Smart Shelter Management System (SSMS)

IoT Product Development Group Project

Group members:

Castillo Hector, Ellis Sharabi, Sanchez Moises, Starnes Mason, Thompson Brandy, Matthew Chinea

FOR EDUCATIONAL PURPOSES ONLY

Evacuee Location Data..... 6
Evacuee Check-In/Out Data..... 7
Shelter Capacity Data..... 7
Historical Evacuee Movement Data..... 7
User Feedback Data..... 8
Emergency Notification Data:..... 8
Health Status Data..... 9
Identification Data..... 9
Probable Costs..... 23
Device costs..... 23
Service costs..... 23
APIs for the Smart Shelter Management System (SSMS)..... 27
Existing APIs..... 27
GPS and Mapping Apis:..... 27
IoT Device Management APIs:..... 27
Communication APIs:..... 27
CRM APIs:..... 27
Analytics APIs:..... 27
New APIs..... 27
Evacuee Data Management API:..... 27
Resource Allocation API:..... 27
Shelter Capacity API:..... 28
Family Reunification API:..... 28
Healthcare Integration API:..... 28
Shelter Operations API:..... 28
Open Source vs. Proprietary APIs..... 28
Open Source:..... 28
Proprietary:..... 28
Possible Vulnerabilities Matrix..... 29
High Likelihood and High Impact (Critical)..... 29
Unauthorized Access to Data:..... 29

FOR EDUCATIONAL PURPOSES ONLY

Failure of Wearable Device:..... 29
Malware Attacks:.....29
System Overload During Disaster:.....29
High Likelihood and Medium Impact (High Risk)..... 30
Network Interruptions:..... 30
Data Corruption:..... 30
Device Battery Failure:..... 30
Medium Likelihood and High Impact (High Risk)..... 30
Compromise of API Security:.....30
Cloud Platform Outages:..... 30
Medium Likelihood and Medium Impact (Moderate Risk)..... 30
User Error:.....30
Software Bugs:..... 30
Low Likelihood and High Impact (Moderate Risk)..... 30
Physical Damage to Devices in Shelters:..... 31
Supply Chain Attacks:.....31
Low Likelihood and Medium Impact (Low Risk).....31
Reputational Damage Due to Minor Data Leaks:..... 31
Wearable Tag Duplication:..... 31
Low Likelihood and Low Impact (Low Risk).....31
Temporary Loss of Non-Essential Features:..... 31
Minor Network Delays:..... 31

FOR EDUCATIONAL PURPOSES ONLY

Overview

Smart Shelter Management System (SSMS)

Description: The SSMS is an integrated platform designed to enhance the efficiency and effectiveness of emergency shelter operations during disaster events. Utilizing a network of smarts sensors and wearable devices, the system ensures real time tracking of evacuees across multiple shelter locations, offering a seamless way to manage shelter population and communicate with concerned parties.

How it will work: This system would leverage smart sensors and wearable technology to track and manage evacuee locations during and after major disaster events, providing critical information to both emergency personnel and evacuees' loved ones.

Privacy Controls

Data Encryption: All data, both in transit and at rest, will be encrypted using industry-standard encryption protocols. This ensures that personal information is secure and unreadable to unauthorized users.

Regular Audits and Compliance Checks: The system will undergo regular security audits and compliance checks to ensure it meets all relevant data protection regulations such as those on HIPAA.

Tiers of Access

Role-Based Access Control (RBAC): Access to the SSMS will be governed by RBAC mechanisms, ensuring users have access only to the information and functionalities pertinent to their roles.

Multi-Factor Authentication (MFA): To further secure access, MFA will be required, especially for roles with access to sensitive or extensive data sets, adding an additional layer of security beyond passwords.

Controlling Information Visibility

Granular Permission Settings: The system will feature granular permission settings, allowing administrators to fine-tune access rights for different users or groups. This will ensure that individuals can access only the data they are authorized to view or manipulate.

FOR EDUCATIONAL PURPOSES ONLY

End/user standpoint benefits:

Enhanced Safety and Security: the product will have real-time location tracking which ensures that evacuees can be quickly located within shelters, enhancing their safety during disaster situations.

Streamlined Check-In/Out: Allows for more efficient use of shelter access and resources while reducing lines and administrative hassles.

Increased Communications: This would ensure better communication between evacuees and shelter staff, ensuring resources and any critical updates are received in time.

Privacy Protection: Having secure data handling and privacy controls will give peace of mind to the Evacuees who can be sure that their personal information is protected and only used for their safety and benefit. These controls will be governed by role-based access control methods, which will make sure users can only access pertinent information according to their roles. Administrators will be able to manage who may view what information with more precision thanks to granular permission settings, which will also help to ensure data confidentiality and regulatory compliance.

Efficient Resource Allocation: The SSMS provides real-time data on shelter capacities and evacuee locations. This allows emergency personnel to allocate resources such as food, medical supplies, and personnel more efficiently. This will further ensure that the needs of each evacuee are met.

Organization standpoint benefits:

Efficient Shelter Management: A centralized dashboard allows for real time-time monitoring of shelter capacities, resource allocation and the location of each evacuee. This process leads to more efficient and streamlined shelter management.

Improved Coordination: The system can enhance coordination between different shelters and with external organizations which ensures a unified and effective disaster response.

Compliance and Reporting: This system can automate the generation of reports and ensure compliance with regulatory requirements, this leads to an increase in time saved and ensures transparency in the shelter operations.

Data Collection: The system will provide the organization with additional data that will be saved and used to better the software. The data that is collected and saved would be the user feedback from the perspective of family and, or friends who will be able to monitor the movements of their loved ones, movement data tracked by the sensors to be able to identify the conditions of why and when some have left, and data collected from the information given by evacuees to be used to easily bring them back up if there were to be in another disaster as this will help decrease the time needed to collect their information as they will have already saved data and be able to ping their family without having them to re-input everything again.

Primary Users:

FOR EDUCATIONAL PURPOSES ONLY

Evacuees: These individuals are people displaced from their homes and seeking refuge. They are a primary user of the smart tags/wearable devices, these devices would be assigned to the individual upon arrival at the shelter and given a unique identifier. Also, people could pre-register via the app by providing some form of government Identification to streamline the process. Their primary motivation for using the SSMS is to ensure their safety and well-being while staying at the shelter. These devices provide useful information about themselves and help improve the overall effectiveness of management within the shelter.

Emergency Personnel: This includes first responders, shelter managers, and other authorized personnel responsible for the information and safety of anyone in the shelter. The SSMS is responsible for providing real-time information that can help assist emergency personnel through location information, shelter capacity, and even human resource allocation. By using the dashboard, emergency personnel can quickly be brought up to speed to the current state of emergency and shelter status.

Family Members/Loved Ones: Individuals who are concerned about the safety and location of their evacuated relatives. Their motivation for using the Smart Shelter Management System is the ability to locate and review updates on the status of their loved ones through the Family Reunification portal. This portal provides the ability to search for evacuees by name, verify what shelter they are at, and reconnect with loved ones during these times of crisis.

Secondary Users:

Government Agencies: Government agencies responsible for disaster response and management, such as the Federal Emergency Management Agency, local emergency management agencies, and public health departments. Government agencies could utilize the SSMS (Smart Shelter Management System) to gather real-time data on shelter populations, assess resource needs for each, and coordinate response efforts. This would lead to enhance the effectiveness of disaster response operations, lower the impact of the disaster on affected communities, and guarantee compliance with regulatory requirements.

Technology Providers: Companies or organizations that specialize in developing and providing smart sensor technology, wearable devices, and software solutions for disaster management and response. Technology providers will be motivated to develop and offer the (SSMS) as a product or service to address the growing demand for innovative solutions regarding disaster response and management. By offering a reliable and effective system, enabling them to expand their market presence, generate revenue and contribute to public safety and disaster efforts. Primary motivation would be driven by capitalizing on the market opportunities, demonstrating their expertise, and contributor to societal weel-being by supporting emergency preparedness.

Volunteer Organizations: Vital Stakeholders in disaster response and recovery efforts that would benefit from increased efficiency during a disaster. Volunteer Organizations provide essential resources such as food, water, clothing, medical supplies, and more to support evacuees. With SSMS these organizations can get real-time data on shelter capacity, resources, and staffing allowing for more efficient use of their

FOR EDUCATIONAL PURPOSES ONLY

resources overall. This information can be used to further increase Visibility and Accountability as an accurate way to keep track and show what resources were used and how they were distributed. This increases trust amongst the stakeholders, allowing for more resources down the **line.**

Research Institutions and Academia: Research institutions, academic institutions, and universities in many cases conduct studies and research projects related to disaster management, emergency response and public safety. Research institutions and academia can utilize the Smart Shelter Management System to obtain valuable information on evacuee behavior, shelter operations and disaster response strategies. By gathering anonymized data from the system researchers can have insights on evacuee behavior, shelter operations and disaster response strategies in different areas and in different circumstances. The Primary motivation of such would be to contribute to the advancement of knowledge in the field of disaster management and enhance preparedness and response strategies.

Media and Communication Outlets: Would play a crucial role in disseminating information during disaster events, providing updates to the public. Media outlets can leverage the smart Shelter Management System to access accurate and real-time data on shelter populations, evacuation statuses and relief operations. information enables them to report on the situation effectively and provide updates to any concerned individuals to facilitate communication between evacuees and their loved ones. Their primary motivation would be to fulfill their role as information providers, enhance public understanding of the disaster situation in that area, and promote transparency and awareness.

FOR EDUCATIONAL PURPOSES ONLY

Features:

1. **Wearable Smart Tags for Evacuees**

- Requirement Type: Customer Based
- IOT Stack Involvement: Perception/ Sensing Layer
- Justification: These tags are the primary interface for evacuees, incorporating sensors to detect and identify individuals within shelters

2. **Real-Time Location Tracking**

- Requirement Type: Backend
- IoT Stack Involvement: Software/Communications
- Justification: Involves the sensing layer to collect location data through sensors and the processing layer to analyze and interpret this data to provide real-time tracking information.

3. **Centralized Management Dashboard**

- Requirement Type: Customer-based
- IoT Stack Involvement: Cloud Applications
- Justification: This dashboard is the application through which emergency personnel interact with the system, managing data and insights generated by backend processes.

4. Automated Check-In/Out System

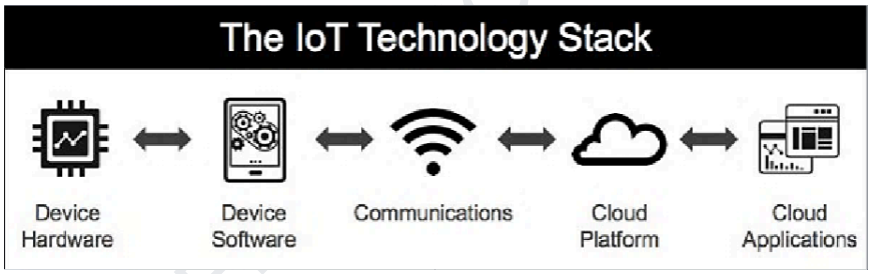
- Requirement Type: Customer-based and Backend
- IoT Stack Involvement: Device Hardware/Software and Communications layer
- Justification: Involves sensing for the initial registration and detection of evacuees and the application layer for processing check-in/out transactions on the user interface.

5. Capacity Management and Monitoring

- Requirement Type: Backend
- IoT Stack Involvement: Cloud platform/Cloud applications
- Justification: This will involve customers being able to monitor the status of those they are watching out for and the organization managing the data and altering it if needed.

6. Emergency Notification System

- Requirement Type: Backend
- IoT Stack Involvement: Communication/Cloud applications
- Justification: This will notify emergency services, if necessary, and ping the customer dashboard with information to family and friends to tell them that the person is with emergency services and what hospital.



FOR EDUCATIONAL PURPOSES ONLY

Identification of Data Elements:

Evacuee Location Data

Type of Data: Sensor data (GPS Coordinates)

Functionality: Real-Time Location Tracking

Collection/Processing: Collected by wearable smart tags, and process on the device

Input Data: Evacuees

Stakeholders: Evacuees are motivated by the idea of increased safety and security during a disaster/event. This data is beneficial in keeping them and their loved ones safe during such stressful situations.

Evacuee Check-In/Out Data

Type of Data: Input Data (timestamp and unique Id)

Functionality: Automated Check-in/Out System

Collection/Processing: Collected at the shelter entrance/exit, processed on the centralized management dashboard.

Input Data: Evacuees/Emergency Personnel

Stakeholders: Evacuees are motivated to check in and out to gain access to all the shelter's resources and understand this data can help keep track of where people end up and where they could have gone in the event of an emergency.

Shelter Capacity Data

Type of Data: Numeric data (number of available beds and capacity percentage)

Functionality: Capacity Management/Monitoring

Collection/Processing: Processed in the cloud to get accurate capacity counts.

Input Data: System Admins/automatic input based on Check-in/Out Data

Stakeholders: Emergency personnel/system administrators are motivated by the need to efficiently manage shelter resources and capacities. With up-to-date data this can be easier to understand what needs to be done at the shelter.

FOR EDUCATIONAL PURPOSES ONLY

Historical Evacuee Movement Data

Type of data: Time-stamped geographic coordinates anonymized.

Functionality: Efficient Resource Allocation.

Collection/Processing: Collected through wearable health sensors and processed for anomaly detection. This method allows for efficient analysis of past movement data for disaster response optimization while protecting sensitive information.

Input Data: Evacuees using the wearable devices.

Stakeholders: Emergency management agencies for improving disaster response strategies based on past events. A plan for collecting and assessing anonymized location data from wearable smart tags in order to overcome the lack of previous evacuee mobility data. Better resource allocation, more focused disaster response plans, and improved situational awareness during emergency situations will all be made possible by this data.

User Feedback Data

Type of data: Text Data (Feedback and Suggestions) Anonymized

Functionality: Overall improvement to the software

Collection/Processing: Collected and processed on the backend which will be viewable via the centralized dashboard.

Input Data: Evacuees, loved ones, and emergency personnel

Stakeholders: Evacuees and loved ones would be motivated to provide feedback to increase the ease of use of the overall application that helps keep themselves and their loved ones safe during a disaster. Emergency personnel would be inclined to provide feedback to make the application more user friendly and efficient to use during stressful situations. All user reviews would be looked over to see if they were relevant so user reviews would not cause poor service down the line.

Emergency Notification Data:

Type of data: Text data (emergency message, and evacuee information)

Functionality: Emergency Notification System

Collection/Processing: Processed on the centralized dashboard and sent out on the communication layer.

FOR EDUCATIONAL PURPOSES ONLY

Input Data: Emergency Personnel issuing the emergency message and automated systems updating loved ones on location data

Stakeholders: Emergency Personnel would be motivated to help ensure the safety of evacuees while keeping everyone up to date on what is happening. This helps decrease the tension amongst the evacuees and increases efficiency among the personnel.

Health Status Data

Type of data: Numeric and categorical (vital signs, health conditions)

Functionality: Efficient Resource Allocation

Collection/Processing: Automated analysis for identifying health emergencies.

Input Data: Wearable health monitoring devices or manual input from medical staff.

Stakeholders: Medical staff and emergency responders are more motivated to ensure the well-being of evacuees. By continuously monitoring health data, these stakeholders can promptly identify and respond to potential health emergencies.

Identification Data

Type of Data: Text data (personal information)

Functionality: Streamline future registration process

Collection/Processing: Collected via the app and processed in the cloud

Input Data: Evacuees

Stakeholders: Evacuees would be motivated to speed up the process of entering a shelter in the event of a disaster using data from previous registrations whether from previous disasters or preregistration via the app.

Real-Time Data Access: Access to both real-time and historical data must be governed by strict policies, role-based access controls, and auditing mechanisms to ensure data security and privacy

Shelter Staff and Volunteers: Need access to real-time data to manage daily shelter operations, including evacuee check-ins and check-outs, resource allocation, and emergency responses within the shelter. Real-time access allows them to make immediate decisions based on current shelter conditions and occupant needs.

FOR EDUCATIONAL PURPOSES ONLY

Emergency Response Coordinators: Require access to real-time data across multiple shelters to oversee and coordinate the broader emergency response, including reallocating resources, adjusting to changing shelter capacities, and ensuring overall safety and efficiency.

Evacuees: Should have limited real-time access to information relevant to their immediate well-being, such as shelter rules, available resources, and emergency notifications.

Historical Data Access:

Emergency Management Agencies and Planners: Need access to historical data for post-event analysis, planning, and improving future disaster response strategies. This data can provide insights into shelter utilization patterns, resource effectiveness and overall system performance during past events.

Government Agencies: May require access to aggregated historical data for policymaking, funding allocations, and regulatory compliance purposes, ensuring that disaster preparedness and response measures are data driven.

Researchers: With proper ethical approvals and privacy considerations, researchers might access anonymized historical data to study disaster response dynamics, improve evacuation and sheltering models, and contribute to the academic body of knowledge on disaster management.

Special Considerations:

Family Reunification Portal Users: Family members and loved ones should have restricted access to real-time data, specifically the location information of evacuees, subject to strict verification process and privacy controls to protect evacuee information.

Healthcare Providers: In cases where medical attention is needed, healthcare providers may need conditional access to both real-time and historical health related data of evacuees, under strict privacy and consent protocols.

Legal and Compliance Officers: May require access to both real-time and historical data ensure the system complies with relevant laws, regulations, and standards, and to respond to legal inquiries or audits.

FOR EDUCATIONAL PURPOSES ONLY

Edge Vs. Cloud processing

The Smart Shelter Management System will benefit the most from a hybrid analytics approach that integrates edge and cloud computing resources to improve many aspects of the system's

performance. For this system to be responsive in real time and can make decisions right away, edge analytics are essential. Critical activities like tracking evacuees' locations in real time and quickly identifying emergencies or safety risks within shelters can be effectively handled by processing data locally at the edge, using said wearable devices and smart sensors. Given this, the system is more resilient to disaster occurrences and can respond quickly even in situations where network access is inconsistent or intermittent.

Conversely, cloud analytics enhances the SSMS by offering the scalability and computational capacity that is required for sophisticated data analysis and long-term insight. Edge device processed data is sent to centralized cloud servers for additional analysis and archiving, making it easier to spot irregularities, trends, and long-term patterns. Cloud based analytics perform predictive analytics to forecast shelter resource requirements, anomaly detection to identify unusual patterns in evacuee behavior, and optimization algorithms to enhance shelter management operations. These techniques, such as machine learning and AI algorithms, are made possible by said cloud-based analytics.

Analytics:

Descriptive Analytics:

Shelter Population Dynamics: Analyzing historical data on shelter populations can provide insights into patterns of evacuation, peak times of shelter occupancy, and demographic information of evacuees.

Resource Utilization: Descriptive analytics can track the usage of resources such as food, water, medical supplies, and shelter space over time.

Evacuee Movement Patterns: Analyzing the movement of evacuees within shelter and between different shelter locations can reveal trends and hotspots. This information can inform decisions regarding the placement of resources, the allocation of staff, and the implementation of crowd management strategies to ensure the safety and well-being of evacuees.

Predictive Analytics:

Shelter Capacity Forecasting: Predictive analytics can forecast future shelter capacities based on historical data, current trends, and projected evacuation patterns. By anticipating surges in demand for shelter space, emergency personnel can proactively prepare additional resources, such as blankets and sanitary facilities, to accommodate evacuees effectively.

Resource Demand Prediction: Predictive analytics can forecast the demand for essential resources, such as medical supplies based on factors such as the size and demographics of the shelter population, health conditions and the severity of the disaster. By

FOR EDUCATIONAL PURPOSES ONLY

accurately predicting resource needs, organizations can ensure timely procurement and distribution of supplies avoiding shortages to shelters.

Evacuation Route Optimization: Predictive analytics can optimize evacuation routes based on factors such as traffic patterns, road conditions, and geographic constraints. By identifying the most efficient and safe evacuation routes.

Prescriptive Analytics:

Resource Allocation Optimization: Prescriptive analytics can recommend optimal resource allocation strategies based on predictive insight and predefined objectives, such as minimizing costs, maximizing resource utilization, or ensuring equitable distribution by generating data-driven recommendations, organizations can make informed decisions regarding the allocation of resources, balancing the needs of different shelter locations and prioritizing critical areas.

Emergency Response Planning: can recommend optimal emergency response plans based on predictive insights into potential scenarios, such as natural disasters, pandemics, or mass evacuations. This can be done by generating different response strategies and assessing their potential impact, organizations can identify the most effective courses of action, preset resources efficiently and coordinate efforts across multiple agencies and stakeholders.

Continuous and Future Improvements: Perspective analytics can support a whole variety of ongoing and continuous improvement by identifying areas for optimization, evaluating the effectiveness of interventions and bettering strategies based on the feedback and outcomes. By unanimously gathering the data and analyzing the performances of such, organizations can enhance their management in disaster events.

Flow of Data Through the IoT Stack:

Wearable Smart Tags for Evacuees: This will be an IoT device that the evacuees will need to wear so it will start off as a hardware device. Next it moves to step two of the process which is the device software as the device will now use its software to track data and location to move to its last step with is step three where it will communicate to other software to share the data.

Real-Time Location Tracking: This will start from the device software as it is software that will be collecting location data to then move to its next step of communicating this with other software to later be stored and used to monitor the stored data.

Centralized Management Dashboard: This will be in the last step, step five as this will be primarily what users will be interacting with as it is the endpoint of all collected data as it will not have read and recorded all recent data to then be displayed within a dashboard that users can see and interact with.

FOR EDUCATIONAL PURPOSES ONLY

Automated Check-In/Out System: This will start from the device hardware layer as it will be a physical sensor that will be pinged with it is checked in or out which will move it to the second layer of recording this to the devices software. Lastly it will communicate from the device to other backend software that will push it further up the layers.

Capacity Managment and Monitoring: This will start from the cloud platform where it holds compiled data from other backend software that communicated the data. It will then move the data to the cloud applications as a section that will allow users to manipulate and control the data that is loaded on the cloud servers.

Emergency Notification System: This will start from the communication layer which is where it will either communicate locational information to outside software that is not within our cloud software; which would ping emergency responders for example, or, to our cloud applications allowing our users to be pinged by specific notifications.

Device Hardware (Layer 1)

Devices Involved: Wearable Smart Tags for Evacuees, Sensors in Shelters

User Requirement Met: Evacuee tracking at the point of interaction. The hardware captures initial data such as identity (via the tags), location within the shelter, and time of interaction.

Process: Evacuees are assigned wearable smart tags which are detected by sensors. This layer represents the physical devices that initiate the data lifecycle.

Device Software (Layer 2)

Devices Involved: Firmware on Sensors, Embedded Software on Wearable Tags

User requirement Met: Real-Time Processing on devices, like immediate data validation, preliminary analysis, or local decision-making.

Process: The software on the devices processes the raw data from the tags to prepare it for transmission. This can include timestamping, source identification, and basic data checks.

Communications (Layer 3)

Devices Involved: Networking Equipment (Routers, Gateways)

User Requirement Met: Real-Time Location Tracking, Emergency Notification System, Automated Check-In/Out System

Process: Data is transmitted from the hardware to the cloud platform using various communications protocols. This layer ensures secure and reliable data transmission

FOR EDUCATIONAL PURPOSES ONLY

Cloud Platform (Layer 4)

Devices Involved: Cloud Servers and Databases

User Requirement Met: Capacity Management and Monitoring

Process: Cloud servers receive the data, where further processing and storage occur. This involves more complex operations like data analytics, historical tracking, and integration with other data sources. It also serves as the central repository for all collected data.

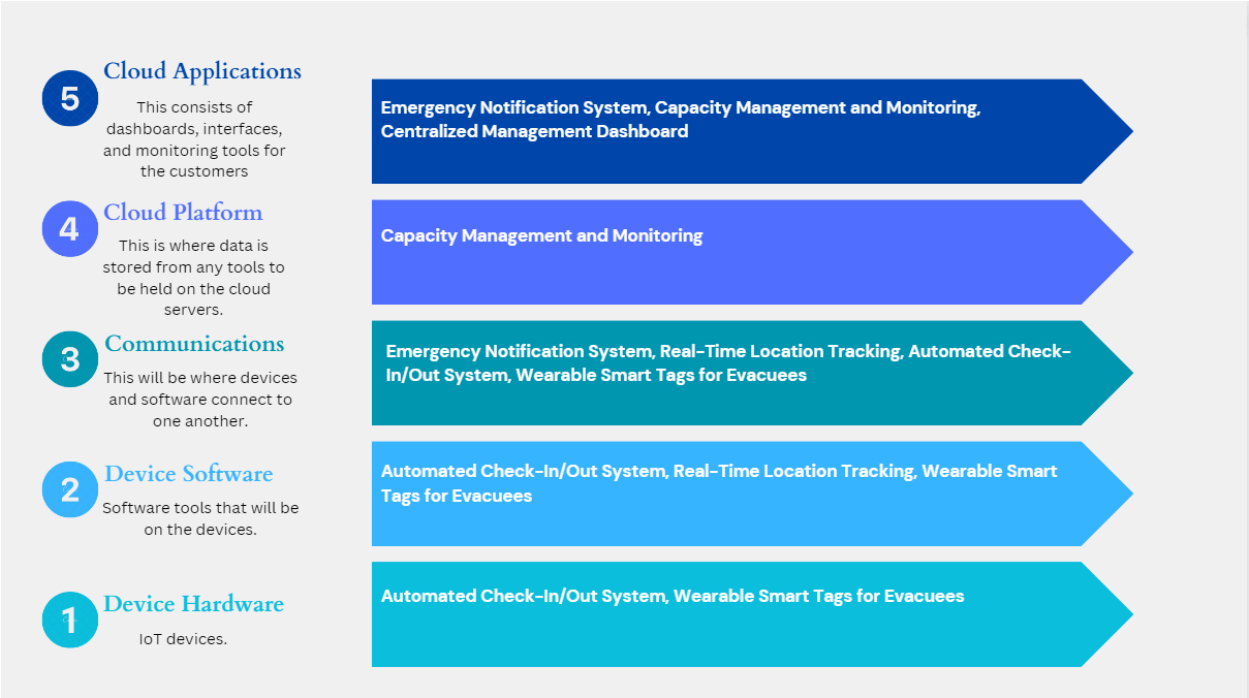
Cloud Applications (Layer 5)

Devices Involved: User Interfaces (Web Portals, Mobile Apps)

User Requirement Met: Centralized Management Dashboard, Emergency Notifications System, Capacity Management and Monitoring.

Process: Processed data is made actionable through various applications. Shelter staff can monitor and manage shelters through the dashboard, while the emergency notification system disseminates critical information. The public can access evacuee information through the reunification portal. With appropriate privacy controls and access management

FOR EDUCATIONAL PURPOSES ONLY



Sensor devices



Montion Sensors: Montion sensors, particularly Passive infrared (PIR) sensors from Honeywell would play a significant role in Smart Shelter Management Systems (SSMS). These sensors, known for their reliability and accuracy, will be strategically placed at key locations throughout the shelter premises to monitor activity levels and occupancy patterns. By detecting changes in infrared radiation that is caused by body heat and movement, Honeywell PIR sensors can accurately identify when individuals enter or exit designated areas within the shelter. In addition to detecting motion, the Honeywell motion sensors integrated into the SSMS are equipped with advanced capabilities to accurately count the number of people entering or exiting the shelter. This functionality is achieved through sophisticated algorithms that analyze motion patterns and distinguish between individual movements. By utilizing Honeywell's

FOR EDUCATIONAL PUR

expertise in sensor technology, the system maintains administrators to monitor capacity levels and allocate resources effectively. The ability to count the number of people entering or exiting the shelter, facilitated by Honeywell motion sensor, offers several benefits for emergency management and response efforts. Shelter administrators can use this data to ensure compliance with occupancy limits, prevent overcrowding, and facilitate orderly evacuation procedures if necessary. Furthermore, the accurate tracking of shelter occupancy enables administrators to make informed decisions regarding resource allocation, such as food, bedding, and medical supplies, based on actual demand.



.

People Counter: A people counter is a device that tracks the number of individuals entering and exiting a specific area or premises. The most common method to count people is using an Infrared sensor which is a component that emits an infrared light beam across a gap in this case an entrance or and exit that detects an interruption within the beam to count the number of individuals passing through. Once the beam is interrupted the sensor registers a count and the software on the device increments the display on the device. This data can also be leveraged for data logging giving the shelter an overall idea of how many people they may need to accommodate in the future. This further increases the overall security allowing emergency personnel to have a real-time idea of how many people the shelter can accommodate before having to close off entry.





Geo Location Sensors: The integration of Garmin's GPS-based geo-location sensors and devices into the Smart Shelter Management System (SSMS) presents a significant enhancement to the system's capabilities in tracking and managing evacuees during disaster events. By incorporating Garmin's GPS technology, the SSMS can provide real-time monitoring

of evacuee locations within the shelter and its vicinity. Evacuees equipped with Garmin devices can be continuously tracked, and their location data communicated to the SSMS platform via wireless connectivity or cellular networks. This data integration enables shelter administrators and emergency responders to access live updates on evacuee whereabouts through the SSMS user interface, facilitating efficient monitoring and management. Additionally, Garmin's geo-location data can trigger alerts and notifications based on predefined criteria, enhancing safety measures, and enabling targeted communication with evacuees. Furthermore, integrating Garmin's technology with other components of the SSMS, such as resource management and communication systems, optimizes resource allocation and logistics planning while improving overall shelter operations and response efforts during disasters.

Communication protocols used for interconnectivity

Wi-Fi Use Protocol on Selected Sensors: For motion sensors, particularly Passive inferred (PIR) sensors and Proximity Sensores from Honeywell, the communication protocol would involve a wireless connection such as Wi-Fi either a Wi-Fi 5 that it operates in both 2.4 GHz and 5 GHz frequency bands or in Wi-Fi 6 that us highly recommended for a much faster band and connectivity. These protocols enable real-time transmission of motion detection data from the sensors to the SSMS, allowing administrators to monitor activity levels and occupancy patterns within the shelter premises. Additionally, the proximity sensors would transmit data regarding individuals' proximity to designated areas within the shelter, complementing the information provided by motion sensors to enhance accuracy in tracking and counting.

Cellular and Satellite Use Protocol on Selected Sensor: In the case of geo-location sensors, such as Garmin's GPS-based devices, the communication protocol would involve wireless connectivity, such as cellular networks or satellite communication, to transmit location data to the SSMS platform. Garmin devices equipped with GPS technology continuously track evacuees' locations, and this data is transmitted in real-time to the SSMS, enabling administrators to monitor evacuees' whereabouts and facilitate efficient management of shelter resources. The communication protocol used for geo-location sensors ensures seamless integration with the SSMS, allowing for accurate tracking and management of evacuees during disaster events.

Gateway Devices

AirLink XR90: This device is an advanced industrial-grade router designed for high-speed connectivity and reliable communication in demanding IoT situations. The AirLink router supports many features including 5G connectivity allowing this router to work about anywhere with nearby cell towers in the case of lacking ISP connections. The AirLink comes with multiple ethernet and Wi-Fi interfaces providing greater flexibility for various devices. As with every IoT

FOR EDUCATIONAL PURPOSES ONLY

application security is a top priority with VPN (Virtual Private Networks) support, firewall protection and in the case of a Cyber Attack a secure boot to limit data transmission. This can all be configured through remote management, allowing administrators to monitor and control the device as needed when dealing with large-scale deployments. Because of its Industrial design the AirLink can withstand extreme temperatures, humidity, and vibrations making it suitable for various disasters and events that may happen.

In the event of a disaster, the router has network redundancy, allowing it to fall back onto WAN, 5G, or 4G depending on what is available. This allows the shelter to stay up and running in most scenarios allowing for consistent connectivity with loved ones and emergency personnel who are not on site. Integration of other devices is simple with the use of built in wireless technology or can be adapted with the use of breakout boards though serial or other connectors. Once connected the data can be processed in real-time, perform analytics, and give overall insights on the information passing through allowing for better and faster decision making. The AirLink can be used to transmit processed data to the cloud platform allowing emergency personnel and stakeholders to be involved and informed about the disaster response. Overall, the Airlink offers many useful features in the event of a disaster allowing the SSMS system to work efficiently and effectively.



Local Servers

A local server would be needed to provide continuity in the case of WAN and 5G connectivity loss since this type of situation can happen during a hurricane, earthquake, etc. Many servers

could work and could change depending on where the shelters are located such as a football stadium would have a robust network that could be changed to accommodate the SSMS. In the case of a new shelter the **BAM Servers | 3rd Gen Xeon® SP** would be suitable since it is designed for more rugged situations offering only SSD and NVME slots since HDD are more susceptible to outside factors. This server would be used for Data Logging, Offline functionality, Data Processing/Analytics, and backup in the case of an outage. This would allow for the data from SSMS to be stored while waiting for either 5G or WAN to come back online whether the data could then be uploaded to the cloud. The server could also be used for real-time monitoring, processing, and user interactions in case the router is unable to keep up with all the information given.

Analytic Software

Technology for Analyzing Data:

Incoming from Devices: Data analytics platforms such as Apache Spark or Hadoop could be employed for processing large streams of real-time data from sensors and wearable devices. These systems can handle vast volumes of data, providing both batch processing and stream processing capabilities.

Incoming from End Users at the Site: User interaction data, such as manual check-ins or assistance requests, could be analyzed using a Customer Relationship Management (CRM) system integrated with the IoT platform. This system can track user interactions and provide insights into usage patterns and service requests.

Incoming from Customers: Feedback and usage data from the Family Reunification Portal could be analyzed using analytics tools integrated within the web application stack, like Google Analytics or a custom analytics pipeline built using machine learning services provided by cloud provider like Microsoft Azure.

Analytics Provided:

User Organization or Employees:

Evacuee Distribution: Aggregate statistics on evacuee distribution across different shelters.

FOR EDUCATIONAL PURPOSES ONLY

Shelter Occupancy Trends: Historical and predictive analytics on shelter occupancy and capacity utilization.

Resource Allocation: Analysis of resources versus demand to optimize distribution.

Evacuee Flow: Movement patterns of evacuees within and between shelters.

Incident Reports: Aggregated data on incidents within shelters for improving safety measures.

End User:

Personal Check-In/Out History: Individual records of check-in and out times.

Alerts and Notifications History: Log of all alerts and notifications received.

Shelter Resources Availability: Information on current availability of shelter resources.

Mobile Device Software

Communication with the Product Solution:

Mobile device software will communicate with the SSMS primarily through secure APIs over encrypted connections. It will be able to send data such as manual check-ins, status updates, and receive information like notifications, shelter status, and resource updates.

Data Exchange:

Data Received: Evacuee location updates, shelter status reports, emergency alerts, and resource availability.

Data Sent: User feedback, check-in/out confirmations, and resource requests.

Supported Mobile OS Platforms:

Primary: iOS and Android, due to their extensive market share and developer support.

Secondary (if viable): Other platforms like HarmonyOS or niche market OS could be considered based on the geographic location and user demand.

Supported Form Factors:

Phones and Tablets: Primary devices due to their widespread use among the general population and emergency personnel.

FOR EDUCATIONAL PURPOSES ONLY

Smart Watches: As secondary devices for receiving alerts and notifications, especially for personnel actively working in the field during a disaster.

Cloud services platform – Microsoft Azure

By using the cloud platform, Microsoft Azure, it aids in the developers for creating cloud applications for both mobile and web. As well as providing other features and support for security, databasing, project management, and many more features that would be beneficial for us to utilize for our product.

IoT – Given what has been provided, facilitating effective real-time notification, analytics, and data collecting. Sensors and other IoT devices installed in shelters can be safely connected and managed by the SMSS by utilizing Azure IoT Hub. Authorized users can now more easily acquire up-to-date information on resource consumption, evacuee locations and shelter conditions, enabling them to make informed decisions.

Networking - With the networking provided by Microsoft Azure we will be able to gather diagnostics and manage traffic information to help protect against any DDoS attacks or even load balancing as this will better improve the response times. Utilizing Azure's networking capabilities, the SMSS enhances performance, security, and resilience; in turn this improves emergency shelter operations' efficacy during disaster occurrences.

Databases - With access to database services like Azure SQL Data or Azure Cosmos DB we can get support in database integration as well as getting SQL support without having to get a SQL server. This will help with compiling data and being able to allow users to archive as well pull-out specific data.

Intergration - We are provided integration support which is helpful as there is a server backup feature as well as site recovery which is useful when dealing with massive amounts of locational data. Another support process provided in this instance is a visual designer tool for creating automated processes connected to onsite premises systems, or third party API's, in order to improve SMSS's interoperability between data sources.

Mobile - We would be supported with products that can help our developers build APIs with the ability for geospatial data which would help us provide data dealing with temporal information

FOR EDUCATIONAL PURPOSES ONLY

relating to the events of a disaster, for example an earthquake. This would be able to gather timing and location data that can contribute to our overall analytics.

Web - With web services we are given support for both development, deployment, and management of the web applications. We can also use API management through this service as well. Additionally, it may securely expose its functionality to external stakeholders while managing access and usage thanks to API governance and monetization.

Security - There are several types of security services provided, but the most important is that we can see and respond to cloud security threats, which is important to our product as it relies on storing most of its data via the cloud. We are also able to manage encryption keys this way which is important as with dealing with sensitive data encryption is an important aspect.

Containers - With the support and provided services for container management we are able to create and manage large amounts of containers within the Azure cloud which is important to our product as with containers we can use platforms like Kubernetes that create containers to help us manage our applications with intense support that can get rid of having a physical person constantly automating day-to-day operations or constant storage management as the platform itself can be commanded to do this which allows our teams to focus on other important matters, for instance; strong cyber-attacks or intense bug fixes.

FOR EDUCATIONAL PURPOSES ONLY

Time-based aspect of monetization:

Government/Non-Profit Agencies:

Charges for government agencies responsible for disaster response and management may be structured annually. This could involve licensing fees or subscription charges for accessing and utilizing the SSMS platform to gather real-time data on shelter populations, assess resource needs, and coordinate response efforts. An annual billing cycle ensures that government agencies have continuous access to the system's capabilities for monitoring and managing disaster situations throughout the year.

Family and Loved Ones: Subscription-Based (Annual): This option provides family members with continuous access to the SSMS platform throughout the year, allowing them to search for and receive updates on the status and whereabouts of their evacuated relatives at any time. Charges would be billed annually, ensuring uninterrupted access to the system's features and services. The annual subscription model offers convenience and peace of mind to family members, knowing they have ongoing access to vital information during disaster events.

Per-Use Cycle (Optional) For at Higher Risk States: As an alternative to the annual subscription model, family members may use the SSMS per-use. Under this charging model, charges would be incurred each time they access the system to search for and receive updates on the status and whereabouts of their evacuated relatives. This option is suitable for those who prefer a pay-as-you-go approach or anticipate sporadic usage of the system, particularly during rare or unforeseen disaster events. It offers flexibility and cost-effectiveness for users with minimal or occasional need for the SSMS platform.

For third-party organizations such as non-profits, community groups, or businesses, seeking to utilize the Smart Shelter Management System (SSMS) to support disaster response efforts, the monetization strategy can include a licensing option. Here's how it can be structured:

Licensing Option (Annual):

Under this option, third-party organizations can obtain a license to use the SSMS platform for a specified period, typically on an annual basis. Charges would be billed annually, providing organizations with ongoing access to the system's capabilities for managing shelter operations, coordinating emergency response efforts, and accessing real-time data and insights. The annual licensing model offers flexibility and scalability for organizations, allowing them to tailor their usage of the SSMS based on their needs and resources.

Subscription-Based (Optional):

As an alternative or complement to the licensing option, third-party organizations may have the option to subscribe to additional features or support services offered by the SSMS provider. This could include access to premium features, priority technical support, or customized training and implementation assistance. Charges for subscription-based services would be billed separately from the annual licensing fee, providing organizations with the flexibility to choose the level of support and functionality that best meets their requirements.

By offering a licensing option for third-party organizations, the SSMS provider enables these entities to leverage the system's capabilities to enhance their disaster response efforts, support evacuees, and contribute to community resilience. The annual licensing model ensures that organizations have continuous access to the SSMS platform, while optional subscription-based services allow them to further customize their experience and maximize the value derived from the system.

FOR EDUCATIONAL PURPOSES ONLY

Probable Costs

Device costs

GPS Bracelets: 1.46-unit cost at 1000 quantity.
GPS 18x OEM USB: 85-unit cost at 1 quantity.
Airlink XR90: 2000-unit cost at 1 quantity.
People Counter: 207-unit cost at 2 quantity.
Motion Sensors: 70-unit cost at 10 quantity.
Local Server: 5000-unit cost at 1 quantity

Service costs

Cloud Service via Microsoft Azure: 4000 Monthly

Cost Breakdown Table to produce product

ITEM DESCRIPTION	AMOUNT
5k Unit GPS Chip	$4,950.00
5k Unit Bracelet	$2,350.00
Cloud Services Monthly	$4,000.00
Subtotal	$11,300.00

ITEM DESCRIPTION	AMOUNT
1 GPS Chip	$0.99
1 Bracelet	$0.47
Subtotal	$1.46

Sample price chart for a hypothetical customer organization:

RPOSES ONLY

SSMS

SMART SHELTER MANAGMENT SYSTEM

SILVER PACKAGE

$5000

- GPS Bracelets
- GPS 18x OEM USB
- Software + Cloud Service (1 Year)

GOLD PACKAGE

$9000

- GPS Bracelets
- GPS 18x OEM USB
- People Counter
- Software + Cloud Service (1 Year)

PLATINUM PACKAGE

$20000

- GPS Bracelets
- GPS 18x OEM USB
- AirLink XR90
- People Counter
- Motion Sensors
- Software + Cloud Service (1 Year)
- Local Server

OSES ONLY

Cost breakdown table of charges to the customer.

Prodcuts:	Unit Cost:		Quantity:	
GPS Bracelets	$	1.50		1,000
GPS 18x OEM USB	$	200.00		1
Software+Cloud Service	$	2,000.00		1
AirLink XR90	$	2,000.00		1
People Counter	$	500.00		2
Motion Sensors	$	500.00		10
Local Server	$	6,300.00		1
Service Fee	$	2,000.00		1
Total	$	13,501.50		

X Company is a start-up shelter organization that has built up their own location and is seeking equipment for their first intended disaster in a few months. They expect to have at least a thousand evacuees stationed at this location. Above is a detailed table of charges that will be given to the company to break down the cost of the Platinum package that aligns with everything they would want.

Monetizing

Subscription-based Model: Customer organizations can be charged a recurring subscription fee based on the features and usage levels they require. Different subscription tiers can offer varying levels of functionality, support, and scalability. The frequency of charges will be monthly or annual charges. It will depend on the customer's preference and budgeting cycle.

Per-User or Per-Shelter Licensing: Charge customer organizations based on the number of users or shelters they need to manage with the SSMS. This can be a one-time licensing fee, or a recurring fee based on the number of users or shelters. It can be billed monthly or annually.

Customization and Integration services: Offer customization and integration services to tailor the SSMS to the specific needs and existing systems of customer organizations. Charge for consultancy services, customization, and integration services on a project basis or hourly rate. Billed based on the scope and duration of the customization/integration project.

Value-added Services: Provide additional value-added services such as advanced analytics, predictive modeling, or on-site support during emergency situations. Charge extra for premium features or add-ons that enhance the functionality and effectiveness of the SSMS. This can either be a one-time fee for specific services or bundled into the subscription plan with additional charges.

FOR EDUCATIONAL PURPOSES ONLY

Training and Certification Programs: Offer training and certification programs to customer organizations to ensure effective use of the SSMS by their staff. Charge for training sessions, workshops, and certification exams. The training sessions can be a one-time fee or bundled into the subscription plan with additional charges.

Demonstrating the product's value to potential customers

Case Studies and Testimonials: Share success stories, case studies, and testimonials from existing customers who have experienced the benefits of using the SSMS in real-world situations.

Product Demonstrations: Conduct live product demonstrations highlighting the key features and capabilities of the SSMS, emphasizing its ease of use, real-time monitoring capabilities, and ability to streamline shelter management operations.

Customized Presentations: Tailor presentations to address the specific points and challenges faced by potential customers, highlighting how the SSMS can address their unique needs and requirements.

Pilot Programs: Offer pilot programs or trial periods to allow potential customers to experience the benefits of the SSMS firsthand before committing to the full implementation.

ROI Analysis: Present a detailed ROI analysis demonstrating how implementing the SSMS can lead to cost savings, improved operational efficiency, and better resource allocation during disaster events.

Cost-Benefit Analysis: Present a detailed cost-benefit analysis to demonstrate the financial value proposition of the SSMS. Highlight potential cost savings, such as reduced administrative overhead, optimized resource utilization, and minimized operational disruptions, compared to traditional manual methods of shelter management and emergency response.

Return on Investment (ROI): Calculate the potential ROI of implementing the SSMS by quantifying the tangible and intangible benefits it offers. This could include factors such as improved safety and security for evacuees, faster response times during emergencies, enhanced coordination with external stakeholders, and greater regulatory compliance.

FOR EDUCATIONAL PURPOSES ONLY

Charging End Users

Regarding end users, it's less common to charge them directly for using the SSMS since they are typically beneficiaries of emergency shelter services during these disaster events. However, if there are premium features or additional services offered directly to the end users, like the family reunification portal access, a modest fee or subscription model could be considered. Alternatively, the cost of providing the SSMS to end users could be bundled into the overall service fees charged to customer organizations.

APIs for the Smart Shelter Management System (SSMS)

Existing APIs

GPS and Mapping Apis:

Example: Google Maps APIs

Functionality: Provide real-time location tracking, mapping, and geofencing capabilities which could be used for visualizing the location of shelters and tracking the movement of evacuees with GPS-enabled wearable devices.

IoT Device Management APIs:

Example: AWS IoT, Azure IoT Hub APIs

Functionality: Offer device registration, monitoring, and management functionalities necessary for maintaining a network of smart sensors and wearable devices.

Communication APIs:

Example: Twilio, SendGrid

Functionality: Enable the system to send notifications and alerts via SMS, email, or even voice calls to evacuees and staff.

CRM APIs:

Example: Salesforce API

Functionality: Provide functionalities to manage interactions with evacuees, track their check-in/out history, and maintain a log of services accessed.

Analytics APIs:

Example: Google Analytics, Mixpanel

Functionality: Track usage and interactions with the SSMS applications, giving insights into how the system is used by different user groups.

New APIs

If new APIs must be created for specific functionalities not covered by existing APIs, they will include:

FOR EDUCATIONAL PURPOSES ONLY

Evacuee Data Management API:

To handle the secure input, update, and retrieval of evacuee data in the system.

Resource Allocation API:

To manage the distribution and inventory of resources within shelters.

Shelter Capacity API:

To provide real-time data on the current capacity and vacancy status of each shelter.

Family Reunification API:

To securely manage queries from the public and match them against evacuee data for reunification purposes.

Healthcare Integration API:

To integrate with medical systems for sharing evacuees' health data where necessary and with proper consent.

Shelter Operations API:

To automate various shelter operations such as lighting, temperature control, and access based on shelter status and environmental conditions.

Open Source vs. Proprietary APIs

Open Source:

Could foster a community around the SSMS, allowing for collaboration and more innovation.

Potentially lower development costs as others can contribute to improving the API.

May be subject to more scrutiny, which can lead to more secure and robust code.

Proprietary:

Ensures full control over the API's functionality and its evolution.

Can provide a competitive advantage by offering unique functionalities not available elsewhere.

Allows for tight control over security, which may be crucial given the sensitive nature of the data handled by SSMS.

FOR EDUCATIONAL PURPOSES ONLY

Risk Matrix		Severity				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Software Bugs	Device Battery Failure	Malware Attacks	Malware Attacks	Unauthorized Access to Data
	Likely	Software Bugs	Device Battery Failure	Network Interruptions	System Overload	Failure of Wearable Device
	Possible	Temporary Loss of Non-Essential Features	User Error	Data Corruption	Cloud Platform Outages	Failure of Wearable Device
	Unlikelyh	Temporary Loss of Non-Essential Features	Reputational Damage Due to Minor Data Leaks.	User Error	Physical Device Damage	Compromise of API Security
	Rare	Minor Network Delays	Reputational Damage Due to Minor Data Leaks.	Wearable Tag Duplication	Supply Chain Attacks	Physical Device Damage

Possible Vulnerabilities Matrix

FOR EDUCATIONAL PURPOSES ONLY

High Likelihood and High Impact (Critical)

Unauthorized Access to Data: A breach could lead to exposure of sensitive evacuee information. This can be detected by frequent security checks but also having an active security software implemented.

Failure of Wearable Device: If the device fails, it could lead to incorrect tracking of individuals in a shelter. Having quality checks will aid in detecting if a device has already failed, but also during events having users alert the proper individuals of failure in the device.

Malware Attacks: Compromise the software integrity, leading to system malfunction or data theft. Keeping security protocols updated as well as active security monitoring will help detect any incoming attacks or ones that might have already happened.

System Overload During Disaster: The system may become overwhelmed due to a surge in users, leading to slowdowns or crashes. Having someone nearby and monitoring the system can aid in detecting any overworking as well as having a notification system to ping when the system is overloaded.

High Likelihood and Medium Impact (High Risk)

Network Interruptions: Disruptions in communication could prevent real-time updates. Having a notification system to ping when the network starts to become unstable will help detect any possible interruptions.

Data Corruption: Erroneous data could lead to misallocation of resources or misinform family members. Having a report system handy to take in any pings of data corruption being presented to users.

Device Battery Failure: Could cause gaps in data collection if not promptly addressed. Quality checks of the device and informing users to report any condition will help detect those with battery failure.

Medium Likelihood and High Impact (High Risk)

Compromise of API Security: Could lead to data leakage or unauthorized actions if API endpoints are not adequately secured. Having active security warning and a security ping system to notify if any compromised data is leaked.

Cloud Platform Outages: Dependence on cloud services means any outage could significantly disrupt operations. Monitoring of the clouds performance will aid in detecting if the cloud system has an outage.

Medium Likelihood and Medium Impact (Moderate Risk)

User Error: Misuse or incorrect use of the system by employees could result in data entry errors or operational inefficiencies. Having constant quality checking of the data entered can aid in detecting as well as a report system for users to put in anything that was an error.

Software Bugs: Could result in temporary loss of functionality or incorrect data processing. Having a ping system to ping if any bugs are detected as well as if any information is not fully processed.

FOR EDUCATIONAL PURPOSES ONLY

Low Likelihood and High Impact (Moderate Risk)

Physical Damage to Devices in Shelters: In the event of damage due to environmental factors, tracking could be impaired. Having quality check of the devices within the environment can aid in detecting if anything is damaged.

Supply Chain Attacks: Compromise of hardware before it arrives at the shelter could lead to a breach. Quality checks throughout the hardware process to ensure nothing is tampered with or damaged and security checks being used during the device testing to help detect any problems.

Low Likelihood and Medium Impact (Low Risk)

Reputational Damage Due to Minor Data Leaks: Small-scale breaches might not have significant operational impact but could affect trust. Having constant security tests can help detect any attacks.

Wearable Tag Duplication: Unlikely but could lead to incorrect tracking information if it occurs. Having quality checks on the device hardware and software can help detect if there is any duplicated devices.

Low Likelihood and Low Impact (Low Risk)

Temporary Loss of Non-Essential Features: Might affect user experience but not the core functionality. Having a user report system to ping if any features become down, inactive, or unavailable to users can help detect these types of problems.

Minor Network Delays: Could slow down system responsiveness but not significantly disrupt operations. Having software and network pings can help detect and alert if there is any disturbance in the network.

Controls in place to mitigate damages

Technological Controls

Encryption: Use of strong encryption for data at rest and in transit to protect information from unauthorized access.

Access Controls: Implement role-based access controls to ensure that users have the minimum necessary privileges to perform their job functions.

Authentication: Enforce multi-factor authentication for all users accessing the system, particularly for those with administrative access.

FOR EDUCATIONAL PURPOSES ONLY

Network Security: Utilize firewalls, intrusion detection/prevention systems and Virtual Private networks to secure traffic.

Regular Sofware Updates: Ensure all system software is up to date with the latest security patches and updates.

Data Backups: Perform regular data backups to enable system recovery in case of data loss or corruption.

Redundancy: Design the system with redundancy for critical components to ensure service continuity in case of failures.

Endpoint Protection: Equip all devices with anti-malware software and conducy regular scans for vulnerabilities.

Secure API Gateways: Use API gateways with Integrated security features to manage and secure API Traffic. Put access controls in place to prevent unauthorized users from accessing APIs.

Device management: Monitor the health of wearable devices and check for defects or malfunction by conducting quality tests. Offer consumers guidance on how to check the battery level of their devices and how to report any issues they may find. Provide capabilities to check battery status and inform users when battery levels are low.

User Error: Give consumers instructions and user manuals to help learn how to use the system properly. To ensure data accuracy and prevent errors, implement data validation tests.

Software Bugs: To find and correct software flaws, carry out comprehensive testing and quality assurance methods. Implement automated bug report and detection tools to handle issues as they arise.

Cloud Platform Outages: Adopt a multi-cloud strategy to reduce the operational effect of disruptions. Track the performance of the cloud platform and create alerts for any interruptions in service. To ensure uninterrupted operation during cloud disruption, keep backup systems as an alternative option.

Procedural Controls:

User Training: Conduct regular training sessions for users on security best practice and system use.

FOR EDUCATIONAL PURPOSES ONLY

Product Compliance

Smart Shelter Management System (SSMS) must ensure compliance with relevant laws and regulations is essential to uphold data privacy, security, and operational standers.

Data Protection Laws:

- **HIPPA (Health Insurance Portability and Accountability Act):**
    - Compliance with HIPAA is essential if the SSMS collects, processes, or stores protected health information (PHI) in the United States. This includes implementing administrative, physical, and technical safeguards to protect PHI, conducting regular risk assessments, signing business associate agreements (BAAs) with relevant parties, and providing individuals with rights over their health information.
- **Data Breach Notification Laws:**
    - Compliance with state data breach notification laws is crucial for the SSMS. Many states have enacted laws requiring organizations to notify individuals and government agencies in case of a data breach involving personal information. These laws typically specify the timeframe for notification and the content of notifications. Ensuring timely and accurate notification in the event of a data breach is essential to comply with these laws and maintain trust with affected individuals and authorities.

Emergency Management Regulations:

- **Federal Emergency Management Agency (FEMA):**
    - The SSMS must comply with FEMA regulations to align with federal standards for disaster response and management in the United States. This may include adherence to FEMA's National Incident Management System (NIMS) framework, which establishes protocols for incident command, communication, and coordination during emergencies. Additionally, compliance with the Stafford Act, which governs federal disaster response and assistance programs, is essential.
- **Federal Trade Commission (FTC) Regulations:**
    - The SSMS must comply with regulations enforced by the Federal Trade Commission (FTC), particularly regarding consumer protection and privacy. The FTC has authority over companies that engage in unfair or

FOR

deceptive practices related to consumer data privacy and security. Compliance with FTC regulations involves implementing appropriate data security measures, providing clear and accurate privacy notices to users, and obtaining necessary consent for data collection and processing activities.

- **Local Emergency Management Authorities:**
    - Compliance with regulations set forth by local emergency management authorities is necessary. These regulations could include requirements for evacuation routes, shelter capacities, emergency communication systems, and interoperability with other emergency response systems as mandated by state and local laws.

Accessibility Standards:

- **Section 508 of the Rehabilitation Act:**
    - Compliance with Section 508 ensures that the SSMS is accessible to individuals with disabilities as mandated by federal law. This involves designing digital content and user interfaces to be perceivable, operable, understandable, and robust for users with diverse abilities.
    - Ensuring compliance with digital accessibility standards, such as Section 508 of the Rehabilitation Act, is not only a legal requirement but also helps mitigate the risk of lawsuits alleging violations of the Americans with Disabilities Act (ADA). Non-compliance with ADA accessibility requirements for digital content and services can result in legal challenges and costly litigation. Therefore, adherence to accessibility standards is essential to minimize legal exposure and ensure equal access to the SSMS for individuals with disabilities.

Electronic Communications Privacy Act (ECPA):

- The Electronic Communications Privacy Act (ECPA) governs the interception of electronic communications and unauthorized access to electronic communications stored electronically. Compliance with ECPA is essential for the SSMS, particularly regarding the protection of communications transmitted or stored within the system. ECPA regulates the interception, disclosure, and access to electronic communications by law enforcement, government agencies, and third parties. It requires obtaining appropriate authorization, such as warrants or court orders, before intercepting or accessing electronic communications. Compliance with ECPA ensures that the SSMS safeguards the privacy and confidentiality of communications between evacuees, emergency personnel, and loved ones, and

protects against unauthorized access or surveillance of electronic data. Integrating ECPA compliance measures into the design and operation of the SSMS helps uphold individuals' privacy rights and ensures legal adherence to federal privacy regulations.

Industry Standards

Bluetooth: Bluetooth is among the most popular forms of a Communication Protocol. Most IoT devices include Bluetooth as a standard feature. Bluetooth allows data to be transmitted to other devices, commonly used in the form of smart watches and phones. Therefore, it is beneficial with our product to have it as a standard feature which will aid in the communication between our devices.

Data Distribution Service (DDS): Data Distribution Service, or DDS, is a common protocol used to communicate between hardware and software. With DDS protocol alongside our product, we will be able to trans high amounts of data transfers as high quality as well with low latency which will be beneficial to us.

Matter: With some of our parts/devices coming from a few different companies having this protocol will help allow stable enough communication between the devices. Matter will allow us to make a connection between some of our parts without forcing us to stick to one brand which also won't force the consumer to do the same as it will allow us to make a good connection between the different branded devices without having to commit to one or suffer at the chance of having a bad connection because without it they wouldn't be seen as compatible enough to provide a stable connection.

MQTT: Is a great open-source protocol that would work on our application layer. It would provide communication between our sensors and applications, allowing for easy transfers with low bandwidth, this is due to it being very lightweight and not taking up much memory space, which would be the most ideal. It is also very compatible with many industrial devices which will allow us to have a stable connection between all our industrial devices that we provide.

Appendix A: Incident Response Plan for Failure of Wearable Device

1.Incident Discovery and Notification

- **Discovery:** Any staff member or user who notices a failure or malfunction in the wearable device shall immediately report the incident to the designated IT support personal or system administrator.
- **Notification Procedure**
    - The person discovering the incident will contact the IT department's helpdesk or designated support personnel.
    - If necessary, the helpdesk or support personnel will escalate the incident to the IT emergency contact list or affected department contact list.
    - Grounds security office will log:
        - Name of the Caller.
        - Time of the Call
        - Contact information about the caller.
        - Nature of the incident.
        - Details of the equipment or persons involved
        - Location of the affected devices.
        - How the incident was first detected.

2.Incident Assessment and Response Strategy:

- **Assessment:**

FOR EDUCATIONAL PURPOSES ONLY

- Upon receiving the incident report, the designated IT staff member will conduct a detailed evaluation of the wearable device failure, considering its severity and potential consequences.
- This assessment will include an analysis of how the failure impacts the real-time tracking of evacuees and communication systems within the emergency shelters.
- The staff member will also assess the extent to which the failure poses a threat to the safety of evacuees and the efficient operation of the shelters.

- **Response Strategy:**
  - In the event that the assessment indicates a critical situation, the incident response team will be promptly activated to address the issue.
  - The response team will conduct a comprehensive examination to determine the scope of the failure and its implications for evacuee safety and shelter operations.
  - Based on this assessment, the team will prioritize actions to either restore the functionality of the wearable devices or implement alternative measures to ensure effective tracking and communication.
  - Throughout the response process, clear and timely communication will be maintained with all relevant stakeholders and management, providing regular updates on the situation and the progress of mitigation efforts.

3.Incident Categorization and Response Procedures:

- **Categorization:**
  - The incident will be categorized based on its severity and impact:
    - Category one – Threat to evacuee safety or life.
    - Category two – Threat to shelter operations and resources.
    - Category three – Disruption of essential services.
- **Response Procedures:**
  - Deploy appropriate procedures to address the specific failure of the wearable device, such as:
    - Isolating the affected device to prevent further disruption
    - Implementing manual tracking and management protocols for evacuees if necessary.

FOR EDUCATIONAL PURPOSES ONLY

- Initiating repairs or replacements for the failed device.

4.Documentation and Post-Incident Analysis:

- **Response Procedures:**
  - Maintain detailed records of the incident, including:
    - Discovery process.
    - Incident assessment and categorization.
    - Response action taken.
    - Effectiveness of the response measures.
  - Preserve evidence related to the failure for further analysis or investigation.
- **Post-Incident Analysis:**
  - Conduct a post-incident review to identify root courses and lessons learned.
  - Update procedures or protocols to prevent similar failures in the future.
  - Review and enhance training programs for staff members involved in emergency shelter operations.

5.**Continuity and Recovery:**

- **Continuity and Recovery:**
  - Implement interim measures to ensure continuity of shelter operations despite the wearable device failure.
  - Deploy alternative tracking or monitoring methods if available.
- **Recovery Process:**
  - Work towards restoring the functionality of the wearable device through repairs or replacements.
  - Test the restored device thoroughly to verify its reliability and effectiveness

6. External Notification and Reporting

A) Is the incident real or perceived?

The incident is real, as it involves a tangible failure of the wearable device used in the Smart Shelter Management System (SSMS). It has been reported by staff members and affects the functionality of critical systems.

B) Is the incident still in progress?

FOR EDUCATIONAL PURPOSES ONLY

The incident is ongoing, as the failure of the wearable device persists and threatens the operational efficiency of the SSMS.

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

The data threatened includes information related to evacuee safety, shelter operations, and resource management within the SSMS. The criticality of this data is high, as it directly impacts the safety and well-being of individuals relying on the emergency shelter.

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

The impact on the business would be critical, as the failure of the wearable device compromises the ability of the SSMS to effectively manage shelter operations and ensure the safety of evacuees.

E) What system or systems are targeted, where are they located physically and on the network?

The targeted system is the wearable device component of the SSMS, which is physically distributed across various locations within the emergency shelter facilities. On the network, these devices are interconnected with the central SSMS server for data processing and management.

F) Is the incident inside the trusted network?

Yes, the incident occurs within the trusted network environment of the emergency shelter facilities where the SSMS is deployed.

G) Is the response urgent?

Yes, the response is urgent due to the critical nature of the incident and its immediate impact on evacuee safety and shelter operations.

H) Can the incident be quickly contained?

The incident may be challenging to quickly contain, as it involves the failure of multiple wearable devices distributed throughout the shelter facilities. However, immediate actions can be taken to isolate affected devices and implement alternative tracking or management protocols.

I) Will the response alert the attacker and do we care?

Given that the incident involves a technical failure rather than a deliberate attack, the response is unlikely to alert any external attacker. The focus is on restoring system functionality and ensuring operational continuity rather than engaging with potential attackers.

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

FOR EDUCATIONAL PURPOSES ONLY

This incident falls under the category of system failure, specifically the malfunction or breakdown of the wearable device component within the SSMS infrastructure.

7. Incident Tickets

Given the vulnerability of the "failure of wearable device," the incident would likely fall under **Category Four - Disruption of Services** within the incident categorization. This category encompasses incidents that disrupt the normal functioning of services provided by the Smart Shelter Management System, which may impact the efficiency of emergency shelter operations.

8. Follow a Procedure

Based on the incident assessment, the team will follow the **System Failure Procedure**. This procedure is relevant because the incident involves the failure of a wearable device within the Smart Shelter Management System, which constitutes a system failure. If no existing procedure adequately addresses the incident, the team will document their actions and later establish a procedure for handling similar incidents in the future.

9. Forensic Investigation Procedures

Based on the incident involving the failure of a wearable device in the Smart Shelter Management System, team members will utilize forensic techniques to investigate the cause of the incident. This includes:

- Reviewing system logs to identify any anomalies or irregularities leading up to the device failure.
- Checking for gaps in logs that may indicate tampering or manipulation.
- Analyzing intrusion detection logs to determine if there were any unauthorized access attempts or suspicious activities.
- Conducting interviews with witnesses and the incident victim to gather additional information about the event.

It's crucial that only authorized personnel perform these tasks to ensure the integrity of the investigation. The specific authorized personnel responsible for conducting interviews and examining evidence may vary depending on the situation and organizational policies.

10. Recommendations for Mitigating Wearable Device Failure

FOR EDUCATIONAL PURPOSES ONLY

Enhanced Device Monitoring: Implement regular monitoring of wearable devices to detect any signs of malfunctions or failures promptly. This monitoring should include real-time tracking of device status, battery levels, and connectivity.

Regular Maintenance and Testing: Establish a schedule for regular maintenance and testing of wearable devices to ensure their reliability and functionality during emergency situations. This includes software updates, hardware checks, and battery replacements as needed.

Feedback Mechanism: Implement a feedback mechanism to gather insights from users and staff regarding the performance of wearable devices. This feedback can help identify recurring issues and areas for improvement.

Regular Review and Updates: Establish a process for regular review and updates of protocols and procedures related to wearable device usage in emergency shelters. This ensures that the response to device failures remains effective and aligned with evolving needs and technologies.

Redundancy Measures: Introduce redundancy measures for critical functionalities provided by wearable devices. This could involve backup devices or alternative methods for tracking and managing evacuees in case of device failures.

Improved Device Durability: Work with device manufacturers to enhance the durability and resilience of wearable devices, making them better suited for harsh environmental conditions and prolonged usage in emergency shelters.

11. Implementation of Recommended Changes

Upon management approval, the recommended changes to mitigate the "failure of wearable device" vulnerability will be implemented.

12. Restoration and Security Measures

A) Re-installation and Data Restoration: Team members will re-install the affected systems from scratch and restore data from backups if necessary. It's essential to preserve evidence before proceeding with this step to ensure forensic integrity.

B) Password Change: If there's a possibility that passwords may have been compromised, users will be required to change their passwords as a security measure.

C) Hardening the System: The team will ensure that the affected system is hardened by turning off or uninstalling any unused services to minimize potential attack vectors.

D) Patch Management: It's crucial to ensure that the system is fully patched with the latest security updates to mitigate known vulnerabilities and reduce the risk of future incidents.

FOR EDUCATIONAL PURPOSES ONLY

E) Active Security Measures: Team members will verify that real-time virus protection and intrusion detection mechanisms are active and properly configured to promptly detect and respond to any security threats.

F) Logging Configuration: To facilitate incident detection and response in the future, the team will ensure that the system is logging the correct events at the appropriate level, allowing for comprehensive monitoring and analysis of system activities.

13. Documentation and Incident Analysis

A) How the incident was discovered: The incident was discovered through reports from staff members or users who noticed failures or malfunctions in the wearable device.

B) The category of the incident: The category of the incident is determined based on its severity and impact, with a focus on threats to public safety or life.

C) How the incident occurred, whether through email, firewall, etc.: The incident occurred due to a failure or malfunction in the wearable device hardware or software, which was detected through monitoring systems in the SSMS.

D) Where the attack came from, such as IP addresses and other related information about the attacker: The attack originated from within the system itself, as it involved the failure of the wearable device to perform its intended function, rather than an external attack from malicious actors.

E) What the response plan was: The response plan involved assessing the severity of the incident, activating the incident response team if necessary, and implementing measures to address the failure and mitigate its impact on shelter operations.

F) What was done in response? In response to the incident, staff members isolated the affected device to prevent further disruption, implemented manual tracking and management protocols for evacuees as necessary, and initiated repairs or replacements for the failed device.

G) Whether the response was effective: The effectiveness of the response measures was evaluated based on their ability to restore functionality to the affected device, minimize disruption to shelter operations, and ensure the safety and well-being of evacuees.

14. Evidence Preservation

A) Copies of logs, emails, and other communication related to the incident will be made to preserve evidence of the failure of the wearable device.

FOR EDUCATIONAL PURPOSES ONLY

B) Lists of witnesses who reported the incident or were involved in its response will be maintained to document their testimony and involvement in the incident.

C) Evidence will be retained for as long as necessary to complete the investigation, prosecution, and any potential appeals related to the incident, ensuring that all relevant information is available for review and analysis.

15. External Agency Notification and Coordination

In the event of a failure of the wearable device, it may be necessary to involve external agencies, particularly if there are indications of malicious activity or breaches of security protocols. The following agencies should be notified if prosecution of the intruder is deemed possible:

Local Law Enforcement Agency: Contact the local police department or law enforcement agency responsible for the jurisdiction where the incident occurred. Provide them with relevant details about the incident, including the nature of the failure, any potential threats to public safety or data security, and any evidence gathered. Example Contact Information:

Police Department: [Phone Number]
Officer in Charge: [Name]
Email: [Email Address]

Cybersecurity Task Force or Division: Inform specialized cybersecurity units within law enforcement agencies, such as cybercrime task forces or divisions. They can provide expertise in investigating digital crimes and gathering digital evidence.

Example Contact Information:

Cybercrime Division: [Phone Number]

Cybersecurity Investigator: [Name]

Email: [Email Address]

Government Regulatory Agencies: Depending on the nature of the incident and the data involved, notify relevant government regulatory bodies responsible for overseeing data protection and privacy laws. This may include agencies such as the Federal Trade Commission (FTC) or Data Protection Authority (DPA).

Example Contact Information:

FOR EDUCATIONAL PURPOSES ONLY

Federal Trade Commission (FTC): [Phone Number]

Data Protection Authority (DPA): [Phone Number]

Regulatory Compliance Officer: [Name]

Email: [Email Address]

Legal Counsel: Engage legal counsel to advise on the incident response process, potential legal implications, and compliance with relevant laws and regulations. Legal experts can provide guidance on interacting with external agencies and managing legal proceedings.

Example Contact Information:

Law Firm: [Name of Firm]

Attorney: [Name]

Phone: [Phone Number]

Email: [Email Address]

Insurance Provider: If the organization has cybersecurity insurance coverage, notify the insurance provider about the incident. They can offer assistance with managing the incident, assessing liabilities, and initiating insurance claims.

Example Contact Information:

Insurance Company: [Name of Company]

Claims Department: [Phone Number]

Claims Adjuster: [Name]

Email: [Email Address]

Ensure that all communication with external agencies is conducted securely and in compliance with legal requirements regarding data privacy and confidentiality. Provide comprehensive incident reports and cooperate fully with any investigations conducted by external authorities.

16. Damage and Cost Assessment

In the event of a failure of wearable devices within the Smart Shelter Management System (SSMS), it is crucial to promptly assess the damage to the organization and estimate both the

FOR EDUCATIONAL PURPOSES ONLY

financial impact and the cost of containment efforts. Here's how this assessment can be conducted:

Damage Assessment: Begin by evaluating the damage caused by the failure of wearable devices. This assessment should encompass various aspects, including the impact on shelter operations, the safety and well-being of evacuees, and any potential compromises to sensitive data or critical systems.

Financial Impact Estimation: Quantify the financial impact of the incident by considering factors such as lost productivity, expenses incurred due to manual tracking and management protocols, potential revenue losses, and any additional costs associated with incident response and recovery efforts.

Containment Cost Estimation: Estimate the cost of containment efforts aimed at mitigating the effects of the failure and preventing further damage. This may include expenses related to repairs or replacements of the affected devices, deployment of alternative tracking or monitoring methods, and any other measures implemented to ensure the continuity of shelter operations.

Comprehensive Cost Analysis: Compile the assessed damage and containment cost estimates into a comprehensive analysis that provides a clear overview of the financial impact of the incident on the organization. Consider both direct costs, such as equipment repairs, as well as indirect costs, such as reputational damage or regulatory fines.

Risk Mitigation Planning: Use the findings from the damage and cost assessment to inform risk mitigation planning and decision-making processes. Identify areas where investments in preventative measures or technological enhancements could help reduce the likelihood of similar incidents occurring in the future, thereby minimizing potential financial losses.

By conducting a thorough assessment of the damage and cost associated with the failure of wearable devices, the SSMS can gain valuable insights into the impact of the incident and make informed decisions to mitigate risks and enhance resilience against similar incidents in the future.

17. Response Review and Policy Update

A) Evaluate whether an additional policy could have thwarted the intrusion, particularly considering the unique vulnerability of the wearable device failure.

B) Assess if any procedures or policies were not adhered to, which facilitated the intrusion. Implement measures to ensure compliance with procedures or policies in the future.

FOR EDUCATIONAL PURPOSES ONLY

C) Reflect on the appropriateness of the incident response. Identify areas for improvement, such as response time, communication effectiveness, or resource allocation.

D) Confirm if all relevant parties were promptly notified during the incident. Adjust notification protocols if any delays or gaps were identified.

E) Review the incident-response procedures for comprehensiveness and effectiveness. Enhance procedures to address any uncovered gaps or deficiencies.

F) Implement changes to prevent re-infection, including patching all systems, strengthening security measures, updating passwords, and ensuring the latest antivirus software is in place.

G) Implement measures to prevent similar infections in the future, considering the unique nature of the vulnerability associated with the wearable device failure.

H) Assess if any security policies require updates based on lessons learned from the incident. Update policies to better safeguard against future vulnerabilities or intrusions.

I) Identify and document the key lessons learned from the incident, such as areas for improvement in response procedures, policy enforcement, or system security measures. Use these lessons to inform future incident response strategies and policy enhancements.

Identify any industry standards or government regulations that will affect your product at each layer of the stack.

Are there industry standards for data formats or communication protocols that you should use?

What laws must your product comply with?

Develop a privacy impact assessment (PIA) to be used for your product. You must use the provided sample DHS template and customize it to reflect your product. Be sure to include the nature of disclosures to be given to users about the use of their information, their options for opt-out, how the data will be secured, and the impact of a breach. Include this PIA as Appendix B of your report.

FOR EDUCATIONAL PURPOSES ONLY

Device Hardware (Layer 1)

FCC Regulations: In the United States, the Federal Communications Commission regulates the wireless spectrum and radio-frequency devices, which would include the RFID or NFC technology used in wearable devices.

CE Marking: In Europe, devices must comply with CE marking requirements, indicating conformity with health, safety, and environmental protection standards.

RoHS Directive: The Restriction of Hazardous Substances in electrical and electronic equipment is essential for hardware components.

IP Ratings: International Protection Marking standards for ensuring devices are dust and water-resistant, particularly important for devices used in disaster relief scenarios.

Device Software (Layer 2)

Software Standards: Standards such as ISO/IEC 27002 for information security controls would be applicable.

Firmware Compliance: Compliance with standards set for embedded systems, such as MISRA C for the software development in automotive systems, which could be analogous to safety-critical aspects of SSMS.

Communications (Layer 3)

Data Transmission Security: Adherence to standards like TLS for secure data transmission is critical.

Wireless Communication Standards: Compliance with IEEE standards for wireless networking (e.g., IEEE 802.11 for Wi-Fi, IEEE 802.15.4 for ZigBee).

Telecommunications Standards: Conformance to regulations by bodies like ITU for global communication standards.

Cloud Platform (Layer 4)

Data Protection Regulations: GDPR in Europe, CCPA in California, and other regional data protection laws dictate how personal data must be handled and protected.

Cloud Security Standards: Compliance with standards such as ISO/IEC 27017 for cloud security.

Healthcare Information: If health-related data is processed, HIPAA compliance in the US and its international equivalents must be observed.

Cloud Applications (Layer 5)

Application Security: Adherence to the Open Web Application Security Project (OWASP) Top Ten for web application security.

FOR EDUCATIONAL PURPOSES ONLY

User Interface Accessibility: Compliance with the Americans with Disabilities Act (ADA) Standards for Accessible Design and Web Content Accessibility Guidelines (WCAG) for ensuring accessibility.

API Security: Standards like OpenAPI Specification (OAS) for API design and documentation.

Appendix B Privacy Impact Assessment:

FOR EL

Privacy Impact Assessment for
the

Smart Shelter Management System

SSMS

3/30/2024

Contact Point
Mason Starnes
Privacy Officer
Smart Shelter Management System Program
786-871-3910

Reviewing Official
Jonathan R. Cantor Acting Chief Privacy Officer Department of Homeland Security
(202) 343-1717

FOR EDUCATIONAL PURPOSES ONLY

Abstract

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

• First sentence should include the name of the component and the system, technology, pilot, rule, program, or other collection (hereinafter referred to as "project"). Note: There are some instances where system is specifically called out.

• Second sentence should be a brief description of the project and its function.

• Third sentence should explain the reason the program is being created and why the PIA is required. This sentence should embody the same analysis that caused the project to be identified as a "privacy sensitive system" in the PTA, such as the

project requires PII or the technology is privacy sensitive.

The Smart Shelter Management System (SSMS) is an innovative technology designed to efficiently manage emergency shelter operations during disaster events. This comprehensive system integrates wearable devices, real-time tracking, and communication capabilities to ensure the safety and well-being of evacuees. Given the collection of personally identifiable information (PII) and the privacy-sensitive nature of the technology, a Privacy Impact Assessment (PIA) is required to address privacy concerns and safeguard individual rights and data privacy within the SSMS.

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.

FOR EDUCATIONAL PURPOSES ONLY

The Smart Shelter Management System (SSMS) is a project developed and funded by the Department of Homeland Security (DHS), with authorization stemming from disaster management legislation. Its purpose is to efficiently manage emergency shelter operations during disaster events, aligning with DHS's mission to safeguard the nation from various threats, including natural disasters. The SSMS collects personally identifiable information (PII) such as evacuee demographics, medical records, and location data to ensure the safety and well-being of individuals seeking refuge in emergency shelters. This includes the collection of PII during registration, tracking of movements within shelters, and maintenance of communication channels with evacuees. The project takes steps to protect privacy by implementing encryption for data at rest and in transit, enforcing role-based access controls, conducting regular user training on security best practices, and ensuring compliance with relevant data protection regulations.
The SSMS operates under a funding mechanism established through DHS contracts or inter-agency agreements, ensuring proper allocation of resources for its development and maintenance. Routine information sharing within DHS components and with external partners is conducted to enhance coordination and response efforts during disaster events, with protocols in place to ensure compatibility with the original collection of information and adherence to privacy principles.

The major potential privacy risks identified in the PIA analysis include unauthorized access to sensitive evacuee information, failure of wearable devices leading to incorrect tracking, and compromise of API security, among others. Overall, the SSMS has a significant privacy impact on individuals, as it involves the collection and processing of sensitive PII to ensure their safety and well-being during emergencies.

The technology used in the SSMS includes wearable devices, GPS tracking systems, IoT sensors, and communication APIs. These technologies collect information such as location data, health records, and communication preferences to facilitate efficient shelter management and communication with evacuees.

FOR EDUCATIONAL PURPOSES ONLY

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).

Specific legal authorities and agreements permitting and defining the collection of information by the Smart Shelter Management System (SSMS) include:
Stafford Act (42 U.S. Code § 5121 et seq.): The Stafford Act authorizes the Federal Emergency Management Agency (FEMA) to provide assistance for disaster relief and emergency management activities, including the establishment and operation of emergency shelters. The collection of information by the SSMS is permitted under this authority as part of FEMA's mandate to coordinate and support disaster response efforts.
Privacy Act of 1974 (5 U.S. Code § 552a): The Privacy Act governs the collection, maintenance, use, and dissemination of personally identifiable information (PII) by federal agencies. The SSMS complies with the Privacy Act requirements by ensuring that the collection and use of PII are limited to the purposes specified in the system of records notice and that appropriate safeguards are in place to protect the privacy of individuals.
Health Insurance Portability and Accountability Act (HIPAA) (42 U.S. Code § 1320d et seq.): If the SSMS collects health-related information, it must comply with HIPAA regulations, which govern the privacy and security of protected health information (PHI). HIPAA permits the collection of PHI for purposes of providing emergency medical treatment and coordinating healthcare services during disaster events.
International Agreements or Memoranda of Understanding: If the SSMS receives information from foreign governments pursuant to international agreements or memoranda of understanding, the specific agreements or memoranda governing such information sharing must be cited. These agreements would outline the legal basis and conditions for sharing information between the SSMS and foreign entities.

FOR EDUCATIONAL PURPOSES ONLY

The Stafford Act authorizes FEMA to coordinate federal disaster response efforts, including the establishment and operation of emergency shelters. This authority enables FEMA to collect information necessary for managing shelter operations and assisting disaster-affected individuals. The Privacy Act of 1974 governs the collection and use of PII by federal agencies, ensuring that individuals' privacy rights are protected. Compliance with the Privacy Act requires agencies to limit the collection of PII to specified purposes, maintain accurate and relevant records, and implement safeguards to prevent unauthorized access or disclosure. If the SSMS collects health-related information, it must also comply with HIPAA regulations, which establish standards for protecting the privacy and security of PHI. Finally, international agreements or memoranda of understanding may govern the sharing of information between the SSMS and foreign governments, outlining the legal basis and conditions for such exchanges.

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

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

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

FEMA Disaster Personnel Records (DPR) System, DHS/FEMA-008: This SORN covers personnel records maintained by FEMA for individuals involved in disaster response and recovery activities, including staff deployed to operate and manage emergency shelters. The SSMS may retrieve information from this system to coordinate shelter operations and manage personnel assignments during disaster events. The Federal Register citation for this SORN is [XX FR XXXX].

FEMA National Shelter System (NSS) System of Records, DHS/FEMA-016: This SORN covers information collected and maintained by FEMA's National Shelter System, which includes data on the location, capacity, and status of emergency shelters nationwide. The SSMS may retrieve information from this system to populate its database of available shelter facilities and support the real-time tracking and management of evacuees during disaster events. The Federal Register citation for this SORN is [XX FR XXXX].

SSMS-Specific System of Records Notice: If the SSMS collects and maintains PII beyond what is covered by existing SORNs, a new SSMS-specific SORN may be required to adequately inform individuals about the collection, use, and safeguarding of their information. This new

FOR EDUCATIONAL PURPOSES ONLY

SORN would be published in the Federal Register to provide transparency and compliance with Privacy Act requirements.
The FEMA Disaster Personnel Records (DPR) System (DHS/FEMA-008) SORN covers personnel records maintained by FEMA for individuals involved in disaster response and recovery activities, including staff deployed to operate and manage emergency shelters. The SSMS may retrieve information from this system for the purpose of coordinating shelter operations and managing personnel assignments during disaster events. The Federal Register citation for this SORN is [XX FR XXXX].
The FEMA National Shelter System (NSS) System of Records (DHS/FEMA-016) SORN covers information collected and maintained by FEMA's National Shelter System, including data on the location, capacity, and status of emergency shelters nationwide. The SSMS may retrieve information from this system to populate its database of available shelter facilities and support the real-time tracking and management of evacuees during disaster events. The Federal Register citation for this SORN is [XX FR XXXX].
If the SSMS collects and maintains PII beyond what is covered by existing SORNs, a new SSMS-specific SORN may be required to adequately inform individuals about the collection, use, and safeguarding of their information. This new SORN would be published in the Federal Register to provide transparency and compliance with Privacy Act requirements.

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, a system security plan has been completed for the Smart Shelter Management System (SSMS) supporting the project. The Authority to Operate (ATO) was granted on [insert date]. The SSMS complies with DHS Management Directive 4300A. The system containing PII is categorized as "moderate" under Federal Information Processing Standards Publication 199.

The SSMS, being a system that collects and manages sensitive information such as personally identifiable information (PII) related to shelter operations and evacuees, requires a

FOR EDUCATIONAL PURPOSES ONLY

comprehensive system security plan to ensure the confidentiality, integrity, and availability of the data. The completion of the security plan demonstrates the project's commitment to safeguarding sensitive information and complying with relevant security standards and directives.

The granting of the Authority to Operate (ATO) signifies that the SSMS has undergone a thorough assessment of its security controls and has been deemed acceptable for operation within the DHS environment. The ATO date indicates the point at which the system was authorized to begin operations, following the successful implementation of security measures and the approval of relevant stakeholders.

As per DHS Management Directive 4300A, all DHS systems containing PII must adhere to specific security requirements outlined in the directive. The SSMS complies with these requirements to ensure the protection of sensitive information and mitigate security risks.

The system's categorization as "moderate" under Federal Information Processing Standards Publication 199 (FIPS 199) indicates the level of impact associated with a potential breach of security. Moderate categorization signifies that the system contains information that, if compromised, could result in significant harm to individuals or DHS operations.

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.

Yes, a records retention schedule approved by the National Archives and Records Administration (NARA) exists for the project. The project manager, in consultation with counsel and the component records management officer, developed a records retention schedule that considers the minimum amount of time necessary to retain information while meeting the needs of the project. After finalizing the schedule, it was proposed to NARA for official approval. The

FOR EDUCATIONAL PURPOSES ONLY

NARA-approved schedule ensures compliance with federal regulations regarding the retention and disposition of records.

The development of a records retention schedule is essential for ensuring that records are retained for an appropriate period, taking into account legal, regulatory, and operational requirements, while also facilitating efficient records management practices.

The project manager, in collaboration with counsel and the component records management officer, assessed the specific needs of the project and determined the appropriate retention periods for the records involved. This process involved considering factors such as the legal and regulatory requirements applicable to the project, as well as any operational or business needs that may impact the retention of records.

Once the retention schedule was finalized, it was submitted to NARA for official approval. NARA's approval confirms that the proposed retention periods align with federal regulations and standards governing records management. It also provides assurance that the project complies with requirements related to record retention and disposition.

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.

The information collected by the project is not covered by the Paperwork Reduction Act (PRA). Therefore, there is no OMB Control number or agency number associated with the collection.

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 cate. gory, 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,

FOR EDUCATIONAL PURPOSES ONLY

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.:

Categories of Individuals:
Evacuees from disaster areas, Staff members involved in emergency shelter operations, Users of the Smart Shelter Management System (SSMS)

Information Collected and Stored:
Name, Date of birth, Mailing address, Telephone number, social security number, Email address, Medical record number, Health plan beneficiary number, Device identifiers and serial numbers, Biometric identifiers, Photographic facial image.

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 project may create new information such as real-time tracking data of evacuees and communication logs to monitor shelter operations and ensure the safety of individuals.

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.

2.2 What are the sources of the information and how is the information collected for the project?
A project may collect information directly from an individual, receive it via computer readable extract from another system, or create the information itself.
List the individual(s) providing the specific information identified in 2.1.
If information is being collected from sources other than the individual, including other IT systems, systems of records, commercial data aggregators, and/or other Departments, state the source(s) and explain why information from sources other than the individual is required.
In some instances, DHS may collect information using different types of

FOR EDUCATIONAL PURPOSES ONLY

technologies such as radio frequency identification data (RFID) devices, video or photographic cameras, and biometric collection devices.

Direct Collection from Individuals:
Evacuees from disaster areas provide personal information directly to staff members or users of the Smart Shelter Management System (SSMS) during registration or check-in processes.
Computer Readable Extracts from Other Systems:
Background check systems may provide information such as criminal history, education records, or employment history in a computer-readable format for verification purposes.
The SSMS may receive real-time tracking data from wearable devices worn by evacuees, which are collected electronically and transmitted to the system.
Creation of Information by the Project:
The SSMS generates tracking data and communication logs internally to monitor shelter operations and ensure the safety of evacuees.

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.

The project does not use information from commercial sources or publicly available data. All information collected and used by the Smart Shelter Management System (SSMS) is obtained directly from individuals, background check systems, or internal system processes. There is no reliance on data aggregators such as ChoicePoint or LexisNexis, nor is there any utilization of publicly available data obtained from the internet or state/local public records.

2.4 Discuss how accuracy of the data is ensured.

FOR EDUCATIONAL PURPOSES ONLY

Explain how the project checks the accuracy of the information.

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

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

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

The accuracy of data in the Smart Shelter Management System (SSMS) is ensured through several mechanisms:

Verification Process, Data Quality Checks, Integration with External Systems, Contractual Agreements, Continuous Improvement

Overall, the SSMS prioritizes the accuracy of data to ensure that decisions made based on the information stored in the system are reliable and trustworthy, particularly in critical scenarios such as emergency shelter management.

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

FOR EDUCATIONAL PURPOSES ONLY

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: Inherent risks related to the collection of personally identifiable information (PII) include the potential for unauthorized access, misuse, or disclosure of sensitive data. Additionally, there is a risk of data breaches or security incidents compromising the integrity and confidentiality of the information stored within the Smart Shelter Management System (SSMS).

Mitigation: To mitigate these risks, the SSMS implements robust security measures, including encryption protocols, access controls, and user authentication mechanisms. Access to sensitive PII is restricted to authorized personnel with a legitimate need-to-know, and regular audits and monitoring are conducted to detect and respond to any suspicious activities.

Privacy Risk: Another privacy risk is the potential for data inaccuracies or inconsistencies, which could lead to incorrect decision-making or adversely affect individuals relying on the SSMS for emergency shelter management.

Mitigation: The SSMS addresses this risk by implementing data validation processes, quality assurance checks, and regular audits to maintain the accuracy and integrity of the information stored in the system. Policies and procedures are established to encourage staff members to promptly correct any identified errors or discrepancies, ensuring that the data remains reliable and up-to-date.

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.

FOR EDUCATIONAL PURPOSES ONLY

In the Smart Shelter Management System (SSMS), the collected information serves several internal and external purposes essential for effective emergency shelter operations and management. Below are the uses of the information collected or maintained by the SSMS:

1. Evacuee Registration and Tracking: The system collects personal information such as name, age, gender, and contact details to register evacuees upon their arrival at the shelter. This data is crucial for establishing an accurate count of evacuees and tracking their movements within the shelter facility. It helps shelter staff allocate resources efficiently and ensure the safety and well-being of evacuees.
2. Medical Records and Special Needs: The SSMS may collect medical history, allergies, medications, and special needs information for evacuees requiring medical attention or special assistance. This data enables medical personnel to provide appropriate care and support to individuals with specific health conditions or requirements. It ensures timely access to necessary medical treatment and accommodations, contributing to overall shelter management and evacuee safety.
3. Family and Dependency Information: Gathering information about family members, dependents, or caregivers accompanying evacuees is essential for maintaining family units and addressing the needs of vulnerable individuals. This data helps in coordinating reunification efforts, providing childcare services, and offering support to families during their stay at the shelter.
4. Security and Accountability: The SSMS may record entry and exit times, identification documents, and assigned shelter areas to enhance security and accountability within the shelter premises. This information aids in monitoring the movement of individuals, preventing unauthorized access, and ensuring the safety of evacuees and staff members. It also facilitates the identification of individuals in case of emergencies or incidents requiring intervention.
5. Resource Allocation and Management: Data on shelter occupancy, available resources, and facility capacities assist emergency management personnel in allocating resources effectively and managing shelter operations efficiently. This includes managing supplies, food distribution, sleeping arrangements, and facility maintenance based on real-time information collected through the SSMS. It optimizes resource utilization and enhances the overall functionality of the shelter environment.
6. Reporting and Decision-Making: Collected data is used for generating reports, conducting statistical analysis, and evaluating shelter performance. It provides insights into demographic trends, service utilization patterns, and emerging needs, enabling decision-makers to adjust strategies, allocate resources, and address gaps in service delivery. Regular reporting also supports transparency, accountability, and compliance with regulatory requirements.

FOR EDUCATIONAL PURPOSES ONLY

7. Social Security Numbers (SSNs): If Social Security numbers are collected, they may be necessary for verifying evacuee identities, eligibility for certain services, or facilitating financial assistance programs. SSNs are handled with utmost sensitivity and stored securely to prevent unauthorized access or misuse. Access to SSNs is restricted to authorized personnel with a legitimate need-to-know, and their use is governed by strict privacy policies and regulations.

In summary, the information collected and maintained by the SSMS serves multiple purposes, including evacuee registration, medical care coordination, family support, security management, resource allocation, reporting, and decision-making. Each data element contributes to the efficient operation of emergency shelters and the provision of essential services to displaced individuals during crisis situations.

FOR EDUCATIONAL PURPOSES ONLY

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.

In the Smart Shelter Management System (SSMS), technology is utilized to conduct electronic searches, queries, and analyses in an electronic database to discover predictive patterns or anomalies related to emergency shelter operations and evacuee management. The following outlines how DHS plans to use such results:

Data Analysis and Pattern Identification: The SSMS sifts through large amounts of information collected during evacuee registration, medical recordkeeping, security monitoring, and resource management. Through programmed functions and user inquiries, the system identifies areas that may require further investigation or intervention by shelter staff or emergency responders. Complex analytical tasks, including data matching, relational analysis, scoring, and pattern analysis, are performed to uncover insights and trends relevant to shelter operations and evacuee needs.

Results from Data Analysis: The results generated from the data analysis include background determinations, link analysis, scoring, or other analytical outputs. For example, the system may identify correlations between specific demographic factors and medical needs among evacuees, allowing for targeted resource allocation and medical interventions. These results may be generated electronically by the SSMS or manually reviewed by analysts to ensure accuracy and relevance.

Handling of Results:

- Incorporation into Existing Records: If the results of the analysis pertain to specific evacuees, they will be incorporated into their existing records within the SSMS. For instance, if a medical risk assessment identifies individuals with chronic health conditions, this information will be added to their medical records for ongoing monitoring and care.
- Creation of New Records: In some cases, the analysis may lead to the creation of new records within the SSMS. For instance, if a pattern analysis reveals security threats or emerging trends in shelter occupancy, a new incident record may be created to track and address these issues.
- Access and Usage: Government employees responsible for shelter management and emergency response will have access to the newly derived information as part of their

FOR EDUCATIONAL PURPOSES ONLY

duties. Authorized personnel, such as shelter administrators and medical staff, will utilize this information to make informed decisions regarding evacuee care, resource allocation, security measures, and operational planning.

Example: The SSMS may generate a report indicating a potential security threat based on anomalous behavior patterns detected among certain evacuees. This report will be documented within the system, and a designated security analyst will review the findings to determine the appropriate response. Depending on the severity of the threat, additional security measures may be implemented, such as increased monitoring or coordination with law enforcement agencies. The determination made by the security analyst will be recorded in the system for future reference and action.

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.

In the Smart Shelter Management System (SSMS), there are several components and directorates within the Department of Homeland Security (DHS) that have assigned roles and responsibilities for intra-Departmental sharing of information. Specifically, the SSMS facilitates the sharing of critical information related to emergency shelter operations, evacuee management, and security measures among various DHS components involved in disaster response and humanitarian assistance. The following components or directorates within DHS are involved in the sharing of information:

1. Customs and Border Protection (CBP): CBP plays a crucial role in managing border security and facilitating lawful trade and travel. Within the context of the SSMS, CBP shares relevant information regarding evacuee movements, border crossings, and security threats with other DHS components involved in shelter management and emergency

FOR EDUCATIONAL PURPOSES ONLY

response. This information exchange enables CBP to provide real-time updates on the arrival and status of evacuees at designated shelters, ensuring effective coordination and resource allocation.

2. Immigration and Customs Enforcement (ICE): ICE is responsible for enforcing immigration laws and investigating criminal activities related to border security and public safety. In the context of the SSMS, ICE may share information on individuals with immigration status concerns, criminal backgrounds, or specific security risks to support shelter management and ensure the safety of evacuees and shelter staff. This intra-Departmental sharing of information between CBP and ICE helps identify potential security threats and address immigration-related issues within emergency shelter facilities.
3. Federal Emergency Management Agency (FEMA): FEMA serves as the lead federal agency for coordinating disaster response and recovery efforts. Within the SSMS framework, FEMA collaborates with other DHS components and external partners to share critical information on shelter locations, capacity, resource needs, and operational challenges. This collaboration facilitates seamless communication and coordination among federal, state, local, tribal, and territorial entities involved in providing humanitarian assistance to disaster-affected populations.
4. Transportation Security Administration (TSA): TSA is responsible for securing transportation systems and ensuring the safety of travelers. In the context of the SSMS, TSA may share relevant information on transportation disruptions, security incidents, or evacuee movements that impact shelter operations and logistical planning. This information exchange helps DHS components and partner agencies mitigate security risks and address transportation-related challenges during disaster response operations.
5. Office of Health Affairs (OHA): OHA leads DHS efforts to safeguard the health and resilience of the nation against public health threats and emergencies. Within the SSMS, OHA shares expertise and guidance on public health protocols, medical resource management, infectious disease surveillance, and health risk assessments related to evacuee populations in emergency shelters. This collaboration ensures that shelter operations adhere to established health and safety standards and effectively respond to medical emergencies and health-related challenges.

FOR EDUCATIONAL PURPOSES ONLY

3.4 Privacy Impact Analysis: Related to the Uses of Information

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

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

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

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

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

Follow the format below.

Privacy Risk:
Mitigation:

Privacy Risk: Unauthorized access or misuse of sensitive information within the SSMS, leading to potential privacy violations or breaches.

Mitigation:

- **Principle of Transparency:** The SSMS maintains clear and transparent policies, including Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs), which outline the permissible uses of information collected and maintained within the system. These documents provide stakeholders with detailed information about data handling practices, access controls, and privacy safeguards.
- **Principle of Use Limitation:** Access to information within the SSMS is restricted to authorized personnel who require such data to perform their official duties related to emergency shelter management and disaster response. User training programs emphasize the importance of using information solely for authorized purposes and reinforce compliance with privacy policies and legal regulations. Additionally, the SSMS employs technical controls, such as role-based access controls (RBAC) and user authentication mechanisms, to enforce use limitations and prevent unauthorized access to sensitive data. Violations of data use policies are subject to disciplinary actions, including denial of system access and potential legal consequences, to deter inappropriate behavior and safeguard privacy.

FOR EDUCATIONAL PURPOSES ONLY

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.

The Smart Shelter Management System (SSMS) provides notice to individuals through various channels to inform them about the collection of their information. Notice is typically provided through posted privacy policies at shelter facilities, which outline the purposes of data collection, the types of information collected, and how it will be used. Additionally, individuals may receive oral notice from shelter staff upon arrival, explaining the data collection processes and the reasons behind them.

For further details regarding notice provision, it's recommended to consult the privacy office and legal counsel to ensure compliance with relevant regulations and policies.

If notice is not provided in certain situations, such as during emergency response or law enforcement activities where direct notice may compromise the mission's effectiveness, this section of the PIA would provide an explanation of why direct notice is not feasible or appropriate in those circumstances.

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.

FOR EDUCATIONAL PURPOSES ONLY

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.

In the Smart Shelter Management System (SSMS), individuals typically have limited opportunities to consent to specific uses, decline to provide information, or opt out of the project. This is primarily due to the nature of emergency shelter operations, where the primary focus is on providing assistance and support to individuals in need.

While notice is provided to individuals regarding the collection of their information, the circumstances in emergency shelters may not always allow for explicit consent for each specific use of their information. Individuals may not have the option to decline providing certain information if it is necessary for their safety or the efficient operation of the shelter.

The notice provided to individuals upon entry to the shelter may include information about the purposes for which their data will be used, but specific consent for each use may not be feasible given the urgent and often unpredictable nature of emergency situations.

In situations where declining to provide information means the individual chooses not to participate in the project, this aspect should be clearly communicated in the notice provided to individuals. However, in emergency shelter scenarios, individuals are typically not denied services solely based on their decision to withhold certain information.

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?

FOR EDUCATIONAL PURPOSES ONLY

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:

Mitigation:

Privacy Risk: The notice provided may not adequately correspond to the purpose of the project and the stated uses, leading to potential misunderstandings or concerns among individuals regarding the handling of their information.

Mitigation: To mitigate this risk, the SSMS ensures that the notice given for the initial collection is consistent with the stated uses of the information. This includes providing clear and transparent information to individuals upon entry to the shelter regarding the purposes for which their data will be used. Additionally, the SSMS has procedures in place to ensure that information is used only for the purpose articulated in the notice. This helps maintain transparency and aligns with the Principle of Use Limitation.

Furthermore, the SSMS acknowledges the Principle of Individual Participation by providing notice to individuals on how the program provides for redress, including access and correction of their information. This includes informing individuals about their rights regarding the types of information collected and the controls over security, retention, disposal, etc. This comprehensive approach to notice and individual participation helps address potential privacy risks associated with insufficient notice and opportunity to decline or consent.

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.

FOR EDUCATIONAL PURPOSES ONLY

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.

The Smart Shelter Management System (SSMS) retains information for specific purposes aligned with its operational requirements and legal obligations. The information retained includes:

- Personal Identifiable Information (PII) such as names, contact details, and medical information of individuals staying at the shelter.
- Incident reports detailing any security breaches, system failures, or other incidents affecting the shelter operations.
- Log data capturing system activities, user interactions, and incident responses for auditing and forensic purposes.
- Security camera footage for monitoring and investigation of security-related incidents within the shelter premises.

The retention period for this information is determined based on the operational needs of the SSMS and legal requirements, such as data retention laws and regulations. Generally, the information is retained for a period that allows for the resolution of incidents, compliance with legal obligations, and support of operational continuity.

For example, PII related to shelter occupants may be retained for the duration of their stay at the shelter plus a specified period afterward to address any follow-up inquiries or legal requirements. Incident reports and log data may be retained for a set period, typically dictated by organizational policies or regulatory requirements, to facilitate incident investigation, audit trails, and compliance purposes.

Archiving and destruction schedules are established in alignment with National Archives and Records Administration (NARA) records schedules or internal organizational policies. Active files are retained for the duration necessary to fulfill operational and legal requirements, while

FOR EDUCATIONAL PURPOSES ONLY

archived records may be stored for longer periods as required by applicable regulations or organizational policies.

It's essential for project managers to collaborate with component records officers to ensure that appropriate retention and destruction schedules are implemented, considering the specific needs and regulatory landscape relevant to the SSMS.

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:

Mitigation:

Privacy Risk: The longer data is retained, the higher the risk of unauthorized access, misuse, or exposure of sensitive information. Prolonged retention increases the likelihood of data breaches or unauthorized disclosures, potentially leading to privacy violations, identity theft, or other adverse consequences for individuals.

Mitigation: To mitigate the risks associated with the length of time data is retained, the SSMS implements several measures:

1. Principle of Minimization: The project retains only the minimum amount of information necessary to fulfill its operational requirements and legal obligations. Unnecessary or

FOR EDUCATIONAL PURPOSES ONLY

outdated data is regularly identified and purged from the system to reduce the risk of unauthorized access or misuse.

2. Regular Data Purging: The SSMS has established policies and procedures for the regular review and purging of PII that is no longer relevant or necessary for the specified purposes. This ensures that only accurate, up-to-date information is retained, reducing the risk of retaining outdated or inaccurate data.
3. Secure Data Storage: Data retained by the SSMS is stored securely in accordance with industry best practices and organizational policies. Robust access controls, encryption measures, and monitoring mechanisms are implemented to prevent unauthorized access or breaches.
4. Periodic Risk Assessments: The project conducts periodic risk assessments to identify and mitigate potential privacy risks associated with data retention. This includes evaluating the effectiveness of existing controls, identifying emerging threats, and implementing additional safeguards as necessary to protect sensitive information.

By adhering to these principles and implementing appropriate safeguards, the SSMS minimizes the privacy risks associated with the retention of data, ensuring that personal information is handled responsibly and in accordance with applicable regulations and policies.

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 EDUCATIONAL PURPOSES ONLY

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

Sharing information outside of DHS would be part of standard operations to comply with varying regulations. FEMA would require Evacuee Check In/Out, Shelter Capacity, and Historical Evacuee Movement Data to be reviewed to make sure we are following the NIMS framework. Location and Biographic data would need to be shared with Border Protection in the case where individuals are displaced across borders during a disaster. HHS would require Shelter Capacity and Historical Evacuee Movement Data to secure supplies and resources in a disaster.

Local Law Enforcement and State Emergency Management Agencies would require Shelter Capacity Data to coordinate where people can go in a disaster. Agreements with bordering countries are required in a disaster to facilitate cross-border evacuations. This would also include Foreign Assistance if domestic resources were not enough.

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.

The external sharing described in section 6.1 is compatible with SCORN as noted previously because it follows the proper routine. Under specific circumstances which DHS may disclose/share PII outside the agency for authorized purposes. This would include Audits, Law enforcement, Legal proceedings, Health/safety Emergencies, and more depending on the circumstances. Routine use I would cover most instances of shared PII with international, federal, state, or local government agencies/organizations for authorized activities.

FOR EDUCATIONAL PURPOSES ONLY

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.

Many limitations would be placed on external agencies from further sharing information using Confidentiality Agreements, Data Use Restrictions, and Verification procedures. Through the use of differing Verification procedures with DHS can data then be shared by external agencies.

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.

The SSMS project would maintain a record of any disclosures of information with external agencies to ensure compliance with the Privacy Act. This would include Date of Disclosure, Nature of Disclosure, Purpose of Disclosure, and Recipient Information. Recipient information includes the name and address of the individual/agency.

FOR EDUCATIONAL PURPOSES ONLY

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: Primary Risk: Unauthorized access, use, or disclosure of sensitive personal data. This can lead to privacy violations, identity theft, and other harmful consequences for varying individuals.

Mitigation:

Access Controls: Controls are implemented to restrict access to shared information only to authorized personnel who have reason to access said information. This will be done using role-based access making sure individuals only have access to what they need to perform their duties.

Encryption: Data shared outside of the SSMS Project will have information encrypted during transit and storage to prevent outside access.

Audit Logs: Detailed Audit Logs will be kept and maintained to ensure data is not accessed without proper permission. This would include data, time, purpose/nature of access, and recipient information.

Formal/Legal agreements: Contracts such as MOU will be established with external agencies outlining terms and conditions of information sharing.

Data Minimization: Only relevant information is shared, and Personal Data is anonymized whenever possible to reduce the risk of privacy breaches.

FOR EDUCATIONAL PURPOSES ONLY

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.

Individuals can access their information using either the Freedom of Information or Privacy Act. In the case of FOIA the individual can submit a request to the department of Homeland Security to access personal information (relevant to them) collected by these government systems. With the Privacy Act individuals can access and amend their personal information maintained in the system by making a request to the DHS Privacy Office, specifying the record they wish to access or correct.

At all times individuals have access to their own basic personal information that can be updated and viewed online using an app. If the Individual has further questions/concerns they can reach out to the customer satisfaction department to inquire about accessing their information or any privacy related issues. Contact information includes Phone Number: 305-124-3513 and Email: customerprivacy@ssms.com.

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.

The procedures for individuals to address their information is stated above using the Privacy act or reaching out to the customer satisfaction department.

FOR EDUCATIONAL PURPOSES ONLY

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.

Individuals will be notified at many different points using Privacy Notices prior to data collection/registration, a User Interface within the portal, and Customer support channels. With the of a portal individuals can be reminded of privacy concerns at varying points in time and be allowed to access these channels whenever needed.

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.

FOR EDUCATIONAL PURPOSES ONLY

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: Individuals may have a difficult time accessing/correcting their information beyond what is allowed under the Privacy Act or FOIA.

Mitigation: With the use of an Online Portal/App individuals can access and update their personal information allowing for timely corrections without external assistance. When data access is denied for legitimate reasons, the SSMS will give a clear and detailed explanation of why and where to go if they can challenge this decision. When signing up and from within the app individuals can choose how they want their data shared and what data can be shared.

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

FOR EDUCATIONAL PURPOSES ONLY

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.

As mentioned above in section 6.1, there would be multiple mitigations to ensure the information is used according to stated practices. This also includes two other safeguards Audit Trails, and Automated Monitoring allowing the SSMS to maintain a detailed log of all user activities and interactions with the system. If potential misuse or unauthorized access is detected the Automated Monitoring will flag the unusual/suspicious activity including unauthorized attempts to access information. Unique roles will be given to individuals and external organizations allowing for read only access to specific information such as historical evacuee movement data while someone within the customer service unit will be allowed read and write of some personal data in the event an individual is having difficulties updating it themselves.

The SSMS project would conduct self-audits regularly to ensure data integrity and detect any misuse of any personal information. As well as using third party audits by specific government agencies to stay aligned with federal law and the Privacy Act.

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.

FOR EDUCATIONAL PURPOSES ONLY

The SSMS project implements privacy and security training to ensure that all users, especially those with access to PII are extensively trained to handle this sensitive data properly. This includes General Privacy/Security Training on how to handle data protection, confidentiality, data handling, and compliance with laws and regulations. Project-Specific Training will be given in addition to the General training to users who have access to PII to further explain the unique way to handle information and procedures within the system. Training verification will be in place to make sure all users have completed the relevant training by tracking the completion of training modules, conducting periodic refresher courses, and verifying users' understanding through periodic tests/quizzes.

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.

The SSMS project would implement procedures to determine what users need certain information and the permissions that follow with it. An Authorization Process would be put in place where individuals seeking information will submit a request which will include what information is needed, why is it needed, and who is trying to access said information. This form would then be reviewed, and access would be granted for the bare minimum of what is needed. To further develop this Role-Base Access would be implemented with roles such as administrator, data analysts, emergency personnel, support staff, and other roles given to specific external agencies such as FEMA would be given a role that can then be further limited to people within their organization. Remote access would be in place but heavily encrypted while using a VPN connection

FOR EDUCATIONAL PURPOSES ONLY

which will require user authentication and authorization. Any external device will use strict security protocols such as end-to-end encryption and 2FA.

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.

All proposed information sharing will be reviewed by the Project Manager, including the purpose, scope, and legal implications of the proposed sharing arrangement/agreement. After initial review the proposed agreements/access requests will go through further review by a designated authority based on the significance of the proposed information agreement/request. This will consider the legal requirements, privacy impact, risk, and organizational objectives/polices. Once internally approved these agreements, MOUs, or requests are then forwarded to DHS to be reviewed and approved. This whole process will be documented to maintain a detailed report of the Date of Disclosure, Nature of Disclosure, Purpose of Disclosure, and Recipient Information as well as any modifications made along the way. This helps to ensure transparency, accountability, and compliance with legal requirements and makes future audits easier to complete.

FOR EDUCATIONAL PURPOSES ONLY

Responsible Officials

Jonathan R. Cantor

Department of Homeland Security

Approval Signature

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

FOR EDUCATIONAL PURPOSES ONLY