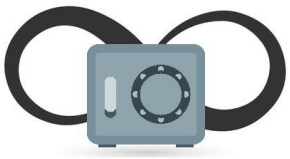
Cloud Safe

NEXT-GEN EVIDENCE SECURITY

Weiler Herrera, Javier Osorio, Arnold Baque, Brian Villamil, Trevor Cadigan

INFINITY SECURITY | TEAM 8



Infinity Security

Contents

Product Overview

Infinity Security will provide the product CloudSafe to improve security when handling evidence. CloudSafe is a mobile app that will connect with various sensors to secure evidence in the evidence room, when out for forensic testing, and when being delivered to court for trial. The goal is to make sure personnel such as evidence custodians, forensic lab personnel, and lawyers can handle evidence without concerning the police department. Using CloudSafe will ensure that everyone knows who currently has possession of the evidence and what was changed when the evidence is handled.

Infinity Security will upgrade and install evidence rooms with state-of-the-art hardware and software that can prevent evidence tampering. Law enforcement agencies from across the country have contracted Infinity Security to modernize their evidence handling process. CloudSafe allows law enforcement agencies to secure their evidence rooms to the next level. The main users of this software will be the individuals inside the department that will be documenting the evidence.

CloudSafe can take these steps to the next level by digitally integrating the chain of custody. CloudSafe will guarantee the integrity of the chain of custody. CloudSafe software uses next generation technology to ensure that evidence borrowed for tasks are returned and unchanged. Using a wide range of IoT sensors CloudSafe can track every step of the chain of custody process.

Stakeholders

Stakeholders include Infinity Security owners who will profit due to the cutting-edge technology solution and employees who acquire income on device installation and maintenance. The government in partnership with Infinity Security will benefit from the increased reliability and availability of evidence. The main users of CloudSafe will benefit with faster and more secure evidence handling. The hardware suppliers that enable Infinity Security to build the solution benefit from increased sales. Individuals who use CloudSafe will experience a faster and easier time completing their tasks.

Primary users

Law Enforcement

Infinity Security works closely with law enforcement agencies to secure high-value evidence using cloud-based solutions. CloudSafe allows law enforcement agencies to monitor the location and handling of evidence in real-time. Additionally, CloudSafe's proprietary features can determine whether evidence has been tampered with once it enters the system.

Secondary Users

Forensics Science Service Provider

CloudSafe is designed with the needs of Forensic Laboratory personnel in mind. Gone are the days of sorting through hastily written names and labels. The modern interface of the CloudSafe app allows it to be used by scientists and technicians productively, and with minimal training.

The unique characteristics of CloudSafe ensure that the evidence has not been tampered with, yielding more accurate lab results. If evidence is damaged or misplaced, the CloudSafe app can display the digital chain-of-

custody to assist in the investigation. In addition, scientists may find CloudSafe useful for transporting substances that must not be contaminated.

Legal Practitioners

Infinity Security is committed to making CloudSafe practical and accessible for legal practitioners. Simply downloading the app and authenticating with the proper credentials gives lawyers access to the most up to date evidence repository for their case.

Lawyers who are working on multiple cases will greatly benefit from the added organization and efficiency of the CloudSafe app. The CloudSafe app provides an intuitive way to obtain the whereabouts of all evidence relevant to their cases. CloudSafe provides cross compatibility with multiple law enforcement agencies. This means that lawyers can use the CloudSafe companion app to work on several cases at a time, provided the agencies are partnered with CloudSafe.

Potential Secondary Markets

Armored Car Services

Armored Car Services can utilize CloudSafe's unique cloud interface security protection to ensure contents being delivered are not tampered. The amount of hardware needed would be reduced to focus on transportation between business A and business B. During a robbery incident, CloudSafe will prove to be useful due to real-time location updates.

Features

Infinity Security strives to keep the partner's organization high-value evidence secure and always tracked. By implementing CloudSafe into the law enforcement agency, the contents of the evidence room will be monitored through the cloud solution. The customer-based features include:

Hardware

The implementation of CloudSafe begins with securing the evidence room itself. To accomplish this, first the Infinity Security hardware team will install a secure grid with sensors that detect when people are inside the room. This grid also houses cameras providing 24-hour surveillance to monitor everyone that comes and goes. Badges and CloudSafe's unique identifier through the mobile app will be needed to enter the room. Scanners will detect restricted items prior to entering. Evidence contents will be stored in smart bins that send out an alert when contents are taken in or out. Each Kevlar bag is equipped with a GPS tracker, so the location of evidence will always be available. To help detect tampering, weight sensors will check to see if the returned contents are identical.

Software

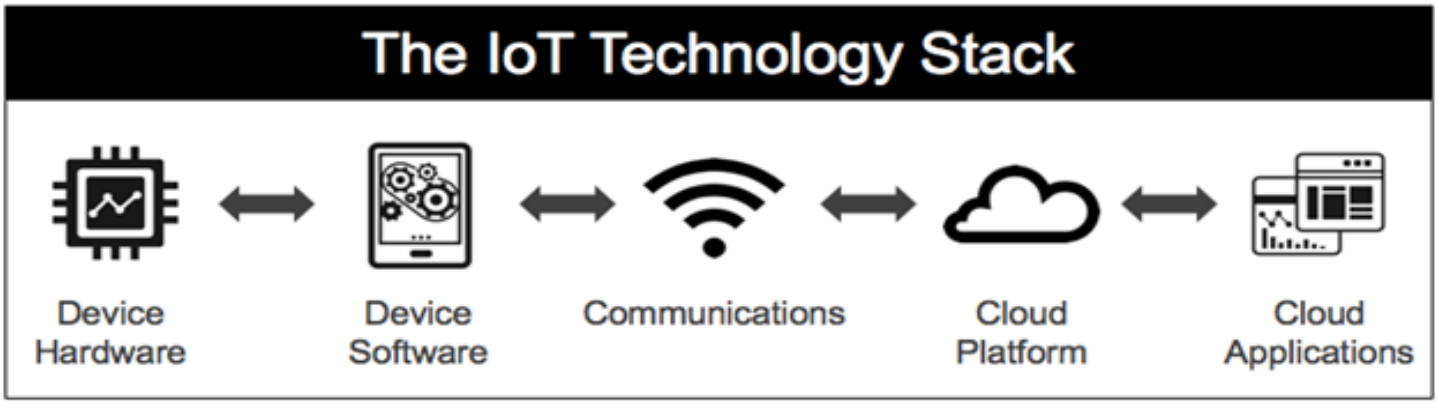
The companion app is the main point of access for the end users. CloudSafe will show a detailed overview of who has the evidence and where the evidence is at currently. Once a user is logged into the app, they will be assigned a unique numeric ID which pairs them with the chosen contents.

Communications

Law enforcement officers will be able to hand off custody of evidence to secondary users through the CloudSafe app. The secondary user will receive a push notification prompting them to accept responsibility of the evidence. Once they accept, responsibility will transfer, and ownership will be updated in the central database. The numeric ID attached to the evidence will help administrators see who the last user was, and which content was checked out.

Back-end Requirements

Infinity Security knows the importance of reliable backend features. These backend requirements include:



Device Hardware:

As the first layer of the stack, this stage will be defining the physical and digital parts of the smart implementation. In this case, the sensors can be installed anywhere that individuals are expected to occupy. The sensors are intended to sense human presence by detecting movement as well as sensing body heat. The idea of incorporating the sensor is to determine who comes into the evidence room and at what time. Cameras with facial recognition will see people coming and going. Scanners for badges, and GPS trackers for passcode protected Kevlar bag. Additionally, lockers will be required as a hardware to attach weight sensors to and offer a location for the bags.

Device Software:

The companion app, CloudSafe, can be downloaded on mobile devices for police departments partnered with Infinity Security. It is important that every employee involved in handling evidence always has the app up to date. The app gives access to some of the core features such as tracking evidence and transferring responsibility.

Communications:

This stack layer will be working to define the network communication frameworks that will connect the Kevlar bag's serial number with the CloudSafe app. The app will track the evidence and the individual carrying it as they enter and leave the building.

Cloud Platform:

All the sensor information will be used to set and determine who has the evidence and where they are with a location tracker.

Cloud Applications:

The last stack stage will handle the results given to the customer. For this product, the smart sensor will be delivering feedback to the evidence room about real-time information for the safe. The main goal here is to ensure that each person going in is recorded and the evidence is not tampered with.

Data Collection

CloudSafe can ensure evidence is treated through a clean chain of custody, and has not been tampered with, by collecting data from various sensors. The types of data collected are sensor, input, and numeric data.

Sensor Data

CloudSafe collects sensor data from multiple devices that are used in the evidence room. The data comes from the cameras, weight sensors, motion sensors, and ambient temperature sensors in the room.

The cameras use facial recognition to record and identify people coming in and out of the room. The camera can also record numerical data such as the height of someone that has entered the room. Collecting this data and processing it can also spot anyone entering restricted areas without clearance or someone that is trying to impersonate another person as well. The cameras also track where people go and what is retrieved from the lockers.

The temperature sensor will be collecting and processing data on the temperature in the room. This can be used to sense environmental hazards such as fires and water damage as well all indicate if there is a human in the room.

The weight sensor, located within each locker, will be collecting numerical data from the smart bins such as the weight. This is recorded in grams to the thousandths place. Recording this data will help spot any changes in the evidence such as someone trying to swap out an object.

Motion sensors record data such as dates and times to log and see what happened at that time that the motion sensors triggered.

Badge readers along with the two-factor authentication and the GPS that is setup will collect numerical data such as date, time, and GPS coordinates of the person activating.

Input Data

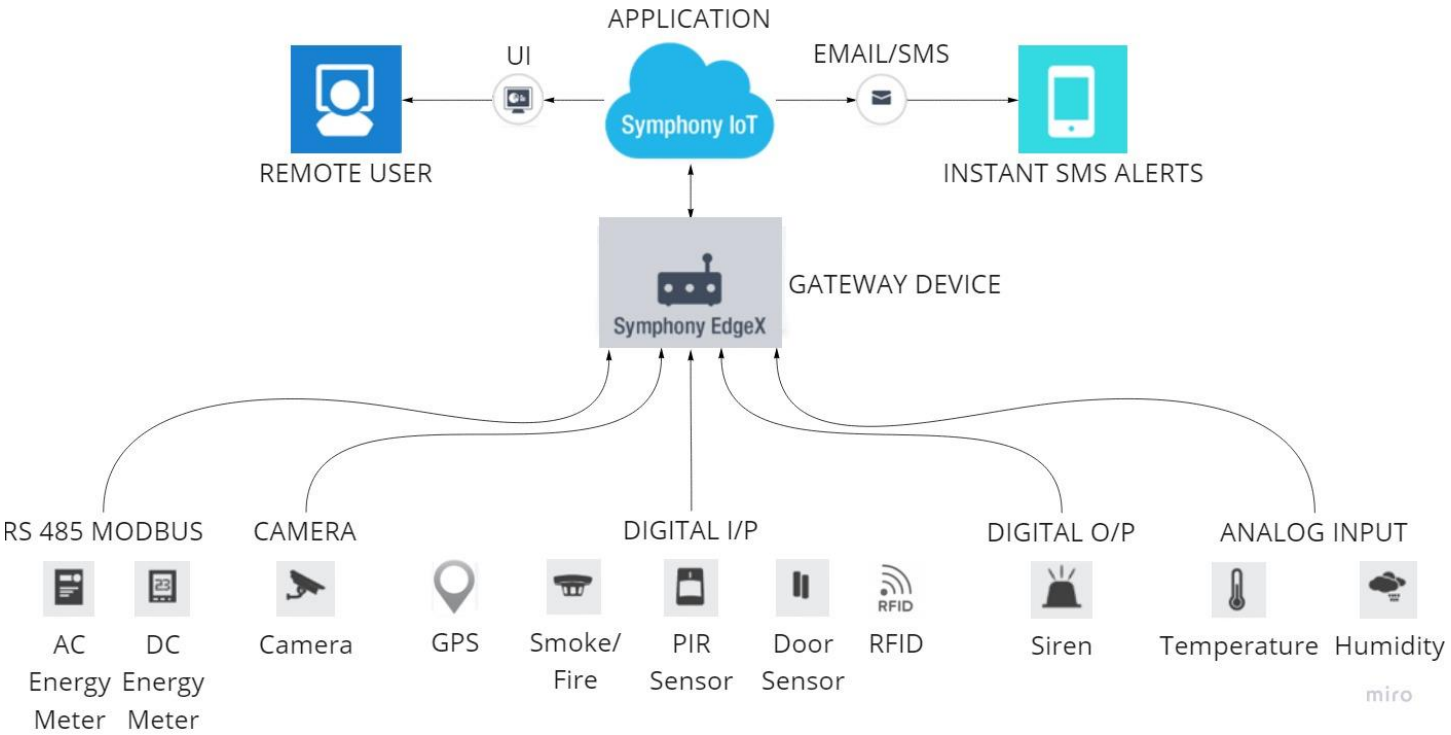
Data input into the system is collected to give certain levels of access. This can include but is not limited to name, occupation, identification number, phone number, height, level of access and who gave that person level of access. Information on the piece of evidence such as details of each sample, and the unique identifier, date and time of collection, type of analysis required, name and signature of the sample collector, official address and contact number, name of the recipient, laboratory's address, signatures of everyone involved in the chain of possession with date, time, and method of delivery, authorization for the analysis of the sample, any other information about the sample.

This information will be taken from the individuals applying for access and cross referenced with the organizations information to ensure accuracy.

Information Access

This data will not be readily available to everyone. Certain individuals will be allowed to input data to give people clearance levels. The level of access an individual has determines what they can see. The higher-level positions such as chief of police or head of the department have more clearance to information. However not all data is meant for all the users. A lot of the data will be for internal use only. Historical data will be kept in storage and must be requested but real time data is available with the right level of access.

Through the process and collection of all this information CloudSafe can enhance its algorithms to increase the accuracy of its tracking in the evidence room. The algorithms will also be able to learn to flag odd behavior, like an intrusion detection system, (IDS). With these systems in place, high-value items from the organization are guaranteed to be secure.



Data Flowing through the IoT Stack. These are all IoT devices that will be gathering data for the cloud.

Data Analytics using Cloud

The sensors will be using cloud analytics to compute, process, and store the data collected from those going in and out of the vault. One important benefit obtained from cloud computing is their architecture that relies on the relationship between the client, in this case the police or security precinct and one or more smart gateway devices. The communication and interaction of these two entities will collaborate to store substantial amounts of data. Another benefit of cloud is the ability to process and compute functions to determine peak fluctuations faster, decrease interference and false-negative data, and manage multiple processes at once. All the qualities mentioned will improve the security of the precinct for untampered evidence. Using cloud analytics to manage the gathered data over cloud analytics computing will allow the IoT devices to increase the speed of data moving back and forth.

Cloud Computing and Analytics Advantages:

Using smart gateways will help process data faster and to minimize the network overload. IoT equipment using this technology provides context awareness as application-level details are available near the client at the network. The software stacks on smart gateways can be upgraded in an agile manner without modifying or having massive implications in the cloud or core network.

Analytics

CloudSafe will give vital insight about the whereabouts of the evidence room's contents. With descriptive, predictive, and prescriptive analytics, the organization will be able to oversee critical data in a streamlined manner. Having this data aggregated will be valuable to the organization for efficiency and optimization.

Descriptive:

CloudSafe can alert at any given time when contents have left their designated area. Its current location will be output to the system and tracked in real time. Users with access will be able to see the history of who has taken out/returned the contents, the locations, and the time it has left the room. These metrics will be displayed in a detailed summary for review. Data will be summarized by daily/weekly averages with important information on each content. Some of this information may include how often an item has been checked out or which person(s) have checked in the most.

Predictive:

If the app recognizes that the contents have been consistently taken out by the same person(s), it will log their identification for future checkouts. This will make it quicker for users to checkout evidence while still being secure. Algorithms can detect if contents will be checked out soon by looking at the case database, and usual checkout times.

Prescriptive:

The app can give a course of action if it believes evidence has been tampered with. Contents can be flagged to be reviewed by administrators. If needed, the last known user can be blocked from entry until it has verified the contents are safe. CloudSafe can learn from false positives to accurately mitigate future risks.

Sensors

Smoke and Fire

Microchip Technology RE46C152E16F

https://www.arrow.com/en/products/re46c152e16f/microchip-technology

This module allows fire/smoke detector system to connect to the central network. This device was chosen because of the feature that sets off all alarms when one goes off. These will be used to protect the evidence room.

Motion Sensor

NCD Industrial IoT Wireless PIR Motion Detection Sensor

https://store.ncd.io/product/iot-long-range-wireless-pir-motion-detection-sensor/

These sensors will be used to detect intruders in the evidence room using its passive infrared sensor. This device was chosen because it is compact, easy to install, and is designed for use with cloud platforms. Another plus is the long range. It also features built in 128-bit AES encryption for added security.

Camera

ADLINK Technology, Inc NEON-1021-M/M4G/SSD32G/64BITS WS7E

https://www.arrow.com/en/products/neon-1021-mm4gssd32g64bits-ws7e/adlink-technology-inc

This smart camera will be used to watch different areas of the evidence room. Since CloudSafe features facial recognition, this device was chosen for its support for machine vision algorithms.

Door Sensor

MAGNETIC OPEN-CLOSED DOOR SENSOR-NB

https://iot-shops.com/product/magnetic-open-closed-door-sensor-nb/?wmc-currency=USD

This sensor can detect whether a door is open or closed. This device was chosen because it detects the current state of a door. If a door is opened and left open it will report that information.

WiFi Push Notification Dry Contact Transmitter for Azure®

https://store.ncd.io/product/wifi-push-notification-dry-contact-transmitter-for-azure/Camera

This sensor can be used to quickly notify administrators when doors are in use. It is designed to report the data from door sensors straight to Azure through Wi-Fi.

Temperature and Humidity

WiFi Temperature Humidity Sensor for Azure®

https://store.ncd.io/product/wifi-temperature-humidity-sensor-for-azure/

This device will be used to monitor the temperature and humidity inside the evidence room. It was chosen because of its compatibility with Azure.

Energy

PHOENIX CONTACT RCM-A/50/85-264V

https://www.arrow.com/en/products/rcm-a5085-264v/phoenix-contact

This device is used to measure the energy usage inside the evidence room.

Siren

CUI Devices CPS-5449-120PM

https://www.arrow.com/en/products/cps-5449-120pm/cui-devices

Siren to send out an alert in the event of a security breach or other emergency.

GPS

Taiyo Yuden GYSFFMAXC

https://www.arrow.com/en/products/gysffmaxc/taiyo-yuden

GPS module to be used for tracking the location of evidence. This component was chosen because of its small form factor.

Weight Sensor

Force Sensor Module 5N Force

https://www.arrow.com/en/products/fmamsdxx005wc2c3/honeywell

This sensor will be used to report the weight of evidence as it enters and leaves the evidence room. It was chosen for its reliability and small size. **Lockers** will be needed to attach weight sensors to. Infinity Security will be choosing lockers from: https://www.schoollockers.com/metal-lockers/vented-metal-box-lockers-261/six-tier-ventilated-steel-box-locker-14727.html?

RFID

Access Control Badge Reader - Omron V600-D8KR12

https://www.arrow.com/en/products/v600-d8kr12/omron

This sensor will be used to allow access to CloudSafe Users into the evidence room. It was chosen for its long range and its resistance to shock, vibration, and temperature.

Gateways

Azure Gateway - Wi-Fi Micro Gateway for Microsoft® Azure®

https://store.ncd.io/product/azure-gateway-wifi-wireless-iot-sensors/

Chosen for its innate compatibility with sensors as well as its long range. This gateway can also report directly to Azure.

IOT Protocols

Cameras/ temperature sensors

CloudSafe is using HTTPS instead of HTTP mainly when it comes to the web access of the cameras. This is due to the higher-level security that HTTPS provides. CloudSafe also give someone access to remote into the camera via SSH and transfer files via SFTP. SFTP provides a much higher level of security that normal ftp. The cameras also use SNMP. SNMP is one of the most widely deployed networking industry protocols and is supported on a variety of hardware. The advantages of using SNMP such as getting SNMP requests, responses traps and receipts outweighs the limitation of a device specific metric.

Access control protocols

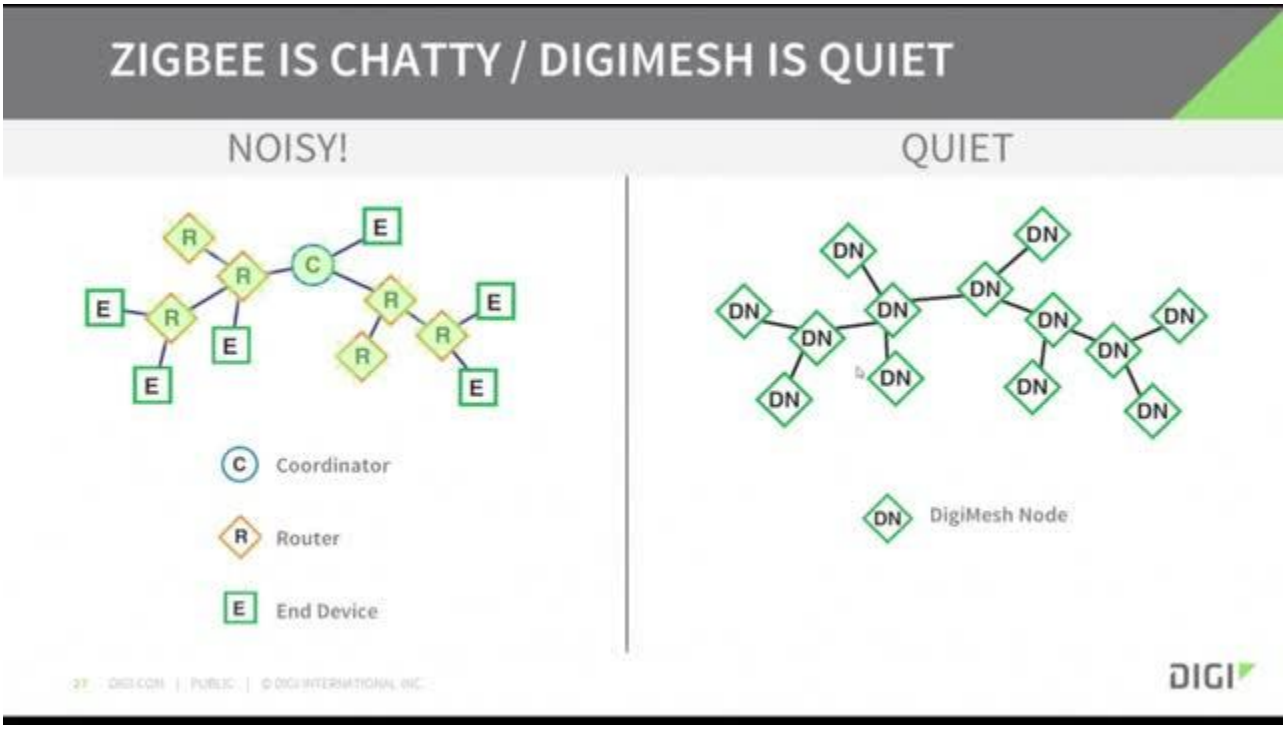
The badge readers that CloudSafe uses follow the current standard used in RFID today. That standard is the EPC global Class 1 Gen 2 protocol. This is an arbitration protocol used in all commercial access control readers.

GPS

The GPS's that CloudSafe uses are also on the global standard of NMEA (National Marine Electronics Association). This protocol was created by the National Marine Electronics Association and NMEA 0183 is the current standard used around the world. All GPS use this standard unless there is a proprietary protocol in place. CloudSafe chooses to use this protocol so that any organization can use a specific GPS device that they trust.

DigiMesh Network

The use of a DigiMesh was chosen instead of a ZigBee Mesh for the IOT devices due to the one homogenous node type that has a high ability to expand the network. It is a simple topology, yet it is also very reliable. It also can encrypt at a 256-bit rate compared to only a 128-bit AES connection a ZigBee mesh network. While Zigbee does have two layers for the MAC address and network address the Digi Mesh network will be more suited in such a densely populated area.



Network

Due to CloudSafe being a next generation platform a next generation Wi-Fi is also needed. Cloud safe uses Wi-Fi 6e. The reason why CloudSafe uses Wi-Fi 6e is due to the better performance it has in crowded areas and in the evidence room there is going to be a lot of materials of different size and densities, so it is best to have the strongest performing wi-fi available. This is done by dividing a wireless channel into sub channels. The weight sensors and the door sensors are all hooked up to the network via Wi-Fi.

Cloud Service Platform

To manage this data, the cloud computing service Microsoft Azure will be utilized. It was chosen for its serviceability and analytical tools which will assist in easily managing the application and its data. Another reason is that a key feature is mobile engagement as this feature is used for collecting real-time data analysis and can push notifications to user's devices. This will allow for alerting head of security when evidence is lost and where it can be found.

Once the data is collected by the sensor, it is uploaded to the cloud where the analysis process begins. All the data will be pushed to Microsoft Azure to collect and analyze large amounts of data coming from the sensors. It will also be used for creating reports, graphs and data charts that can be viewed by the staff and officers to see where the evidence has been and where it is going. The software will also collect thermal readings which are calculated to determine whether the evidence has left the vault or not. The data collected from the officers and forensic scientists will come from the mobile application they use to know when they have the evidence and where it is going. Some of the sensors that are on the Digi mesh are the door sensors and motion sensors.

Cloud over Server

CloudSafe will not have its own server but instead be cloud based to reduces cost. Compared to setting up local IT infrastructure, getting started with the cloud is cost efficient. Running and managing local servers also means the user may come across unanticipated expenditures associated with the management and maintenance of the system. Using both, Xfinity business and AT&T business, can ensure the network is always available.

Benefits of Cloud

Since all the infrastructure needs are fulfilled by the cloud service provider for a fixed cost, no upfront investments are involved. Plus, cloud computing is like another utility service. The cloud provider takes care of all the maintenance, and the user will get everything they will need at any point in time for nominal costs.

Cloud server providers optimize the hardware needs of the data centers, resulting in economies of scale. The server infrastructure of the cloud provider is shared between the workload and the computing needs of other clients.

Depending on the workload, this will ensure the full utilization of hardware sources. Higher efficiencies resulting from economies of scale mean lower costs to the cloud provider, who will in turn reduce costs.

Analytic Software

CloudSafe will work in tandem with different software and solutions to successfully analyze data. These will include Qlik Sense, Esri ArcGIS, and Density. By integrating these platforms into CloudSafe, it can always assure the accuracy of data.

Dynamic Alerting

Qlik Sense will go beyond a traditional Business Intelligence tool by delivering real-time, and up-to-date information. It is designed to support dynamic alerting and event triggering when certain conditions are met. Self-service and centralized models can be enabled to give users the ability to customize alerts freely.

Monitoring for outliers and anomalies can be swiftly done through advanced alert logic. By actively keeping an organization aware of evidence security, users can respond and act accordingly. Data can be visualized through charts, graphs, and objects which can be searched through to pinpoint problems. Administrators can explore interactive dashboards and dive deep into advanced analytics with Qlik's powerful engine.

Location Intelligence

Esri ArcGIS (Geographic Information System) is a location intelligence platform which is capable of tracking moving or stationary assets. Using location-powered analytic tools, back-end users on site will see real-time data displayed and mapped. Administrators can see a live 3D model of the evidence room and its contents to visualize differences from previous checkouts.

Logical/physical UML diagrams work with Esri's geometry model to map perspectives of areas and contents. The ArcGIS suite contains tools that help create spatial analysis which can be transformed into visual data. ArcGIS Enterprise in the Cloud will be the foundation of these features.

Access Control

Density products will be used to assist with access control. Entry by Density is a sensor which can count foot traffic through doorways anonymously. Infrared lasers and computer vision are used to monitor entrance and exit events in real-time. Predetermined boundaries are used to accurately detect users and that data is provided through the Density software.

Aggregate Statistics

Law Enforcement officers will find data from Density valuable to identify discrepancies between the number of user entrances, and badge swipes. Other gathered data from Qlik Sense and ArcGIS can also be immensely useful in protecting the integrity of evidence.

Mobile Device Software

Communications

Mobile devices will communicate with each other and CloudSafe through Wi-Fi. CloudSafe will use Wi-Fi 6e due to its expanded channel numbers as opposed to Wi-Fi 5. Wi-Fi is universal between mobile devices, affordable, well protected and controlled.

Mobile OS Platforms

There will only be two operating systems supported for CloudSafe. IOS from Apple and Android from Google will be used to develop the companion app and regularly updated to fix all bugs.

Form Factors

Phones and Tablets will encompass full accessibility to the CloudSafe app. The features will include full history report, if clearance is given, and being able to send off responsibility of evidence and accepting responsibility of evidence. There will also be a map, google maps if using android and Apple Maps if using Apple iOS, which shows the current location of evidence.

Personal Computers can also access CloudSafe, however this will only be accessible to System Administrators and Evidence Custodians who oversee monitoring analytics and in-depth history reports of location and handling potential changes found within evidence carriers.

Monetization

Infinity Security will be monetizing CloudSafe through a mix of one-time payments and a yearly subscription-based model. Infinity Security's evidence room solution will be installed for a one-time installation fee alongside equipment costs. The cost of installation will depend on square footage of the room.

Maintenance and training are also a way Infinity Security can monetize. Mass trainings will be essential for the organization's employees to understand how this software works, and this will be essential with updates that may change how things work in the app.

End users like, officers and forensics personnel, will have CloudSafe provided to them by the organization. This includes products that the organization will have to buy such as, access cards and GPSs. This will ensure a continuous stream of revenue.

In order to get CloudSafe known, Infinity Security will be hosting demos at conferences such as the IACP Technology Conference. The International Association of Chiefs of Police (IACP) Annual Conference and Exposition is the largest and most impactful law enforcement event of the year. Demos will also hold in the High Technology Crime Investigation Association (HTCIA) conference.

Time-based aspect of monetization

Since CloudSafe will mostly be implemented in law enforcement agencies, charges will be made on an annual and one-time basis. These organizations work with an annual budget, so this would be more ideal. The annual charges include the maintenance and Cloud services. The one-time charges include hardware/software, equipment installation, and the CloudSafe app for service access. Customers can take advantage of annual pricing due to long term savings and affordability. There will also be a la carte options for customers to tailor their organization's experience.

Probable Costs

Type of Hardware/Software	Hardware/Software Name	Type of Charge	Cost to Produce	Price to Sell
Smoke and Fire Sensor	Microchip Technology RE46C152E16F	One-time	$0.69	$1.00
Motion Sensor	NCD Industrial IoT Wireless PIR Motion Detection Sensor	One-time	$200.00	$260.00
Door Sensor	MAGNETIC OPEN-CLOSED DOOR SENSOR-NB	One-time	$122.22	$158.89
Smart Camera	ADLINK Technology, Inc NEON-1021-M/M4G/SSD32G/64BITS WS7E	One-time	$100.00	$130.00
Energy Sensor	PHOENIX CONTACT RCM-A/50/85-264V	One-time	$50.00	$65.00
Badge Reader	Omron V600-D8KR12	One-time	$338.55	$500.00
Smart Siren	CUI Devices CPS-5449-120PM	One-time	$6.50	$8.45
Humidity Sensor	WiFi Temperature Humidity Sensor for Azure®	One-time	$160.00	$208.00
Weight Sensor	Force Sensor Module 5N Force	One-time	$24.79	$32.23
RFID Scanner	Omron V600-D8KR12	One-time	$354.00	$460.2
Gateway	Azure Gateway - Wi-Fi Micro Gateway for Microsoft® Azure®	One-time	$200.00	$260.00
GPD Module	Taiyo Yuden GYSFFMAXC	Annual	$21.02	$7.00
Dry Contact Transmitter	WiFi Push Notification Dry Contact Transmitter for Azure®	One-time	$160.00	$208.00
CloudSafe Bag	Kevlar by DuPont Atlantis Duffle	One-time	$150.00	$200.00
App Download Cost	CloudSafe	One-time	$5.00	$5.00
Installation Fee	Infinity Security Installation	One-time	$20,000.00	$20,000.00
Lockers Installation	Infinity Security Lockers (6-in-1 locker)	One-time	$280.00	$400.00
Maintenance	Infinity Security Maintenance	Annual	$2,000.00	$2,000.00
Cloud Services	Azure	Annual	$30,000.00	$30,000.00
		Total:	$54,172.77	$54,903.77

City of Colorado Springs Police Department

The hypothetical police department located in Colorado Springs will contain 40 daily users on average and have 2 supervisors in charge of monitoring analytical data. The evidence room will be 2000 square feet and have 2 entrances. They will be equipped with 30 CloudSafe bags for transportation.

Type of Hardware/Software	Hardware/Software Name	Type of Charge	Quantity	Price	Total Price

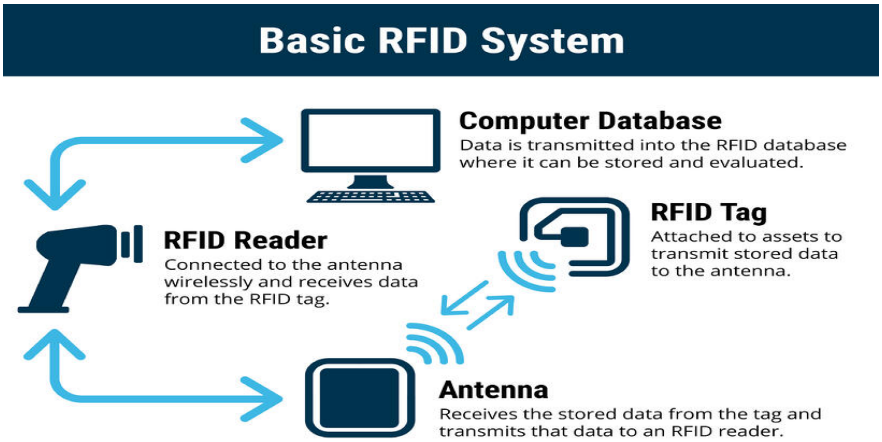
Smoke and Fire Sensor	Microchip Technology RE46C152E16F	One-time	3		$1.00	$3.00
Motion Sensor	NCD Industrial IoT Wireless PIR Motion Detection Sensor	One-time	4		$260.00	$1,040.00
Door Sensor	MAGNETIC OPEN-CLOSED DOOR SENSOR-NB	One-time	2		$158.89	$317.78
Smart Camera	ADLINK Technology, Inc NEON-1021-M/M4G/SSD32G/64BITS WS7E	One-time	8		$130.00	$1,040.00
Energy Sensor	PHOENIX CONTACT RCM-A/50/85-264V	One-time	1		$65.00	$65.00
Badge Reader	Omron V600-D8KR12		One-Time	2	$500.00	$1000.00
Smart Siren	CUI Devices CPS-5449-120PM	One-time	2		$8.45	$16.90
Humidity Sensor	WiFi Temperature Humidity Sensor for Azure®	One-time	3		$208.00	$624.00
Weight Sensor	Force Sensor Module 5N Force	One-time	30		$32.23	$966.90
RFID Scanner	Omron V600-D8KR12		One-time	2	$460.2	$920.40
Gateway	Azure Gateway – Wi-Fi Micro Gateway for Microsoft® Azure®	One-time	3		$260.00	$780.00
GPS Module	Taiyo Yuden GYSFFMAXC	Annual	30		$7.00	$210.00
Dry Contact Transmitter	WiFi Push Notification Dry Contact Transmitter for Azure®	One-time	2		$208.00	$416.00
CloudSafe Bag	Kevlar by DuPont Atlantis Duffle	One-time	30		$200.00	$6,000.00
App Download Cost	CloudSafe	One-time	40		$5.00	$200.00
Installation Fee	Infinity Security Installation	One-time	N/A		$20,000.00	$20,000.00
Locker Installation	Infinity Security Lockers (6-in-1 locker)	One-time	7		$400.00	$2,800.00
Maintenance	Infinity Security Maintenance	Annual	N/A		$2,000.00	$2,000.00
Cloud Services	Azure	Annual	N/A		$30,000.00	$30,000.00
					Total Cost:	$68,399.98

Azure API

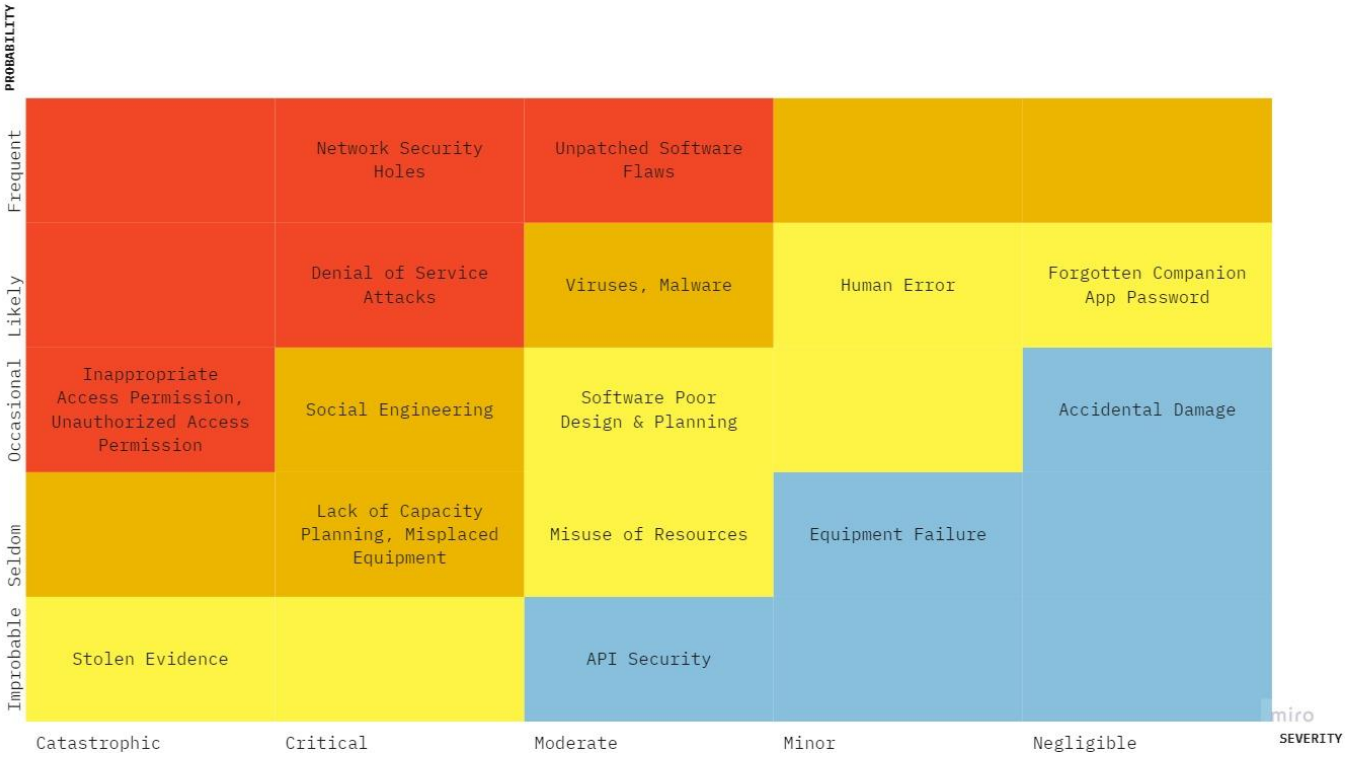
Azure API Management is primarily used to provide a central interface to create, provision and manage API for web and cloud applications and services. With Azure API Management, users can monitor the health of APIs, identify errors, configure throttling, rate limits and more on each API.

RFID

One API will be used is RFID (Radio-frequency identification) which uses electromagnetic fields to automatically identify, and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter. This would allow the user to know who is going in and out of the evidence room and update the database on who has access to the evidence. The devices used that are RFID are the badges given to the officers and forensics team.



Risk Matrix



Risk Matrix Vulnerabilities

Inappropriate Access Permission/Unauthorized Access Permission:

To deter users from tailgating into the evidence room, employees will be trained on correct entry protocols. They will need to scan their employee badge in orderly fashion and avoid letting unauthorized users inside. Disciplinary actions will be given with each occurrence, and failure to comply may lead to termination.

Stolen Evidence:

Any stolen evidence shall be reported to the Evidence Supervisor or higher. An immediate search in the perimeter will be made to find the property by a member of the law enforcement agency. If the stolen evidence cannot be recovered, a further investigation will be made. Location history granted by the GPS device within each bag will be used to recover stolen evidence.

Network Security Holes:

To protect the organization from security breaches, many practices will be implemented. These include an IDS/IPS, a Security Incident Event Manager, and a principle of least-privilege. The system will be secured using IPsec, SSL/TLS, and a VPN. Any suspicious trends will be monitored through analytics and Two-Factor Authentication will be used.

DDOS:

A response plan will be created to respond promptly to successful attacks. Cloud-based providers will be adopted, and network vulnerability assessments will be performed. Employees will be educated not to click on unknown links.

Social Engineering:

An employee awareness program will be given to teach best practices. They will be trained to always verify outsider identities. Penetration testing will also be conducted to detect vulnerabilities.

Lack of capacity planning, Misplaced equipment:

A capacity planning strategy will be implemented to monitor availability of resources. Misplaced equipment will be tracked through the GPS module.

Unpatched Software Flaws:

A managed service provider will be used to automate software patches and maintenance overall. Also, Software Asset Management tools will be used to help manage automate tasks.

Malware:

Using security software such as Sophos who specialize in products for communication endpoint, encryption, network security, email security, mobile security, and unified threat management.

Software Poor Design & Planning:

The larger the IT team the better they will be able to quickly find flaws in the program or fix any vulnerability being exploited with the sensor devices out in the field. The main goal will be to fix any issues as quickly as they appear.

Misuse of Resources:

Infinity Security will be providing training for all the users to avoid any misuse of the product and its resources. On top of that having the customers will sign a waiver after the training to have them know they are now fully responsible for the resources after the training.

Human Error:

There is always a risk of human error, therefore it is necessary to account for it during development. Training Employees mitigates the probability of errors occurring. Constricting employees in options can also mitigate unwanted input errors. Having our users complete a checklist sheet in order to lower the rate for human error occurrences.

Equipment Failure:

Infinity Security will provide a 3-year warranty for Infinity Security products to ensure the users can feel comfortable if there should be any equipment issues with any of the devices. Redundant equipment to ensure fast and easy replacements.

Forgotten Companion App Password:

One of the advantages of building the software to work specifically with the hardware is the support given to clients with their IT difficulties remotely. This way the users will always have 24/7 support for any issue they may come across.

Accidental Damage:

Accidents will happen and is why Infinity Security will be providing warranties with Infinity Security products should any issue be an internal damage but for physical damage, it is recommended the users contact Infinity Security directly to issue replacements and prices will vary depending on the broken device.

API Security

API security is the process of protecting APIs from attacks. Because APIs are very commonly used, and because they enable access to sensitive software functions and data, they are becoming a primary target for attackers. API security is a key component of modern web application security.

Data Standards

Infinity Security collects data using the United States Geological Survey data standards. Such standards include

Temporal

Date / time

- Data Standard: ISO 8601
- Format: YYYY-MM-DD or YYYY-MM-DDT:HH:MM:SS+00:00
- Example (Mountain Standard Time (MST)): 2020-08-11T11:02:49-07:00

Divisions of Geologic Time approved by the U.S. Geological Survey Geologic Names Committee, 2018. (Public domain.)

Geologic time

- Data Standard: Divisions of Geologic Time – Major Chronostratigraphic and Geochronologic Units
- Data Standard: IUPAC-IUGS common definition and convention on the use of the year as a derived unit of time (IUPAC Recommendations 2011): http://doi.org/10.1351/PAC-REC-09-01-22

Geographic location descriptors

Geographic coordinates

- Data Standard: ISO 6709:2008
- Format: ±90.00 and ±180.00 (precision documented by number of decimal places and contingent upon equipment used)
- Example: Latitude: 42.3300; Longitude: -98.1449

Geographic names / codes

- Data Standard: ANSI INCITS 446-2008
- Browse Features in the Data Standard: Geographic Names Information System (GNIS)
- Example: Name: Amicalola Falls; ID: 330601

Watershed boundaries

- Data Standard: Hydrologic Unit Codes (HUC)
- Example:Watershed Name: Upper Kennebec; HUC: 01030001

Country codes

- ISO-3166
- Example: Full name: the United States of America; Alpha-3 code: USA; Numeric code: 840

U.S. state and county codes

- Data Standard: Federal Information Processing Standards (FIPS)
- Example: County Code: 01001; County Name: Autauga; State Code: 01; State Name: Alabama

Classification standards

- Vegetation Classification: United States National Vegetation Classification (USNVC)
- Biological Taxonomy: Integrated Taxonomic Information System (ITIS)*

Best standard practices for protocol

Access control protocols

The badge readers that CloudSafe uses follow the current standard used in RFID today. That standard is the EPC global Class 1 Gen 2 protocol. This is an arbitration protocol used in all commercial access control readers.

GPS

The GPS's that CloudSafe uses are also on the global standard of NMEA (National Marine Electronics Association). This protocol was created by the National Marine Electronics Association and NMEA 0183 is the current standard used around the world. All GPS use this standard unless there is a proprietary protocol in place. CloudSafe chooses to use this protocol so that any organization can use a specific GPS device that they trust.

APPENDIX A

Denial-of-Service Incident Response Plan

This document provides information for identifying, responding to, and documenting a Denial-of-Service attack. Steps 1-5 provide information for contacting the proper staff. Steps 6-8 outline the procedure for determining the type of incident. Steps 8-18 outline the response and aftermath of the specific type of incident, in this case, a Denial-of-Service attack.

1) The person who discovers the incident will call the Infinity Security Technical Support Team. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:
    a) Helpdesk
    b) Intrusion detection monitoring personnel
    c) A system administrator
    d) A firewall administrator
    e) A manager
    f) The security department or a security person.
    g) User of CloudSafe app (Police officer, Lawyer, Forensic Scientist)
    h) Evidence Supervisor
    i) An outside source.
2) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.
3) If the person discovering the incident is not a member of the IT department or affected department, they will call the 24/7 Infinity Security Technical Support Team reachable at xxx-xxx.
4) The Infinity Security Technical Support Team will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The Infinity Security Technical Support Team 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) What equipment or persons were involved?
    f) Location of equipment or persons involved.
    g) How the incident was detected.
    h) When the event was first noticed that supported the idea that the incident occurred.
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 Infinity Security Threat Response Team members to be contacted. The staff member will call those designated

on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the Infinity Security Technical Support team in the previous step. The staff member could possibly add the following:

a) Is the equipment affected business critical?

b) What is the severity of the potential impact?

c) Name of system being targeted, along with operating system, IP address, and location.

d) IP address and any information about the origin of the attack.

6) Contacted members of the Infinity Security Threat 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 incident still in progress?

c) What data or property is threatened and how critical is it?

d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?

e) What system or systems are 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 incident be quickly contained?

i) Will the response alert the attacker, and does it matter?

j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

7) An incident ticket will be created. The incident will be categorized into the following category:

a) Category two - A threat to sensitive data

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

a) Denial of service response procedure.

At this point, the incident is confirmed to be a Denial-of-Service attack. The following steps outline the Denial-of-Service response procedure.

9) Team members will review the load and logs of servers, routers, firewalls, applications, and other affected infrastructure in order to determine the scope of the attack. Network specialists should use a network analyzer to differentiate wanted and unwanted traffic and identify the type of DoS attack. The team shall also review intrusion detection logs, and interview witnesses to determine the origin of the attack. Only authorized personnel should be performing interviews or examining evidence.

10) The team should attempt to mitigate the effects of the attack by:

- Throttling or blocking malicious traffic.
- Suspending unnecessary services.
- If a particular feature or application is being targeted, temporarily disable it.
- Configure filters to only allow connections from a whitelist.

- Utilize the backup ISP to obtain new IP addresses.

11) Team members will recommend changes to prevent the attack from happening or mitigating the effects. Some of these changes could include:
    - Contacting the ISP and cloud provider to discuss DoS mitigation services.
    - Acquiring a traffic filtering/scrubbing service or product.
    - Create a whitelist of IP addresses and protocols related to the most valuable clients in case it is necessary to prioritize traffic.
    - Create a network topology diagram to accompany the response plan.
    - Run DoS attack simulations to identify vulnerabilities and gauge the strength of the response team.
    - Reduce Attack Surface Area
12) Upon management approval, the changes will be implemented.
13) Team members will restore the affected system(s) to a working state. They may do any or more of the following:
    a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    b) Make users change passwords if passwords may have been sniffed.
    c) Be sure the system has been hardened by turning off or uninstalling unused services.
    d) Be sure the system is fully patched.
    e) Be sure real time virus protection and intrusion detection is running.
    f) Be sure the system is logging the correct events and to the proper level.
    g) Identify flaws in firewall protection.
    h) Account for all equipment using the inventory log.
14) Documentation—the following shall be documented:
    a) How the DoS attack was discovered.
    b) The type of DoS attack.
    c) Which systems were vulnerable?
    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.
15) 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.
16) 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.

a) FBI 1-800-CALLFBI (225-5324) for the Major Case Contact Center.

17) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

18) Review response and update policies—plan and take preventative steps so the attack cannot happen again.

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

b) Consider whether a procedure or policy was not followed which allowed the attack, and then consider 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) Was the incident response procedure detailed and did it cover the entire situation? How can they be improved?

f) Have changes been made to prevent another attack? 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 attack?

h) Should any security policies be updated?

i) What lessons have been learned from this experience?

Privacy Impact Assessment for

CloudSafe

DHS/CS/PIA-008(x)

11/4/2021

Contact Point

John Doe

Infinity Security

CloudSafe

305-503-0530

Reviewing Official

Jonathan R. Cantor Acting Chief

Privacy Officer Department of

Homeland Security

(202) 343-1717

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.

CloudSafe is a mobile app that will connect with various sensors to secure evidence in the evidence room, when out for forensic testing, and when being delivered to court for trial. The goal is to make sure personnel such as evidence custodians, forensic lab personnel, and lawyers can handle evidence without concerning the police department. The project can ensure evidence is treated through a clean chain of custody, and has not been tampered with, by collecting data from various sensors.

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 project's goal is to improve security when handling evidence. The project is a mobile app that will connect with various sensors to secure evidence in the evidence room, when out for forensic testing, and when being delivered to court for trial. The goal is to make sure personnel such as evidence custodians, forensic lab personnel, and lawyers can handle evidence without concerning the police department. The project will ensure that everyone knows who currently has possession of the evidence and what was changed when the evidence is handled.

Infinity Security will upgrade and install evidence rooms with state-of-the-art hardware and software that can prevent evidence tampering. Law enforcement agencies from across the country have contracted Infinity Security to modernize their evidence handling process. The project allows law enforcement agencies to secure their evidence rooms to the next level. The main users of this software will be the individuals inside the department that will be documenting the evidence.

The project can take these steps to the next level by digitally integrating the chain of custody. The project will guarantee the integrity of the chain of custody. The project uses next generation technology to ensure that evidence borrowed for tasks are returned and unchanged. Using a wide range of IoT sensors, the project can track every step of the chain of custody process.

1. 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).

Does not apply.

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

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

Does not apply.

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, it was completed on 10/28/2021.

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.

Does not apply.

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.

Does not apply.

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.

The two categories of individuals for whom information is collected are the Primary and Secondary users. The primary user is the law enforcement agency. The secondary users are those authorized to use the product by the law enforcement agency such as the legal practitioners and forensic service providers. For primary users, the following data is collected: name, occupation, identification number, phone number, height, level of access and who gave that person level of access. For the secondary users, the following data is collected: information on the piece of evidence such as details of each sample, and the unique identifier, date and time of collection, type of analysis required, name and signature of the sample collector, official address and contact number, name of the recipient, laboratory's address, signatures of everyone involved in the chain of possession with date, time, and method of delivery, authorization for the analysis of the sample.

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 sensors will be using cloud analytics to compute, process, and store the data collected from those going in and out of the vault. The communication and interaction of these two entities will collaborate to store substantial amounts of data. Using cloud analytics to manage the gathered data over cloud analytics computing will allow the IoT devices to increase the speed of data moving back and forth.

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.

Does not apply

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.

The individuals providing data are the members of the law enforcement agency, lawyers, forensic scientists, and anyone else authorized by the law enforcement agency to be involved in the secure transportation of evidence.

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.

Information from the law enforcement database is required to implement the proper levels of access into the product. The higher-level positions such as chief of police or head of the department have more clearance to information.

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.

CloudSafe collects sensor data from multiple devices that are used in the evidence room. The data comes from the cameras, weight sensors, motion sensors, and ambient temperature sensors in the room.

The cameras use facial recognition to record and identify people coming in and out of the room. The camera can also record numerical data such as the height of someone that has entered the room. Collecting this data and processing it can also spot anyone entering restricted areas without clearance or someone that is trying to impersonate another person as well. The cameras also track where people go and what is retrieved from the lockers.

The temperature sensor will be collecting and processing data on the temperature in the room. This can be used to sense environmental hazards such as fires and water damage as well all indicate if there is a human in the room.

The weight sensor, located within each locker, will be collecting numerical data from the smart bins such as the weight. This is recorded in grams to the thousandths place. Recording this data will help spot any changes in the evidence such as someone trying to swap out an object.

Motion sensors will be record data such as dates and times to log and see what happened at that time that the motion sensors triggered.

Badge readers along with the two-factor authentication and the GPS that is setup will collect numerical data such as date, time, and GPS coordinates of the person activating.

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 non-governmental 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.

CloudSafe uses publicly available data to verify the identities of individuals. Publicly available data is also used to track the status of court cases.

2.4 Discuss how 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.

CloudSafe uses publicly available data to verify the information provided by individuals. Once data is entered into the system, it automatically references public databases to ensure accuracy. The sensors employed by CloudSafe are used primarily for ensuring proper levels of access which by nature verifies the information provided by individuals (I.E. facial recognition, RFID). Cloud Analytics, which are used to aggregate this data, can also be used to identify issues with the accuracy and integrity of the product by detecting inconsistencies .

1. 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: Virus or malware

Mitigation: Data is protected from virus and malware using security software such as Sophos who specialize in products for communication endpoint, encryption, network security, email security, mobile security, and unified threat management.

Privacy Risk : Internal data breach

Mitigation: Data leaked internally is mitigated by restricting access to data through clearance. Every time a request for data is made all factors including the identity of the individual as well as their specific role and context of their request are taken into account.

Privacy Risk : Collection of data not user-consented

Mitigation: All data that is collected must have a valid purpose pertaining to the specific individual. For example, location data does not need to be collected unless the individual is carrying evidence.

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.

CloudSafe collects name, occupation, identification number, phone number, height, and level of access in order to verify the identities of the individuals in the evidence room. This information is used to identify individuals through cameras and sensors.

In order to properly maintain the security and integrity of evidence, CloudSafe collects information on the piece of evidence such as details of each sample, and the unique identifier, date and time of collection, type of analysis required, name and signature of the sample collector, official address and contact number, name of the recipient, laboratory's address, signatures of everyone involved in the chain of possession with date, time, and method of delivery, authorization for the analysis of the sample, any other information about the sample.

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.

A search can be done to determine what evidence a user has been in custody of as well as the date, time and place it was obtained. This search would not create a new record since the information has already been linked together.

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.

Does not Apply

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

In order to access the above information, users are required to log in with their credentials to verify their level of access. This will ensure that sensitive data is only visible to those with the clearance to view it.

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.

Before users download the CloudSafe app, they must agree to the terms of service which outlines all the information collected. The terms state exactly what kind of data is collected, the purpose, and how it is stored. The included PIA provides them with the necessary information to consent to the collection of information.

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/her

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.

Users may opt out of data collection by not agreeing to the terms of service. Data collection is required for the product to produce accurate results, therefore opting out would bar the user from using the product.

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: User does not have opportunity to decline or consent

Mitigation: The terms of service agreement which allows the collection of information is prompted when first using the app. Users are not capable of providing information unless the agree to the terms.

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.

Data will be retained as long it is deemed necessary. Data input into the system is collected to give certain levels of access. This can include but is not limited to name, occupation, identification number, phone number, height, level of access and who gave that person level of access. Data collected from sensors will be retained to accurately maintain evidence security.

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: Low

Mitigation: As mentioned in the Security phase, the system will be secured using IPsec, SSL/TLS, and a VPN. The different protocols that are used by the sensors will also keep the integrity of the user's data. PII will be retained for the users working on current cases, and other associates, if they are still active in the system.

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

A lot of the data will be for internal use only. Historical data will be kept in storage and must be requested but real time data is available with the right level of access. The higher-level positions such as chief of police or head of the department have more clearance to information. The Evidence Supervisor will need to authorize for evidence to be checked out to be analyzed by the FBI.

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.

Does not apply.

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 will not be readily available to everyone. Due to the sensitivity of evidence and data collected from users handling it, disclosing it elsewhere will be limited. An external agency such as the FBI would be allowed to analyze evidence and its related data.

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.

Disclosures of external sharing will be logged in its appropriate database. This would be stored within the organization's Cloud servers.

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: Low

Mitigation: There will be a variety of access controls put in to mitigate data leaks from external sharing. Audit logs will keep track of data that has been shared and who has accessed it. As well as physical access controls from the RFID badges, surveillance cameras, and Density sensors.

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.

Any officer who creates an account, will be able to go to a section within the app that displays the name, email, and phone number inputted for their account. They will have an option to either delete their phone number to allow us to track who has the evidence. They will also be able to review the privacy notice and terms of service.

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.

Within the app, patrons will be able to view their account information and correct any errors or make any changes.

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.

If the police navigate to their account information in the app, there will be a button that gives the option to edit their information.

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: Low

Mitigation: N/A

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.

Protocols are put into place that safeguard against information sharing. Audits will be done every three to six months for any accounts that have been inactive for a year that were not automatically removed by the system. The I.T. team will constantly be on the lookout for any data breaches or intended misuse of information. Our company will be following S.O.C.K.S (Socket Secure) protocols.

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 individuals with access to the PII are the Police staff and head of Police. There is a subsection within their employee handbooks that they must agree to that outlines the proper use of company data.

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.

When the precinct receives the data, the system in the precinct will inform the staff of the name of the forensic scientist who requested the evidence. Once the evidence is confirmed as occupied by an officer, the information is moved from one account to another.

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.

Periodically, the information will be reviewed by the system administrators and help desk.

Responsible Officials

Jason Bourne of Infinity Security

Approval Signature

_____

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security