in mind, it is ideal to keep data for as short of a time as possible while still complying to laws and regulations.

**Mitigation:** The risk can be mitigated by disposing data in a timely manner. Following NARA’s General Record Schedule gives guidelines on how long to keep certain information based on use and importance.

**Section 6.0 Information Sharing**

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

**6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.**

Information can be shared between participants involved in the court case. Whether it’s the FBI working with the CIA or a private sector company; information that includes geolocation, tracking logs and alerts are made available if that organization is a participant in the case. To access the information, participants would need the unique RFID tag on the items being tracked as well as the court case number.

**6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.**

External sharing is compatible with MSPB/GOVT-1 Appeals and Case record in the Government wide section of SORN. One of the purposes of MSPB/GOVT-1 is to locate physical or electronic files and to provide statistical reports. ETS provides live tracking and intricate statistical logs and reports on the status of items being tracked. Every item has a unique RFID tag that is being published to the Federal Registrar.

**6.3 Does the project place limitations on re-dissemination?**

The project is committed to sharing actionable intel/information across all law enforcement agencies when approved by a high-level officer and to the sole discretion of those in charge of said agencies. Limitations will be set by agency officials themselves.

**6.4 Describe how the project maintains a record of any disclosures outside of the Department**.

The project can track/recreate any desired record of disclosure or content based on departmental or governmental needs. This is made possible by our virtual backups which are insured and readily available.

**6.5 Privacy Impact Analysis: Related to Information Sharing**

The project only shares information within internal resources, any request for information sharing to any outside resource will be discusses with high level officials, isolated and monitored as part of agency agreements.

**Section 7.0 Redress**

**7.1 What are the procedures that allow individuals to access their information?**

By default, our system prevents users without clearance from seeing PII, which is masked by a sensor and case ID. Only cleared individuals will be able to see PII with supervisory permission which considers this person has no relation to the person/case in question hence assigned to work on said case.

**7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

An individual as part of the correct user group with clearance to modify erroneous information will be able to make such change. For this action to take place, said action needs to be cleared by a superior officer as well as the information deemed erroneous before any change is authorized.

**7.3 How does the project notify individuals about the procedures for correcting their information?**

There is no need for an individual to correct his/her information as our project uses already established credentials used by that specific individual. Should said individual need to modify the associated information to the credentials he/she should refer to their department or leader for detailed description of process.

**7.4 Privacy Impact Analysis: Related to Redress**

**Privacy Risk:** As stated above, there is no need for an individual to correct or change any information. Were users able to change information like a user credential, then it would pose a security and privacy risk. If a user changes his or her credentials, he or she is at risk of forgetting or losing any new credential, as well as creating a vulnerability to the authentication process of the application.

**Mitigation:** Any individual with access to the project’s application will have his or her own log in credentials which are determined by his or her department. Any information pertaining to each user is corroborated by the user. If any correction is needed, the individual must contact the department in charge of overseeing the user groups of the application.

**Section 8.0 Auditing and Accountability**

**8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?**

The project has been developed in according to standards like ISO and NIST which this PIA is based on as seen in our project documentation we clearly outline how the information is gathered, used and where it will finally reside. All these steps follow protocol and procedures in place to ensure the data and its surrounding infrastructure is protected.

**8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.**

We have established all privacy built in our project; users can seek further training by contacting us directly. Resources are freely available from federal, governmental, or private institutions like (NIST, ISO, and IEEE) just to mention a few.

**8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?**

User groups have been stated (See User Groups Section) We establish who is using the project by using credentials, authentication and which permission this individual has to interact with the solution.

**8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?**

All MOUs are reviewed by the program manager, component Privacy Officer, and counsel and then sent to pertaining authorities for formal review.

**Responsible Officials**

Involved Departments

**Approved Signatures**

Acting Chief Privacy Officer