ALL-IN-ONE EVIDENCE SECURITY PROTECTION SYSTEM

IOT PRODUCT DEVELOPMENT GROUP PROJECT

Table of Contents

Product Overview

In today's world of the criminal justice system high-value evidence has never been more important than it is now, but with the smart technology currently available it is easier to protect evidence integrity. Powered by IoT technology an all in one security system can protect evidence integrity, provide consistent availability, and give accurate accountability. The security system's foundation is built on portable lockers that provide physical security both on site, and during transfer of evidence to other locations. Smart sensors within these lockers will provide analytics to help provide insight on how the lockers are used, and if the evidence being stored properly. Metrics such as weight, temperature, and humidity can be monitored to provide real time updates on the status of all evidence within the lockers.

Working alongside the lockers there will be other sensors, and base stations placed throughout the facility to bring out the full potential of the security system. Base stations will act as securing station to allow evidence to be check in, checked out, and prepped for transfer to other facilities or case trials. Attached to these base stations will be a terminal to allow authorized users to automate the process of getting evidence assigned to them in and out of the base stations. In the evidence rooms and forensic labs where these base stations will be held there will be other sensors tracking movement, humidity levels, facial recognition, and the current location of the evidence lockers. To give thorough security the proximity sensors will also be placed throughout the entire facility providing real time updates of evidence lockers' location.

To give law enforcement ease of access to the security system there will be cloud applications paired with it to be able to view, and analyze the data collected. Users will be able to view graphs, logs, and the current inventory from their mobile phone or computer from any location. Authentication measures are also implemented into this cloud application to provide the peace of mind that only the allowed users will be able to access the different parts of the security system. These measures will also play a part on what users will have access to physically within the facility. With this security system it will give the peace of mind to help those in the criminal justice system continue to provide service to their community.

Potential Benefits

The advancements in technological systems in the criminal justice system have proved beneficial since they have simplified the previously tedious work of tracking down criminals and providing better evidence to support court cases. Vital components like DNA testing, fingerprint databases, and GPS tracking have proved to be critical in court cases for prosecutors and defendants to secure fairness and justice in the ruling. Various individuals and professions, including law enforcement, judges, prosecutors, defendants, and falsely accused criminals, have benefitted substantially from the new technology wave. Therefore, it is imperative to note that technological advancements have improved quality and service efficiency in the criminal justice system. Smart sensors' introduction proves to be essential in protecting high-value evidence in a criminal court case. This has its beneficial implications on both end-users and the organization of application like the police station or district attorney when protecting evidence for a criminal court case.

Potential Benefits to the End User

Preservation of evidence remains a crucial priority in the criminal justice system. This is critical to ensure the defendant's due process is observed and their rights are respected as prescribed in the sixth and fourteenth amendments in the constitution. Attorneys usually question evidence credibility based on the method of collection and preservation integrity. This is why law enforcement facilities will need a system in order to provide secure accessibility to evidence in order to ensure evidence integrity is kept. Installation of the system

will help law enforcement to automate and track the use of all evidence with the smart sensors within the system. By utilizing the smart sensors, evidence can adequately be secured right from the appropriate facility to ensure no evidence tampering. Everyone who encounters the evidence will be logged with what precisely the change process was. This could be placing the evidence into storage, or police staff providing evidence to the labs or third-party officials. The criminal justice department can improve its public trust and approval rating by adopting modern technologies that will enhance the integrity of the evidence for various cases, which will further ensure fairness in the ruling of all matters handled by the department.

Potential Benefits to the Organization

The implementation of smart sensors remains key in every criminal justice system evidence room to uphold integrity in protecting and preserving evidence. Maintaining the integrity in evidence protection and preservation aligns with the international laws and regulations to protect human rights and civil liberties.

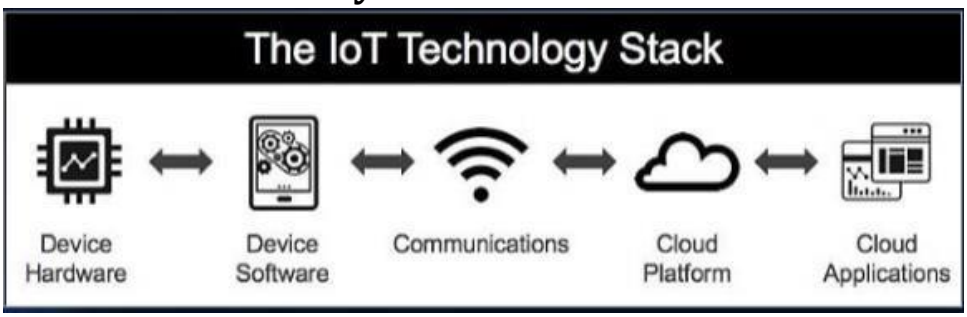
Primary Users

Law enforcement personnel would be the individuals that would have primary access to enter the evidence room with proper authentication. These users would be the ones in charge of entering evidence into the system, keeping track of all activities and alerts within the evidence room. Along with those responsibilities, this user will also use the system when moving evidence between sites and for cases. The system will play a key role in their day-to-day duties since evidence custodians are the primary handlers of evidence for cases.

Secondary Users

Forensic personnel will be using the system in an indirect way by analyzing and testing the evidence that the primary users will manage and log. Lawyers need to know that the evidence is safe and secure from any evidence tampering or destruction. This will be provided by the tracking and logging of all authorized users that interact with the evidence. With this system it can help prevent accidental or intentional improper handling of evidence.

System Features and Functionality



Backend Requirements

Within the device hardware of the IoT stack, lockers will be available in different sizes to be able to fit evidence inside. Each locker will be fitted with a deadlock mechanism, and keypad for physical security controlled by the current state set by users. Smart sensors embedded in the lockers will work together with receivers throughout the facility to provide collected data to the local database system to add to the analytics of the assigned asset in the asset database to then be uploaded to the cloud. Local access to the system will be hosted by a local database to provide availability in the case the internet or cloud platform goes down. Rooms containing base stations will have access card sensors that authorized users will need assigned cards in order to

enter. The rooms will also contain cameras fitted with facial recognition sensor capabilities watching over each of the base stations and their terminals. The functionality these sensors provide encompass the device software portion of the IoT stack.

Customer-Based Requirements

Within the system there will be two front-facing applications that users can access which are the asset database, and admin console. With the admin console users will be able to create and set up user credentials for cloud access, access cards, and associated passcodes. The admin console will also allow users to set up alerts for sensors based on the set thresholds desired. Alerts can be configured for email, text, and cloud application notifications. It will also provide the capabilities to add, configure, and monitor sensors within the system. Users who have access to the admin console can also view log files on a per user basis, and have complete control of the live environment of system giving them the ability to stop or start different areas of the system when needed. The asset database acts as an inventory system for authorized users to be able to add, edit, actively track and checkout any of the evidence that is put into the system. Users will be able to access all of these functions as long as they are connected to the local network of the system. View of the asset database will be available through the cloud application for tracking, alerts and personal user settings that can be accessed from a PC or Phone to provide instant availability to where a user might need it. The terminal attached to base stations will give authorized users access to see the evidence currently assigned to them, and whether another user has it checked out. In the base station terminal authorized users will also be able to change the status of evidence lockers.

Understanding the Data

Data Collection Chart				
Input Device	Type	Examples of Data	Result	Data Location
Admin Console	Text/Numeric	Name, Number, Employee ID, Address, Email, Birthday, Department, Staff Type, Access Card ID	User Profile	Cloud and Local Database
Admin Console	Input	Alerts, Sensor Thresholds, System Status, Card Assignment	System Configuration	Local Database
Asset Database	Text/Numeric	Item Name, Case Number, Locker ID, Type, State of Locker	Asset Entry	Cloud and Local Database
Locker Terminal	Input	Login Credentials, State of Locker	Access to System	Local Database
Locker	Sensor Data	Temperature, Item Weight, Humidity, Acceleration, Keypad Usage	Analytic Logs	Cloud and Local Database
Locker Keypad	Input	Passcode	Access to Evidence	Temporary
Base Station Rooms	Sensor Data	Facial Recognition, Video Feed, Temperature, Humidity, Location, Access Key Usage	Analytic Logs	Cloud and Local Database
Cloud Applications	Input/Sensor Data	Login Credentials, GPS Location	Access to Asset Database, and Case Transfer Mode	Cloud Database

With using this system there will be data collected automatically by sensors, and some manual input by authorized users of the system. As shown in the chart above the manual input required by users will be used for profile creation, system configuration, and access to the system both locally and through the cloud. From the backend of the system sensors will collect their respective data in order to create logs, and analytics for authorized users to view from the asset database. These sensors are embedded into the locker, and placed throughout the facilities. A key example of this are the two lock systems attached to the lockers which include a keypad, and a deadlock. When using the Case Transfer mode every time a user either inputs in the correct or

wrong code the evidence locker will first process the data for authentication. Then the evidence locker will log the time of each attempt to upload it to the local database once it returns to the facility.

Besides the lockers there are two more major key data collectors which are the cloud applications, and the sensors within the base station rooms. Along with the manual input data mentioned before the cloud applications will also collect data in order to audit when a user logs in, incorrect authentication attempts, and any other actions taken within the cloud applications. This data is required for the logs within the admin console that track what and when changes are done by a user to provide accountability. Within the base station rooms there are two key elements their sensors contribute. The first element is the facial recognition captured by the cameras within the room. The second element is the access card portion of the system which collects input data on who tried accessing the different base station rooms, and at what time.

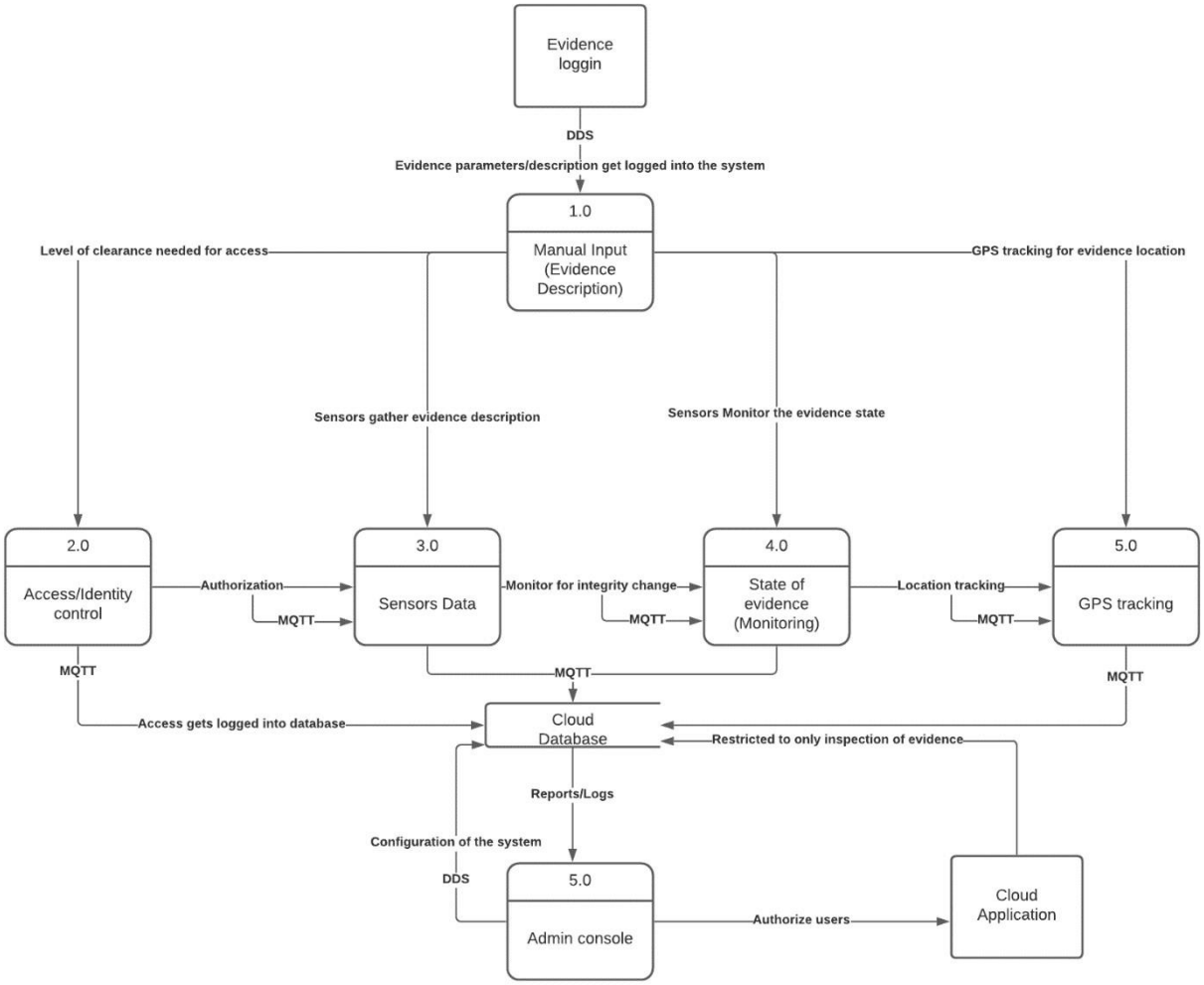
Data Input Responsibility

All authorized users would be required to input information for user accounts that will be used within the system in order to have access to evidence and evidence related data relevant to their assigned case. This will include data provided by themselves, and other primary and secondary users such as the forensic lab personnel.

Access to Collected Data

Real-time data should only be given access to evidence custodians, and upper management of the facility. Evidence custodians will need this data in order to perform day to day operations, and to keep track of evidence when performing transfers. Management will also need access to this data in order to ensure proper chain of custody is being followed. Secondary users should only be given access to historical data related to their assigned case.

Data Flow Meets User Requirements



The system will provide users with a seamless integration of all devices that comprise the solution. The IoT stack provides 5 layers of a range of technologies, standards, and applications that will all be used to develop our solution to meet the customer requirements. The data that is gathered by the system will flow through all 5 layers of the IoT stack. The first pieces of data that will initiate this process will be manually inputted by the user who does the initial inspection of the evidence, after that there will be 5 processes that will work together to create a better understanding of such data to be able to monitor for integrity change, sensors will be able to maintain the state of the evidence, and use GPS technology to track the location of the evidence.

In process one, the user will input data of the evidence for the sensors to understand what values to expect and monitor such as weight, temperature, dimensions, and other evidence features the initial logger might have included. In process two, the sensors will start to monitor the evidence with the base parameters provided by the initial logger of the evidence. In process three, the sensors will use all the data gathered to check the state of the evidence and log any person that uses their access to inspect the evidence. In process four, GPS tracking will let evidence room administrators know if the evidence is being taken away without

authorization and also track for any suspicious movements that might trigger an alarm or notification on the system. After the first four fundamental processes are completed the data will get transferred to the cloud database for storage and creating reports about the state of evidence, monitoring, alerts, and tracking of the evidence. After all of the data is passed to the cloud database process five will come into place. This is where the admin console will generate reports and logs for authorized users to view.

Evidence State Chart			
Desired State	Purpose	Previous State Needed	State Changed From
Stored	Storage in Base Station	First Time Asset, or Any Transfer State	Asset Database, or Base Station Terminal
Intra-Site Transfer	Transfer Within Facility	Stored	Base Station Terminal
Inter-Site Transfer	Transfer Between Facilities	Stored	Base Station Terminal
Case Transfer	Transfer for Court Hearing	Stored	Base Station Terminal

As shown in the evidence state chart above there are four different states evidence can be in that serve different purposes. When adding evidence for the first time to the system the state must be changed through the asset database during the initial creation. Evidence set to the Intra-Site Transfer mode cannot be removed from the facility. If an evidence locker is not detected by receivers during this state the system will automatically send an alert to the configured user. When in Case Transfer mode evidence lockers will be assigned a 24-hour temporary passcode to use on the keypad to access the evidence. Authorized users using Inter-Site, or Case Transfer mode are required to use the GPS feature on their phone in order to provide realtime updates on where evidence should be during transit.

The solution is expected to provide customers with a secure environment for evidence storage, transportation, and inspection. All the effort is being focused on meeting the customer requirements of security and evidence integrity.

Data Analytics Processing

Since most data is collected from sensors automatically and the data being collected is time-sensitive, edge analytics would be more beneficial. Edge analytics will collect, process, and analyze the collected data at the network's edge, close to the sensors. If data were to be analyzed only in the cloud the data would be latent. Using edge analytics reduces latency, is scalable to the amount of data collected, and cuts down on bandwidth use and cost. With data like temperature, humidity, weight, and acceleration, it is imperative to know the real-time data. If anything, unexpected happens, alerts can sound as to which data set has changed, and critical actions can be taken in real time.

The ability for edge to scale to the amount of data will be important as the number of devices grows to accommodate evidence storage and monitoring; edge analytics can accommodate a site's growing processing and analytics. Real-time data from the numerous sensors on each device will grow exponentially, taking up bandwidth resources when transporting data to and from the edge to the cloud. When the data stays on the edge of the network, there is no need for the data to travel any further, saving bandwidth and reducing costs.

Data Analytics

Common types of analytics are used in IoT applications, including descriptive analytics, predictive analytics, and prescriptive analytics. Descriptive analytics is used to analyze historical data, which is then organized and presented in an easy way to understand. This be most ideal for the security system since the aim is to ensure the evidence's integrity. It can also be used in the evidence operations to report easily and gain insights on the stored evidence's status.

Predictive analytics predicts possible occurrences in the future by analyzing past data patterns and trends from historical data. This is useful for organizations to plan effectively, manage risks and set realistic goals. Predictive analytics will help the employees responsible for managing evidence since they will use past data analytics to improve their operational procedures and reinforce stored evidence's integrity. Prescriptive analytics tells organizations the actions that they should take based on the data available to them. The prescriptive analysis relies on both descriptive and predictive analysis to recommend the best possible course of action. It is not very easy compared to the other two analytics. Therefore, it is rarely used in daily operations since the security system auditors could use such prescriptive analysis to help the management employees improve their evidence storage operations.

Access to Data Analytics

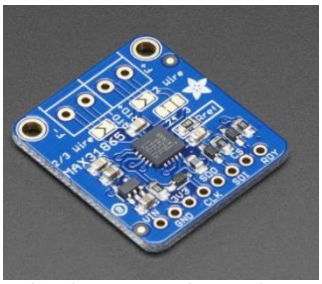
The defense lawyers, the accused, and the prosecution lawyers should have access to both historical and real-time data related to their associated cases since the integrity of the evidence can be deduced from data. The security personnel at the evidence warehouse should have real-time access to the data to observe any unusual trends, and to record who interacts with the data. The judge should have privileges to access both historical and real-time data for easy judgment.

Component Selection

Sensor Devices

Adafruit 3328 - Temperature Sensor

This is a tiny temperature sensor that is also known as a thermistor. It can detect temperature changes quickly and provides accurate readings. This type of sensor has been used in laboratories for many years. A single unit costs $14.95



https://www.arrow.com/en/products/3328/adafruit-industries

TDL110 Transport Data Logger

The transport data logger has tilt, shock, and temperature sensors, and it will record the various parameters once attached to the evidence. Each of the various parameter limits can be modified individually, which will make it easier to trace any transgressions of these limits within the course of storage of evidence. The gadget reinforces the monitoring of the evidence, and it enhances data collection. The device can be connected to smartphones easily via Bluetooth for sharing of data. It costs $122.46. Despite its capabilities the device is manufactured by Bosch, a German company, and hence it must be imported.

https://www.arrow.com/en/products/0273.600.024/bosch

TESEO-LIV3R GPS Receiver

This gadget will be used to report the current location of the evidence lockers. The location sensor can operate within -40oC and 85oC, and this is within the operating temperatures of the other sensors. The sensor can support 3.6 volts for normal operation, and hence it can use the same power supply as the other sensors. A unit costs $13.56.

https://www.arrow.com/en/products/teseo-liv3r/stmicroelectronics

82635D435IDK5P 999AFR Cameras

The RealSense Depth Camera has a field view of 90o, and it can stream up to 90-fps at 1920 x 1080pixel resolution. A total of four cameras will be required to cover all fields of view at the evidence locker. The camera has a range of depth determination of 10 meters, and it integrates an inertial measurement unit (IMU) that allows six degrees of freedom. The operating temperature range of these cameras is 0-50oC, and they require 5V and 700 mA in the power supply. A single unit costs $251.92, and the total cost for four cameras will be $1007.67. Although the camera is relatively costly, it will be ideal for monitoring the evidence lockers since it will provide both facial and object recognition.

https://www.arrow.com/en/products/82635d435idk5p-999afr/intel

SEN-14728 Weight Sensor

This sensor will be used to determine the weight of the evidence inside of the storage lockers. If there is any changes to the weight, an audit alert will be generated in the system. This sensor can translate up to 500g into an electric signal which will tell the Yanzi gateway device the weight of the evidence. A unit costs $10.

https://www.arrow.com/en/products/sen-14728/sparkfun-electronics

Gateway Devices

Yanzi IoT Gateway 2

This gateway backup solution was chosen due to its ability to support autonomous operations even when the internet is down. It ensures safe storage of sensor data in local storage and enables reliable and secure cloud communication with the IoT devices. The gateway has a built-in battery backup that can operate for hours during a power failure. The gateway also communicates with sensors directly to check their status, and this occurs over a secure encrypted network. It has an internal 32GB SD card that can store at least 30 days of sensor data. It can support up to 300 sensors. The power supply can support 12V and 2A output, which can power all other components. The gateway supports both cellular and wireless networks. It has 2 Ethernet ports and one USB port. A unit costs $600. Pricing is available by directly contacting the manufacturer.

https://www.yanzinetworks.com/solution/

Storage

Little Giant – Heavy-Duty Mobile Storage Locker with Handle

A portable heavy duty mobile storage locker with a handle to easily transport and provide physical security both on site, and during transfer of evidence to other locations. This locker provides good visibility and air circulation. It has wheels which can make it easy to load into a storage van or warehouse. It can support up to 2000lbs and has 2 center shelves for storage. A unit costs $1325.62.

https://www.zoro.com/little-giant-mobile-security-locker-36x72-2000-lbs-handle-2-center-shelves-sc2-36726py-1h/i/G7461038/

Local Servers

The local server will depend on the enterprise size of the client. All hardware and storage levels will have plenty of room to expand if more storage is needed for either DB or CCTV footage

Enterprise Level	**Small**	**Medium**	**Large**	
Hardware	Dell PowerEdge VRTX w/ 2 M630 blade	Dell PowerEdge VRTX w/ 3 M630 blade	Dell PowerEdge R6515 Rack Server x 3	
OS	Microsoft Server 2019			
CPU	12-Core Intel E5-2680v3	12-Core Intel E5-2680v3	32-Core AMD EPYC 7542 900GHz	
RAM	96 GB DDR4	256 Gb DDR4	512 GB DDR4	
OS/DB Storage	2 x 800 GB SSD	2 x 3.2 TB SSD	2 x 480 GB SSD for OS	
CCTV Storage	6 x 6 TB HHD	6 x 12 TB HHD	See SAN Storage	
SAN Storage	-	-	PowerVault ME4084 Storage Array	
			2 x 3.84 TB SSD for DB	26 x 12 TB HDD for database

Each hardware specification is per blade.

Communication Protocols

Message Queue Telemetry Transport Protocol (MQTT)

MQTT protocol is designed for Machine-to-Machine communication, and it finds ideal application in remote tracking in IoT. Its primary goal is to gather data from various gadgets by connecting the gadgets and

networks with packages and middleware. All the devices will be connected to the concentrator servers. MQTT will be the main data protocol for the sensor devices and for transmitting telemetry data into the cloud. It is a lightweight protocol with a fast response time that makes interactions between our devices efficient, it ensures smooth data transfer with low bandwidth and reduces the load on CPU and RAM.

Data Distribution Service (DDS)

DDS protocol offers the most versatility and it is an open standard technology that can be integrated with any environment either M2M or server and receive data from the cloud. Communication is peer-to-peer DDS is excellent for managing networks, maximize scalability, increase reliability, minimize latency, and reduces cost/complexity. DDS will be used as the underlying managing data protocol for the network to ensure our solution can scale, have multivendor application operability, efficient use of network resources, practical long-term architecture lifecycle and it is a future-proof international standard that eliminates proprietary stovepipes.

Cloud Platform

The services provided through the platform would be Azure Active Directory (AD) and Azure SQL database. Offering these services through the Azure platform would provide high availability and scalability for the client. The local server would replicate both AD and the asset database from the cloud, allowing authorized users to access the database in a cloud outage. Azure AD would enable the creation of authorized user groups to allow access to the Azure SQL database that would store the evidence location, information, and tracking.

Analytic software

Azure Analysis will be used to analyze data with tools like Power BI and Excel. The appropriate user such as management will be provided analytics showing the average number of times each authorized user will go into a base station, and the average amount of time authorized users stay in the evidence room. Other analytics provided include the average amount of time the evidence spends outside the lockers, which will be detected based off the weight sensor registering no weight within the locker. The system will also provide analytics based on the average time from the starting facility to a locker's destination when authorized users use Inter-Site, and Case Transfer mode. All the activities for the month will be included on a per user and facility basis.

Mobile Application

The system's cloud application will be using Microsoft's Azure App Service for cloud application hosting. Azure App Service provides minimal latency, and downtime for users to ensure high availability. It allows authorized users to communicate with the system from any PC or mobile device. Combining Azure App Service, and Azure SQL Database to host the entire cloud system will provide users with secure access to the system using Azure AD SSO for credentials. Authorized users will be able to access the cloud application through a web browser allowing it to be compatible with Windows, Mac, and Android operating systems. Through the application users will be sending personal data as shown in the data collection chart for log purposes. The system will then send asset database data and alerts based off their permissions. Access to the web application will only be available on phones, tablets, and PCs to give a better viewing experience.

Costs

Overall Recurring Charges			
Item Name	Minimum Cost	Max Cost	Pay Frequency
Azure App Service	$146	$219	Monthly
Azure SQL Database	$2,666	$7,111	Monthly
Azure Analysis	$3,000	$6,000	Monthly
Azure Firewall	$912	$950	Monthly
Security System Software	$3,000	$3,000	Yearly
Maintence Contract	$15,550	$15,550	Yearly
Training Contract	$3,500	$3,500	Yearly
Total*	$102,738	$226,410	

*Total includes monthly cost for the year

Overall One Time Charges			
Item Name	Minimum Cost	Max Cost	Pay Frequency
Lockers	$1,325	$7,500	Per Unit
Cameras	$890	$4,360	Per Unit
RFID Readers	$36	$52	Per Unit
RFID Tags	$2	$6	Per Unit
Dell Server	$7,107	$53,000	One Time
GPS Reciever	$12	$25	Per Unit
Data Logger	$122	$250	Per Unit
Temperature Meter	$180	$375	Per Unit
IoT Gateway	$600	$1,500	Per Unit
Weight Sensor	$11	$32	Per Unit
OS License	$972	$972	One Time
SQL Server License	$899	$13,748	One Time
Site Visits - Non Contract	$300	$300	One Time
Individual Training	$500	$500	One Time
Total	$12,956	$82,620	

The above tables represent a high-level overview of minimum to maximum cost. The primary way to demonstrate value to the customers is to highlight the ease of evidence tracking, data logging, and security

through automation, requiring fewer people to check-in/out the evidence and less paperwork that comes along with evidence movement.

Example Cost

Exam ıle Recurring Charges				
Item Name	Minimum Cost	Quantity	Extended Cost	Pay Frequency
Azure App Service	$146	1	$146	Monthly
Azure SQL Database	$7,111	1	$7,111	Monthly
Azure Analysis	$6,000	1	$6,000	Monthly
Azure Firewall	$950	1	$950	Monthly
Security System Software	$3,000	2	$6,000	Yearly
Maintence Contract	$15,550	1	$15,550	Yearly
Training Contract	$3,500	1	$3,500	Yearly
Total*			$195,534	

*Total includes monthly cost for the year

Example One Time Charges			
Item Name	Minimum Cost	Quantity	Extended Cost
Lockers	$1,325	70	$92,750
Cameras	$890	20	$17,800
RFID Readers	$36	4	$144
RFID Tags	$2	70	$140
Dell Server	$7,107	2	$14,214
GPS Reciever	$12	70	$840
Data Logger	$122	70	$8,572

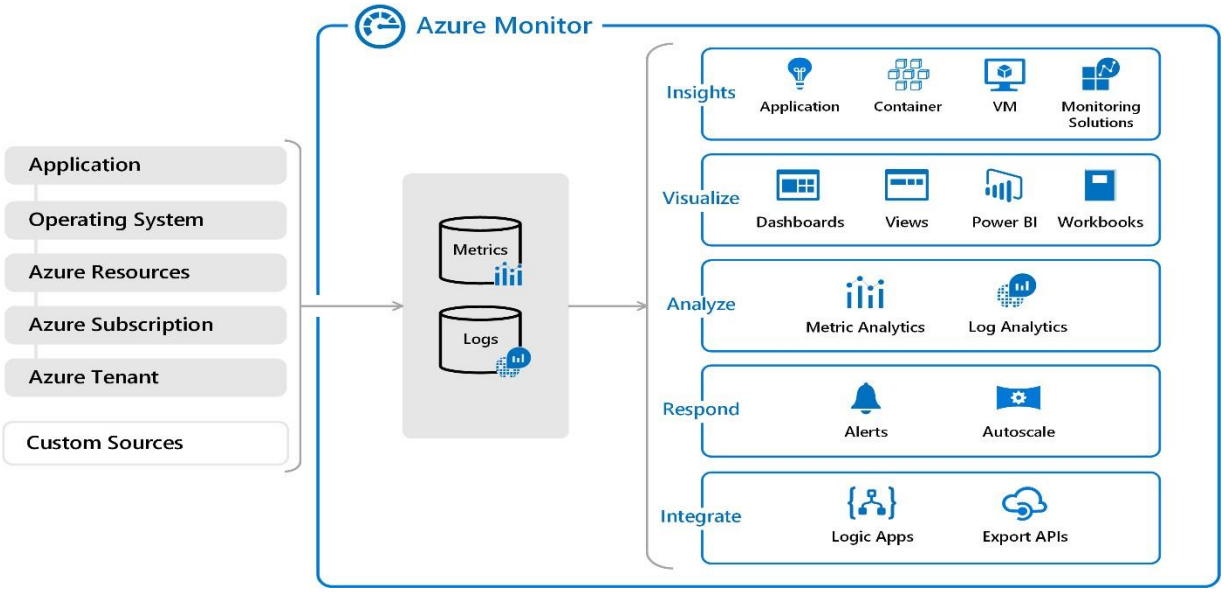
Temperature Meter	$180	70	$12,600
IoT Gateway	$600	70	$42,000
Weight Sensor	$11	70	$735
OS License	$972	2	$1,944
SQL Server License	$899	2	$1,798
Individual Training	$500	1	$500
Total			$194,037

The above charts represent a law enforcement agency with two small facilities under their plan. Their plans will start off with 70 users from the agency as well as 30 free slots for new employees and third parties such as lawyers. In each facility there will be two rooms covered with five cameras and an RFID transponder installed. Each site will include 35 lockers with one local database server running at each site. To ensure protection of the equipment and services of the system the agency will purchase a maintenance contract. The agency will also send six employees to have individual training to learn how to properly configure and maintain the system functionalities.

APIs

The solution will be using the existing API offered by the Azure cloud infrastructure that offers reliability and has a strong reputation for working with industry-leading organizations. Azure Monitor API offers numerous ways of creating calls and deploying solutions with standard technologies like ASP.NET, NODE.js, PHP, Java, Python, and HTML.

- Azure Monitor: This API will offer full visibility into the sensors, applications, infrastructure, and network. Here are some more important features Azure Monitor API offer.
    - Monitoring Data Platform: Data collected fits into two categories, metrics, and logs. Metrics are numerical values that support real-time scenarios and describe some aspect of a system at a particular point. Logs contain data organized into records with different sets of properties for each type. Telemetry data is stored as logs.
    - Autoscale: It allows the solution to have the right number of resources running to handle the load on the infrastructure and applications. Provides the ability to create rules that use metrics collected by the Azure Monitor API to determine automatically when to add resources when load increases.
    - Alerts: Proactive notifications of critical conditions and potentially attempt to take corrective action. Alert rules use action groups that contain unique sets of recipients and actions that be shared across multiple rules. ○ Dashboard: Combines different kinds of data into a single pane and gives the option to share statistics with other users.



Risk

Risk Probability	Risk Severity				
	Catastrophic A	Critical B	Moderate C	Minor D	Negligible E
5- Frequent			Insecure data transfer		
4- Likely	Insecure network services	Insecure API, and web app			
3- Occasional		Lack of secure update mechanism			
2- Seldom	Weak and guessable passwords Misconfiguration	Lack of physical hardening Human error	Inadequate privacy protection	Accidental damage	
1-Improbable	Power Outage			Vandalism	

Catastrophic Vulnerabilities

- **Insecure Network Services:** When left unpatched or on an outdated standard, network services can be left to be exploited by hackers using vulnerabilities that were fixed in the newest updates. This will likely lead to catastrophic damage to a facility possibly giving full access to the system, or data being transferred by these network services. To mitigate the possibility of these exploits the system will be equipped with forced system updates to all IoT devices.

- **Weak and guessable passwords**: Attacks might include the use of techniques like brute force attacks, recycled passwords, and large-scale breaches that might expose previously used passwords by a user. Weak passwords can lead to a security breach allowing the attacker to gain access across the company's systems. Some controls might include the creation of strong password policies that might include password rotations, minimum length, complexity, and account lockouts.
- **Power Outage:** In case of total power failure, the system will be rendered ineffective since it relies on power for its functionality. There is a power backup to ensure continuous system operation.
- **Misconfiguration:** During the initial system setup, there may be errors in changing default system settings during the commissioning stage, which leaves loopholes for attackers. Such errors may occur during system updates. There should be a series of checks by different system specialists to ensure whatever was missed by one person is captured by another person.

Critical Vulnerabilities

- **Insecure API and Web App:** With cloud applications, if improper coding techniques are used without protection it will let hackers have to ability to use attacks such as cross-site scripting or SQL injections. Hackers would then likely be able to cause critical damage by either manipulating, or gaining access to the cloud database for all users through these attacks. The damage can then be mitigated by using a combination of Azure Firewall's services, and proper coding techniques.

- **Lack of Secure Update Mechanism**: When using an automated update system, hackers can send out fake updates through the use of DNS spoofing, TCP Hijacking, or AP impersonation. This can occasionally lead to critical damage to the IoT devices causing them to fail from these fake updates by the Evilgrade attack. To help prevent attacks from happening updates will be required to be signed with a certificate to be approved for deployment. Sensors will also be equipped with self-healing capabilities to recover from fake updates in the case of a successful attack.

- **Lack of physical hardening:** This refers to the likelihood that the IoT devices may have weak default settings that could be exploited. Allows a potential attacker to gain information that can help in a future remote attack or take control of the device. The best control for hardening is to protect in various layers or take a defense-in-depth approach. This means protecting the host, application, OS, user, physical, and all sublevels.
- **Human Error:** As people interact with the system regularly, there is a chance that error through actions such as accidental exposure of passwords can make the system vulnerable. Besides, social engineering

attacks against the system are affected through the system users. It is necessary to remind and train the system users on necessary user behaviors to ensure security of the system.

Moderate Vulnerabilities

- **Insecure Data Transfer**: This vulnerability normally occurs when using communication protocols without any type of encryption to protect data being transferred within the network. If this is not taken care of it could lead to potential frequent man-in-the-middle attacks that would leak user, and company info. To prevent this from happening the system will implement control measures including MQTT payload encryption, and DDS security plugins to protect data transfers between IoT devices.

- **Inadequate privacy protection:** Occurs when sensitive information of customers or the business gets compromised. Attackers can cause integrity damage to such data and the company can be subject to fines by regulatory institutions. Some recommended controls are to record all important operations regarding data so that any anomalous activity can get identified later.

Minor Vulnerabilities

- **Vandalism:** Thieves, burglars, or even insiders can break into the systems and attempt to steal valuable evidence. The damage can include the loss of important evidence pertaining to files and exposure of evidence that belong to active cases. The recommended controls are to have physical security such as man traps, guards, and authentication methods to access the evidence room.

- **Accidental damage:** This usually refers to human error possibilities. Some of the damage might include broken hardware, evidence integrity change, or loss of function. To prevent accidental damage is important that a policy defines what the company considers to be accidental damage and provides a guide on how to report such incident.

Government Regulations and Industry Standards

The federal government has been implementing regulations to guide IoT devices' design and use since they are used to collect data about people within its jurisdiction. The state of California has made significant strides in IoT regulations. Under the state security law SB-327, it is illegal for IoT device manufacturers to include a "reset to factory settings" option for all devices. The law further bans the use of default passwords on IoT devices. Lastly, the law requires IoT device manufacturers to include security features for all devices to protect them and any information collected by such devices against unauthorized access, modification, or disclosure.

IoT Cybersecurity Improvement Act of 2020 was enacted to govern the development and manufacture of IoT devices. The Act was implemented to increase usage of IoT devices by government agencies for

surveillance and collecting environmental data. However, the Act has implications on both private and corporate use of IoT devices. Under the Act, the National Institute of Standards and Technology (NIST) has the mandate of developing security standards and guidelines for the appropriate use and management of IoT devices. In the second provision of the Act, contractors are obliged to disclose their systems' information security vulnerabilities to federal agencies and their resolutions. The information should be reported and disseminated within 180 days of discovery. The final provision of the Act prohibits any agency from procuring and using any IoT device that does not comply with NIST standards and guidelines.

PROFINET is an industry-standard for data communication that could be used since it has been designed for collecting data while also controlling equipment in industrial systems. The product will be collecting information from the users. Io-Link is also another powerful standard that will be used since our product will need to communicate with other sensors.

Appendix A: Incident Response Plan for a Weak and/or Guessable Password

This document discusses an incident response plan for an account with a weak password and that has been compromised by an attacker.

1) If the person discovering the incident is not a member of the facility's internal IT department or affected department, they will call the 24/7 help desk department at 555-1234.
2) If the weak password is reported to the help desk by the account holder, proceed to step 4.
3) If an alert for a weak password or possible malicious account activity has been logged, proceed to step 5.
4) The help desk analyst will refer to the IT emergency contact list and call the designated numbers in order on the list. The analyst will log:
    a) The name of the caller.
    b) Time of the call.
    c) Contact information about the caller.
    d) The nature of the incident.

e) Account type involved.

g) How the password was changed.

f) If any suspicious activity has been noticed on the account.

5) The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using email and phone messages while ensuring other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the help desk analyst in the previous step. The staff member could add the following:

   a) Is the account affected business-critical?

   b) What is the severity of the potential impact?

   c) Name of account, along with account privileges, type of account, and account owner.

   d) Any information about the origin of where the account is being accessed.

6) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.

   a) Is the incident real or perceived?

   b) Is the account being used by a threat actor?

   c) What data or property is accessible with the account and how critical is it?

   d) What is the impact on the business should the account gain higher privileged access? Minimal, serious, or critical?

   e) What other account or systems can be targeted? Where are they located physically and on the network?

   f) Is the incident inside the trusted network?

   g) Is the response urgent?

   h) Can the account be quickly contained?

   i) Will the response alert the attacker, and do we care?

   j) Were there additional attacks that were performed with the compromised account? If so, what type of incident were they? Example: phishing, brute force, dictionary attack, rainbow table, etc.

7) An incident ticket will be created. The incident will be categorized into the highest appropriate level of one of the following categories:

   a) Category one - A threat to public safety or life.

   b) Category two - A threat to sensitive data

   c) Category three - A threat to computer systems

   d) Category four - A disruption of services

8) Team members will establish and follow one of the following procedures basing their response on the incident assessment:

   a) Weak/guessable password

   b) Brute force password attack

   c) Information breach

d) Active intrusion response procedure

e) Inactive Intrusion response procedure

f) Account abuse procedure

The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

9) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses—the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

10) Team members will recommend changes to prevent the occurrence from happening again or allowing weak/guessable passwords.

11) Upon management approval, the changes will be implemented.

12) Team members will restore the compromised account to a safe state. They may do any or more of the following:

    a) Changing the weak password.

    b) Make users change passwords if passwords may have been sniffed.

    c) Be sure the password has been hardened by following password requirements.

    e) Be sure real-time virus protection and intrusion detection is running.

    f) Be sure the accounts are logging the correct events and to the proper level.

13) Documentation—the following shall be documented:

    a) How the incident was discovered.

    b) The category of the incident.

    c) How the account access occurred, whether through email phishing, brute force, 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.

14) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

15) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the attacker is possible. List the agencies and contact numbers here.

16) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the containment efforts' cost.

17) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

    a) Consider whether an additional policy could have prevented the account access.

b) Consider whether a procedure or policy was not followed, allowing the account access, and then considering what could be changed to ensure that the procedure or policy is followed in the future.

c) Was the incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the incident-response procedures detailed, and did they cover the entire situation? How can they be improved?

f) 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.?

g) Have changes been made to prevent a new and similar account access?

h) Should any security policies be updated?

i) What lessons have been learned from this experience?

Appendix B: Privacy Impact Assessment

Privacy Impact Assessment for the

All-in-One Evidence Security Protection System

March 25th, 2021

Contact Point

Andres Alvarez

Abstract

The abstract is the single paragraph that will be used to describe the program and the PIA. It will be published on the DHS web site and Federal Register. It should be a minimum of three sentences and a maximum of four, and conform to the following format:

- First sentence should include the name of the component and the system, technology, pilot, rule, program, or other collection (hereinafter referred to as "project"). Note: There are some instances where system is specifically called out.
- Second sentence should be a brief description of the project and its function.
- Third sentence should explain the reason the program is being created and why the PIA is required. This sentence should embody the same analysis that caused the project to be identified as a "privacy sensitive system" in the PTA, such as the project requires PII or the technology is privacy sensitive.

The All-in-One Evidence Security Protection System is an IoT security system is meant to benefit law enforcement facilities. The purpose of this system is to provide protection, and mobile security for law enforcement to use with evidence. The project is considered a privacy sensitive system, because of the sensitive information the system holds for case trials.

Overview

The overview creates the foundation for the entire PIA. The overview provides the context and background necessary to understand the project's purpose and mission and the justification for operating a privacy sensitive project. Include the following:

- Describe the purpose of the system, technology, pilot, rule, program, or other collection (hereinafter referred to as "project") the name of the Department Component(s) who own(s) or is funding the project, the authorizing legislation, and how it relates to the component's and Department's mission;
- Describe how the project collects and uses PII, including a typical transaction that details the life cycle from collection to disposal of the PII; and

Describe the recommendation for how the program has taken steps to protect privacy and mitigate the risks described in the previous bullet. Note: Do not list every privacy risk in the succeeding analysis sections. Rather, provide a holistic view of the risks to privacy.

Additionally, consider the following as appropriate to the project:

Describe the funding mechanism (contract, inter-agency agreement) that the project will operate under:

Describe any routine information sharing conducted by the project both within DHS components and with external sharing partners and how such external sharing is compatible with the original collection of the information;

Analyze the major potential privacy risks identified in the analysis sections of the

PIA and discuss overall privacy impact of the program on individuals; and

Identify the technology used and provide a brief description of how it collects information for the project.

- The solution/Product put in place aims to protect evidence about cases and maximize the level of physical and digital security around evidence rooms and valuable items belonging to active/past investigations.
- The solution put in place will require minimal PII information to be stored and used in active scenarios where a person needs to be confirmed as an active authorized user to access the evidence room and any lockers/bags containing evidence. The same logic will apply for physical interaction as well as for the cloud application.
- The team developing the solution has put privacy at the forefront of the solution. The systems have secure data protocols like MQTT, DDS, and Microsoft Azure monitor API for maximum protection of data in transit. There is also full accountability of possible risks to the system in the security phase with a full study of the security conditions of the product that include Risk Matrix, categorization of vulnerabilities with description/damage/control, and an incident response plan developed before the solution is deployed.

Additional considerations:

- The funding mechanism being used will be of contract type. Once the solution has been approved by the client/agency the team will proceed with the deployment of the solution upon the required timelines of the client.
- Some extra information is shared with 3rd parties include telemetry being gathered by the solution and system monitoring conditions. Most of this data will be shared through our cloud partner in this case being Microsoft Azure.

- Potential privacy risks have been identified and outlined in the security section of the project proposal. Overall privacy impact for individuals only includes authorized personal who would be the main individuals impacted in case of a privacy breach.
- The solution will gather sensor telemetry in real-time and verify the identity of users trying to access the evidence via physical or through the cloud application. All of this information will be collected into the solutions databases and will be used to provide logs and reports for review later.

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?

List all statutory and regulatory authority for operating the project, including the authority to collect the information listed in question 2.1. Explain how the statutory and regulatory authority permits collection and use of the information. A simple citation without more information will not be sufficient for purposes of this document and will result in rejection of a Privacy Impact Assessment. You must explain how the statutory and regulatory authority permits the project and the collection of the subject information. If the project collects Social Security numbers you must also identify the specific statutory authority allowing such collection.

If you are relying on another component and/or agency, please list their legal authorities.

Where information is received from a foreign government pursuant to an international agreement or memorandum of understanding, cite the agreement and where it can be found (i.e. website).

Example: Section 4011 of the Intelligence Reform and Terrorism Prevention Act of 2004, 49 U.S.C. § 44903(h)(4) (2004).

Not Applicable

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

For all collections of PII where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a SORN in the *Federal Register*. Include the *Federal Register* citation for the SORN. If the information used in the project did not require a SORN, explain why not.

In some instances, an existing SORN (program specific, DHS-wide, or Governmentwide) may apply to the project's collection of information. In other instances, a new SORN may be required.

Not applicable

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

Provide the date that the Authority to Operate (ATO) was granted or the date it is expected to be awarded. An operational system must comply with DHS Management Directive 4300A. Note that all systems containing PII are categorized at a minimum as "moderate" under Federal Information Processing Standards Publication 199. If the project does not trigger the C&A requirement, state that along with an explanation.

For a new project provide anticipated date of C&A completion. If the project does not include technology, state that here.

Yes, the security plan has been completed

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

The project manager, in consultation with counsel and the component records management officer, must develop a records retention schedule for the records contained in the project that considers the minimum amount of time necessary to retain information while meeting the needs of the project. After the project manager and component records management officer finalize the schedule based on the needs of the project, it is proposed to NARA for official approval. Consult with your records management office for assistance with this question if necessary. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule.

Note: All projects may not require the creation of a new retention schedule. Not applicable

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

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.

Identify (1) the categories of individuals for whom information is collected, and (2) for each category, list all information, including PII, that is collected and stored by the project.

This could include, but is not limited to: name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code, facsimile number, mother's maiden name, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, medical records, device identifiers and serial numbers, education record, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic.

Primary and secondary users' data will be collected only for authorization purposes. The data includes name, role in the organization (Forensic or law-enforcement personal), photographic face recognition, and RFID badge assigned.

If the project or system creates new information (for example, a score, analysis, or report) describe how this is done and the purpose of that information.

The system will create reports and logs that will mostly contain information regarding access, telemetry, and geolocation history of the evidence. Access information is gathered through multiple verification methods that include facial recognition (999AFR Cameras) and a unique RFID badge assigned to each authorized user. Telemetry data will be gathered by the sensors (TDL110, Adafruit

3328) deployed in the evidence bags/lockers that will monitor for any state change to the evidence. Geolocation tracking will be performed by the GPS receiver (TESEO-LIV3R) and will provide real-time evidence of evidence location.

If the project receives information from another system, such as a response to a background check, describe the system from which the information originates, including what information is returned and how it is used.

The system will only receive responses from the cloud database provider (Azure) related to telemetry, access, and location logs/reports. All of this data is originated locally in the evidence rooms but the cloud database will provide a configuration panel which is the admin console that will have the ability to modify and configure these requests as the clients deem necessary.

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

A project may collect information directly from an individual, receive it via computer readable extract from another system, or create the information itself. List the individual(s) providing the specific information identified in 2.1.

If information is being collected from sources other than the individual, including other IT systems, systems of records, commercial data aggregators, and/or other Departments, state the source(s) and explain why information from sources other than the individual is required.

In some instances, DHS may collect information using different types of technologies such as radio frequency identification data (RFID) devices, video or photographic cameras, and biometric collection devices.

- Primary and secondary users will provide personal information to be authorized by the system to inspect the evidence. Facial recognition and RFID badges for authentication will be used for final authorization and access into the evidence room.
- Other sources of information include the telemetry gathered by the sensors. All of this data will be specific to the state of the evidence which will include geolocation, temperature, weight, and transport data. The data collected by these devices will be aggregated into logs/reports for future review by the system administrators in the admin console.

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 data includes information from data aggregators such as Choice Point or Lexis Nexis, where the information was originally collected by a private organization for nongovernmental purposes, such as marketing or credit reporting.

Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.

State whether the commercial or public source data is marked within the system.

Example: The commercial data is used as a primary source of information regarding the individual. Alternatively, the commercial data is used to verify information already provided by or about the individual.

Most data being collected by the system will originate locally within the perimeters of the evidence room and by the manual input of the initial evidence loggers. The remaining data collected by the system will come from the cloud applications used by authorized users, and the sensors within the facility including data such GPS location. The solution now does not use any public or commercial sources for data. The solution will have the ability to request public data such as court decisions to determine whether a case has been closed but this decision is entirely up to the client and will require future implantations to the existing solution put into place, default settings of the solution will not use any commercial/public data.

2.4 Discuss how the accuracy of the data is ensured.

Explain how the project checks the accuracy of the information.

Describe the process used for checking accuracy. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why.

Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

Example: The project may check the information provided by the individual against any other source of information (within or outside your organization) before the project uses the information to make decisions about an individual.

The solution will only check for the accuracy of the information within the organization for the authorization process. The system will check authorization with existing records of the authorized person within the organization with facial recognition, RFID badges, and names. The first process in the dataflow of the solution is the authorization process if any of the steps required to verify a user fails then the solution denies permission to the evidence bags/lockers and sends an alert to the system of an attempt to access the evidence by an unauthorized user.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Consider the following Fair Information Practice Principles (FIPPs) below to assist in providing a response:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for DHS to ensure that personally identifiable information is accurate, complete, and current?

Follow the format below.

Privacy Risk:

- Insecure Data Transfer: This vulnerability normally occurs when using communication protocols without any type of encryption to protect data being transferred within the network. If this is not taken care of it could lead to potential frequent man-in-the-middle attacks that would leak user, and company info.

- Inadequate privacy protection: Occurs when sensitive information of customers or the business gets compromised. Attackers can cause integrity damage to such data and the company can be subject to fines by regulatory institutions.
- Insecure Network Services: When left unpatched or on an outdated standard, network services can be left to be exploited by hackers using vulnerabilities that were fixed in the newest updates. This will likely lead to catastrophic damage to a facility possibly giving full access to the system, or data being transferred by these network services.
- Misconfiguration: During the initial system setup, there may be errors in changing default system settings during the commissioning stage, which leaves loopholes for attackers. Such errors may occur during system updates.
- Weak and guessable passwords: Attacks might include the use of techniques like brute force attacks, recycled passwords, and large-scale breaches that might expose previously used passwords by a user. Weak passwords can lead to a security breach allowing the attacker to gain access across the company's systems.
- Insecure API and Web App: With cloud applications, if improper coding techniques are used without the protection it will let hackers have to ability to use attacks such as cross-site scripting or SQL injections. Hackers would then likely be able to cause critical damage by either manipulating or gaining access to the cloud database for all users through these attacks.

Mitigation:

- Insecure Data Transfer: To prevent this from happening the system will implement control measures including MQTT payload encryption, and DDS security plugins to protect data transfers between IoT devices.
- Inadequate privacy protection: Some recommended controls are to record all important operations regarding data so that any anomalous activity can get identified later.
- Insecure network services: To mitigate the possibility of these exploits the system will be equipped with forced system updates to all IoT devices.
- Misconfiguration: There should be a series of checks by different system specialists to ensure whatever was missed by one person is captured by another person.
- Weak and guessable passwords: Some controls might include the creation of strong password policies that might include password rotations, minimum length, complexity, and account lockouts.
- Insecure API and Web app: The damage can then be mitigated by using a combination of Azure Firewall's services, and proper coding techniques

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.

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

Example: A project needs to collect name, date of birth, and passport information because that information provides the best matching capabilities against the terrorist screening database.

The only information being collected and maintained besides the sensor telemetry will be the information provided by primary and secondary users, for authorization purposes this will have to be verified with the internal database of the person who works in the organization and then will have to be verified with the cloud database to determine if they have the authorization to access the evidence bags/lockers. The project will collect names, photographic images for facial recognition, and RFID badges with access for verification. All the information collected will be used to be able to create reports/logs for the system administrators as well for any detection of anomalous behavior or create alerts by any attempt by an unauthorized user to access the evidence room.

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.

Many projects sift through large amounts of information in response to user inquiry or programmed functions. Projects may help identify areas that were previously not identifiable and need additional research by agents, analysts, or other employees. Some projects perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

Discuss the results generated by the uses described in 3.1, including a background determination, link analysis, a score, or other analysis. These results may be generated electronically by the information system or manually through review by an analyst. Explain what will be done with the newly derived information.

Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to

government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Example: The system will generate a response that there is a possible match to the terrorist screening database. This possible match will be maintained in the system with the information previously provided by the individual. A trained analyst will review the possible match and make a determination as to whether or not the individual is on the list. This determination will also be maintained in the system.

The results of the data collected will end up being fitted into reports, logs, and alerts that give administrators the ability to perform any changes to the configuration of the system as they deem necessary. All of the access will be recorded with photographic evidence for facial recognition, name, and RFID badge for confirmation of the verified individual trying to access the evidence. The sensor telemetry data will provide information crucial for the alerts, logs, and reports so the administrators can know if anything has changed with the state of the evidence. All the information being collected will be subject to individual analysis by the system administrators via the admin console. Administrators will have the final say regarding adjustments and configurations to the system.

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

Discuss the intra-Departmental sharing of information (CBP to ICE). Identify and list the name(s) of any components or directorates within the Department with which the information is shared.

Example: Certain systems regularly share information because of the crossover of the missions of the different parts of DHS. For example, USCIS employees regularly use a CBP system to verify whether an individual has entered the country. USCIS employees note that the CBP system has been checked and the date on which it was checked, but do not copy the information to the USCIS system.

Not applicable

3.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

Follow the format below

Privacy Risk: Unintended information collection

Mitigation: All information collected by sensors in data lockers is intended and does not gather any other data. The data collected is pertinent to the evidence and active case.

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.

In many cases, agencies provide written or oral notice before they collect information from individuals. That notice may include a posted privacy policy, a Privacy Act statement on forms, a PIA, or a SORN published in the *Federal Register*. Describe what notice was provided to the individuals whose information is collected by this project. If notice was provided in the *Federal Register* provide the citation, (e.g. XX FR XXXX, Date).

If notice was provided in a Privacy Act statement, attach a copy of the notice for review. Describe how the notice provided for the collection of information is adequate to inform those impacted.

Consult your privacy office and legal counsel on issues concerning the notice to the public for an information collection such as a form.

If notice was not provided, explain why. For certain law enforcement projects, notice may not be appropriate – this section of the PIA would then explain how providing direct notice to the individual at the time of collection would undermine the law enforcement mission.

Notice is given in the form of data collection from evidence lockers, being a known key feature. Users will also be given notice during the cloud account creation process before sign up is complete.

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

This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice.

Additionally, state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/he information. If specific consent is permitted or required, how does the individual consent to each use?

If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate in the project.

There is no option to opt-out of data collection. The evidence locker's data collection is a key feature of the product and is available to both plaintiff and defendant, court, evidence custodian, etc.

4.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

Principle of Individual Participation: Has the program provided notice to the individual of how the program provides for redress including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

Follow the format below.

Privacy Risk: Inadequate privacy protection

Mitigation: All data information is recorded to capture all anomalous activity, discovered and corrected. The defendant would be aware of the locker's data and information regarding evidence provided by the defendant's lawyer.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection

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

The purpose of this question is to identify the specific types of information the project retains. Is all the information the project collects retained? Is there a specific sub set of information retained?

Example: A project may collect extensive PII initially for the purpose of verifying the identity of an individual for a background check. Upon completion of the background check, the project will maintain the new information, the results of the background check (approved/not approved) and delete all application information.

This section should explain the nexus between the original purpose for the collection and this retention period. The minimum amount of information should be maintained for the minimum amount of time in order to support the project.

Example: The project retains the information for the period of time in which fraud could be prosecuted and then the information is deleted.

In some cases, DHS may choose to retain files in active status and archive them after a certain period of time. State active file retention periods as well as archived records, in number of years, as well as the approved or proposed NARA records schedule. Discuss when the time periods begin for inputs, outputs, and master files. Project managers should work with component records officers early in the development process to ensure that appropriate retention and destruction schedules are implemented.

Information is retained for an active/open case for as long as the case is open. Any archived data information is then stored for a varying time that varies between different jurisdictions. Company retention is up to 10 years or the retention period the jurisdiction dictates, whichever is less.

5.2 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated?

Although establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

Follow the format below.

Privacy Risk: Possible loss of data integrity

Mitigation: Only necessary data should be stored per retention period. Data should only be stored in a non-editable state. If data integrity is lost, company retention can provide a copy of the data.

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.

Discuss the external Departmental sharing of information (for example, CBP to FBI). Identify the name or names of the federal agencies and foreign governments.

Example: Customs and Border Protection may share biographic information on an individual with the Federal Bureau of Investigation in order for FBI to conduct a background check. Alternatively, USVISIT may share biographic and biometric information with the intelligence community in order to identify possible terrorists.

For state or local government agencies, or private sector organizations list the general types rather than the specific names.

Example: The program shares information with state fusion centers that have a posted privacy policy. In particular, discuss any international agreements that require information sharing as part of normal agency operations

Information is shared with law offices representing the defendant's active criminal or civil court cases. The information is shared through a web portal for current information. Data collected would also become a public record if the data is presented in court.

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

Note which routine uses support the sharing described in 6.1 related to normal business operations.

Example: Routine use H allows DHS to share biographic information with the FBI to conduct a background check. This is compatible with the original collection because the Immigration and Naturalization Act (INA) requires that USCIS determine whether an individual has committed any disqualifying crimes. Without checking with the FBI, DHS would be unable to meet this requirement of the law.

Not applicable

6.3 Does the project place limitations on re-dissemination?

Describe any limitations that may be placed on external agencies further sharing the information provided by DHS. In some instances, the external agency may have a duty to

share the information, for example through the information sharing environment. But, before disclosing the information to the individual the external agency is required to verify with DHS.

Data sharing from defendant lawyers would vary by jurisdiction and would be dictated by local law.

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

Under subsection (c) of the Privacy Act, DHS must retain an accounting of what records were disclosed to whom, even for systems that are otherwise exempt from certain provisions of the Act. A project may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the program must be able to recreate the information noted above to demonstrate compliance. If the project does not, explain why not.

In the system there are logs kept in place to track when an external user accesses data. These logs are saved to the cloud, and local database for authorized internal users to view later on. The following information is tracked in the access logs:

- User ID
- Date and Time of Access
- Case ID of Asset
- Asset ID
- Public IP
- Type of Device

With the user ID, authorized internal users can match that with the systems records to find their address and full name.

6.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the Department. How were those risks mitigated?

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

Follow the format below.

Privacy Risk: Sharing information with individuals outside of the facility can lead to potential data leak privacy risks. Outside individuals are given cloud access to the system to view information in preparation for court trials. Having this information freely available can have sensitive information viewed by unauthorized individuals.

Mitigation: To mitigate any privacy risks from happening with outside individuals the system has two sets of controls in place. The first control set is the use of two-factor authentication to prevent any unintentional data leaks by potential attackers. The second control set is a contract formed between the facility and any third-party individuals. The contract states that if any information from within the system was to be intentionally shared with unauthorized individuals then the third-party individual will be held legally responsible for such action.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Describe any procedures or regulations your component has in place that allow access to information collected by the system or project and/or to an accounting of disclosures of that information. Generally speaking, these procedures should include the Department's FOIA/Privacy Act practices. If the Privacy Act does not apply, state why this is the case. If additional mechanisms exist, include those in this section. For example, if your component has

a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the Department's procedures.

If the system is exempt from the access provisions of the Privacy Act, explain the basis for the exemption and cite the Final Rule published in the Code of Federal Regulations (CFR) that explains this exemption. If the project is not a Privacy Act system, explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information.

To provide access to users to their information in accordance to the Privacy Act, the cloud application allows users to view any of their related information automatically. This information includes any personal data needed for account creation, and all associated case data that is assigned to the user.

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

Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If the correction procedures are the same as those given in question 7.1, state as much. If the system has exempted itself from the provisions of the Privacy Act, explain why individuals may not access their records.

In the case information needs to be corrected within the system, there are two procedures an individual must follow. If an individual has to change personal information, these changes can be performed through the user's profile within the cloud application. If the information needed to be corrected is related to assigned evidence, or a case then a request for change form must be submitted through the cloud application. Once a form is submitted it can take up to twenty-four hours to be approved, and have the new information reflected. If additional information is needed for the approval then the user will be contacted by the appropriate department.

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

Individuals may be made aware of redress procedures through the notices described above in Section 4 or through some other mechanism. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are weakened significantly.

Example: Some programs provide the information related to redress in a letter when an individual is given an initial negative determination regarding receiving a particular benefit. This would give the individual clear notice of how to address possible problems with the information the Department holds on him. Other programs depend upon a notice in the workplace rather than direct notice to the individual, so redress may be more difficult for the individual.

To properly notify individuals on how to correct their information the system will send an automated email out after the initial creation of their cloud access account. Within the email the following topics will be address:

- How to change personal information within the cloud app.
- How to submit a request of change form for case/evidence information.
- Details on the time frame it will take for a change to be reflected in the system.
- Details on the process if a request needs further information or is denied.

7.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Example: If a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

Follow the format below.

Privacy Risk: With allowing individuals the ability to view, and change any records related to their account inside the cloud application there leaves the possibility to a privacy risk. This risk includes the possibility of an unauthorized user logging into the account to then view or make changes to the individual's information. The procedure to contact individuals if more information is needed, or a request is denied can have a privacy risk as well. If being contacted through an email that is compromised, this can give the unauthorized user further information that might not be in the cloud application.

Mitigation: To mitigate these potential privacy risks there are two sets of security controls as part of the system. The first security control set is the requirement of complex password and two-factor authentication. This will help prevent unauthorized users hacking into an individual's cloud account from a separate device. The second security control set is proper validation of an individual. This will be used to mitigate information being leaked from follow up or denial of change processes. Instead of sending an email, authorized personnel would be required to give a call to the individual requesting the change. Once the call is answered the authorized personnel will ask the individual one of three security questions that were set by the individual. These questions are only allowed to be change through a request form from the app, and require phone call authorization to prove identity.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

Auditing measures are recommended and should be discussed, but other possible technical and policy safeguards such as information sharing protocols, special access restrictions, and other controls should be discussed here as well.

Do the audit measures discussed above include the ability to identify specific records each user can access? Describe the different roles in general terms that have been created to provide access to the project information. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Explain whether the project conducts self audits, third party audits, reviews by the Office of Inspector General or Government Accountability Office (GAO).

Does the IT system have automated tools to indicate when information is possibly being misused?

Example: If certain celebrity records are accessed, a supervisor is notified and reviews to ensure that the records were properly used.

The system contains self-auditing features that track when users logon, access assets, and make changes within any applications. There are settings in the system that allow authorized users to set alerts when certain audit conditions are met. Settings are customizable

to work with all of the system on site, or within the cloud. Within the system there are three access groups as described below:

- **Full Access**: Gives users permissions to read and write information in the system, and check out evidence assigned to them while on site. When using the cloud application to access the system users will only have read permissions.
- **Staff Access**: Gives users the permission to only read information whether on site or using the cloud application. Users in this group can also check out evidence assigned to them.
- **Limited Access**: Gives users the permission to read information when using the cloud application.

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

DHS offers privacy and security training. Each project may offer training specific to the project, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to PII are trained to appropriately handle it.

Explain what controls are in place to ensure that users of the system have completed training relevant to the project.

The company for this system provides privacy and security training as part of the full-fledged system training that clients can send their employees on. This portion of the training includes the following topics:

- Recognizing, and handling social engineering.
- Best practices when accessing data outside the local facility.
- General security practices for password creation, and data handling.
- Showcase of settings to maximize system hardening, and audit usage.

Training will be provided in person to show case these topics in a lab environment to provide hands on experience.

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

Describe the process and authorization by which an individual receives access to the information held by the project, both electronic and paper based records. Identify users from other agencies who may have access to the project information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project information.

Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two- factor authentication).

Example: Certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

To receive access to the system, an individual must go through the account approval process to determine what group they will be assigned to. Staff who will need physical access to evidence, and the ability of editing information within the system will be part of the full access group. Staff who will only need physical access evidence, and the ability to read information will be assigned to the staff group. Third party individuals who need to read information for evidence, for example a lawyer, are put in the limited access group to provide cloud access to the system. Access to physical evidence or information is assigned on a per case basis determined by management of the facility. To protect cloud access to the system, all user accounts are required to use two-factor authentication.

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?

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

When entering a contract to use the all-in-one security system, approval is needed from the Chief of Police for the law enforcement facility, or from someone who has equivalent authority. Approval of new user access and individual information sharing is handled internally by each individual facility the signs up to use the security system. Once the proper approval is performed for new users, digital copies of signed documentation are saved in the cloud.

Responsible Officials

<<ADD Privacy Officer/Project Manager>> Department of Homeland Security

Approval Signature

_____

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security