Terrorism and Targeted Violence

Incident Annex

RECORD OF CHANGES

Change Number	Date of Change	Page or Section Changed	Summary of Change	Authorization Signature	Date of Signature
1					
2					
3					
4					
5					
6					
7					

AUTHORITY AND ADOPTION LETTER

EXECUTIVE SIGNATORY PAGE

The most fundamental function of government is providing for the safety and welfare of the public. An effective Terrorism and Targeted Violence program is essential to ensuring the state of Hawaiʻi fulfills this responsibility when our residents and visitors are threatened or impacted by such incidents.

The State of Hawaiʻi *Terrorism and Targeted Violence Annex* establishes the framework our State Government will use to organize and coordinate its response activities for a coordinated approach to protect against, prepare for, respond to, and recover from terrorism and targeted violence-related incidents.

This annex outlines organizations, actions, and responsibilities of state and county departments and agencies and identifies how they will work together to ensure the state is prepared to execute a well-coordinated, timely and consistent response. It is intended to be a living document that evolves and improves as the outcomes of ongoing planning efforts, exercises and real-world events are incorporated.

This plan is written in accordance with Hawaiʻi Revised Statutes (HRS) Chapter 128A, Homeland Security, and applies to all state departments including agencies, offices, institutions of higher education, commissions, boards, and councils. This plan does not direct the emergency operations of local governments, federal agencies, private sector, or non-governmental organizations. However, it does provide a reference for their response plans, procedures, and actions.

It is important to emphasize that responsibility for the initial response and management of an emergency rests with the affected entity(ies), to include local jurisdictions. The state's response supports state government efforts when additional resources are required or not available within the affected entity. This plan describes how those state resources will be activated, requested, and coordinated to complement response efforts.

This document is maintained by the Hawaiʻi State Office of Homeland Security (OHS) with input from state departments and agencies.

I hereby promulgate and adopt the State of Hawaiʻi *Terrorism and Targeted Violence Annex* to the *State of Hawaii Emergency Operations Plan*.

Frank Pace

Frank J. Pace, Administrator
Office of Homeland Security
Hawaii Department of Defense
August 2, 2021

RECORD OF APPROVAL

Approval #	Approval Date	Approval Authority	Type of Approval
2			
1			

This page intentionally left blank.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE

1. The purpose of this Terrorism and Targeted Violence Annex to the State of Hawaii Emergency Operations Plan (HI-EOP) is to communicate the special roles, responsibilities, and actions that are needed to address a terrorist or targeted violence incident in the State of Hawaii.

2. Because human-caused incidents such as terrorism and targeted violence have an element of preventability that natural hazards lack, this Annex has a unique focus on prevention activities that do not apply to natural hazards.

3. This Annex serves as the mechanism to provide state support to local or federal jurisdictions with law enforcement, public safety, and security operations in response to terrorism or targeted violence incidents in conjunction with or as the cause of activation of the HI-EOP.

4. This Annex applies to all threats and/or acts of terrorism or targeted violence occurring within the State of Hawaii.

5. This Annex contains information that may be sensitive but does not contain any classified material. Consideration should be given to the manner and breadth of distribution of this document.

1.2 SCOPE

1. This Annex applies to all state agencies with responsibilities listed herein.

2. This Annex addresses both terrorism and targeted violence, which correlates with the federal government's increasing recognition that the two topics are intertwined and interrelated.[1]

3. This Annex recognizes that incidents characterized as terrorism or targeted violence may consist of many types of threats. The scope of this Annex is limited to acts of mass violence that do not necessitate hyper-

---

[1] Department of Homeland Security (DHS), *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

specialized aspects of response. Categories of acts of terrorism or targeted violence that are addressed in this Annex include:

    a.   Mass shootings.

    b.   Arson or fire as a weapon.

    c.   Bombings/explosions.

    d.   Kidnapping or hostage-taking.

    e.   Vehicular attacks.

    f.   Other violent attacks meeting the definition of targeted violence, such as stabbings or active-shooter attacks.

4.   Though many aspects of this Annex apply to all types of terrorism and targeted violence (e.g., public alert and warning), this Annex acknowledges that the following types of terrorism have hyper-specialized aspects of response as to warrant separate planning processes and documentation. Types of terrorism that are *not addressed in this Annex* include:

    a.   Cyberterrorism.

    b.   Chemical incidents, including the use of chemical warfare agents such as nerve, blister, choking, and blood agents.

    c.   Biological incidents.

    d.   Radiological incidents.

    e.   Nuclear incidents.

    f.   Explosive incidents that would be covered in a HI-EOP Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Incident Annex.

Addressed in this Annex:	
Shootings	✔
Arson or fire as a weapon	✔
Bombings/explosions	✔
Kidnapping or hostage-taking	✔
Vehicular attacks	✔
Other violent attacks meeting the definition of targeted violence, such as stabbings	✔

Not Addressed in this Annex:						
Cyberterrorism	Chemical incidents	Biological incidents	Nuclear incidents	Explosive incidents covered by the HI-EOP	Fatality management/ mass fatality incidents	Mass casualty incidents (MCI)
✖	✖	✖	✖	✖	✖	✖

5.   Broader response topics not addressed in this Annex, unless there are special considerations that need to be developed for terrorism and targeted violence, include fatality management for mass fatality incidents.

1.2.1 RELATIONSHIP TO OTHER PLANS

1. This plan is an Annex to the HI-EOP, which is the state's all-hazards plan that establishes the framework used to coordinate the state response to, and initial recovery from, emergencies and disasters. This Annex addresses unique planning and response requirements for terrorism and targeted violence incidents but is not intended to duplicate or alter the response concepts outlined in the HI-EOP*.*

2. This Annex is not intended to duplicate or alter other Annexes to the HI-EOP or any of the State Emergency Support Function (SESF) Annexes that have bearing on acts of terrorism or targeted violence (e.g., SESF #9: Search and Rescue, SESF #10: Oil and Hazardous Materials).

STATE OF HAWAII
EMERGENCY OPERATIONS PLAN
BASIC PLAN

HAWAI'I EMERGENCY MANAGEMENT AGENCY
November 2019
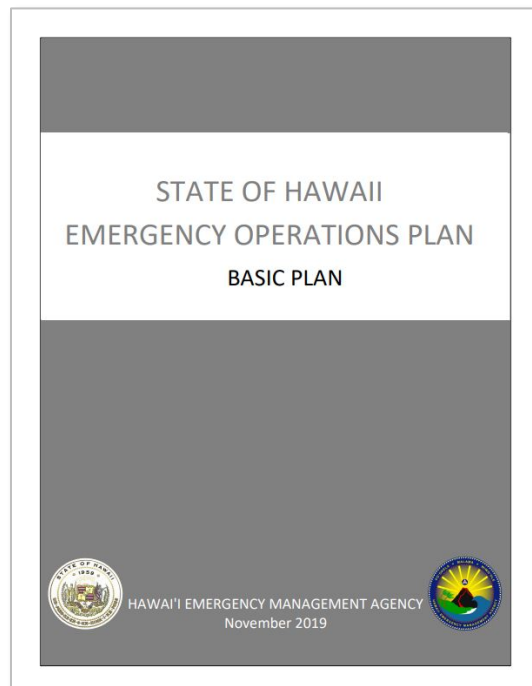
This page intentionally left blank.

2. SITUATION AND ASSUMPTIONS

2.1 SITUATION OVERVIEW

1. Terrorism is considered by the U.S. Department of Defense (DOD), Department of State, Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI) to be an "emerging threat." While not a *new* threat, terrorist activities have the potential to become increasingly advanced or have the potential to be influenced by the increasing use of online communication to reach recruits and disseminate propaganda.[2]

2. Shifts in domestic terrorism activity can occur quickly and frequently, depending on changes in political or social circumstances, requiring law enforcement to remain alert to all forms of potential domestic terrorism. Because domestic terrorism requires a political or social motivation, the potential for changes in these areas to produce quick swings in activity remains high. Events such as elections, new legislation, and social justice-related incidents all have the potential to spark activity in previously dormant movements or see the emergence of new domestic terrorism actors.[3]

3. Rather than attempting to define domestic terrorism as an extreme application of a mainstream political belief, it is easier to distinguish domestic terrorists from mainstream individuals. Generally, domestic terrorists believe force or violence is an acceptable means to accomplish their goals. This may include those who justify force against property or infrastructure as a valid means to an end, those who justify the use of violence against people, or individuals who believe both are justified. While no actual percentage exists for domestic terrorists, an implicit assumption in the extreme nature of their beliefs is that they make up a small portion of the population.[4]

4. Gun violence in the U.S. continues to be a problem. In 2019, there were 28 active shooter incidents in the United States, including one in Hawaii. These incidents resulted in 247 total casualties, including 97 fatalities and over 150 injuries. These statistics do not include all gun-related incidents.[5]

---

[2] GAO, *Long Range Emerging Threats Facing the United States as Identified by Federal Agencies*, December 2018. https://www.gao.gov/assets/700/695981.pdf

[3] Texas Department of Public Safety (TDPS)*, Texas Domestic Terrorism Threat Assessment*, January 2020. https://www.dps.texas.gov/director_staff/media_and_communications/2020/txTerrorThreatAssessment.pdf This resource was used for information that pertains not just to Texas.
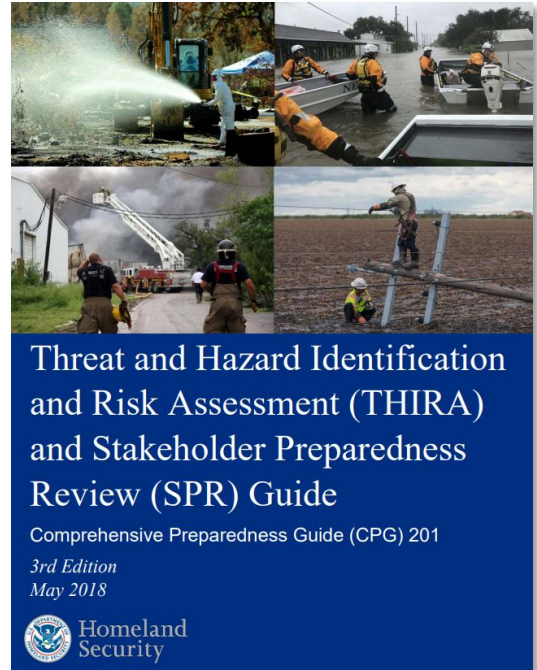
[4] Ibid.

[5] FBI, *Active Shooter Incidents in the United States in 2019*, April 2020. https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2019-042820.pdf/view

2.2 THREAT ANALYSIS

This section provides an overview of threats to the state of Hawaii, including assessments and documentation, specific terrorism and targeted violence threats, and vulnerability analysis. This section primarily focuses on threats and vulnerabilities in Hawaii, but includes some CCTA, terrorism, active shooter, and targeted violence case studies from both across the U.S. and worldwide. This information is intended to provide a broad understanding and should be considered in conjunction with other statewide documents such as the HI-EOP and the THIRA.

2.2.1 ASSESSMENT AND DOCUMENTATION

1. The Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) help the State of Hawaii understand present and potential threats, risks, and hazards as well as determine the level of capability needed to address them. The outputs from the THIRA lay the foundation for determining a community's capability gaps during the SPR process.

Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide
Comprehensive Preparedness Guide (CPG) 201
3rd Edition
May 2018
Homeland Security

   a. The FEMA (Federal Emergency Management Agency) Comprehensive Preparedness Guide (CPG) 201, 3rd Edition, provides guidance for conducting a THIRA and SPR.[6] The THIRA includes standardized language to describe threat and hazard impacts and capability targets. This allows communities to collect more specific, quantitative information while also providing important context. Through the updated SPR process, communities collect more detailed and actionable data on their current capabilities and identified capability gaps. Communities then indicate their intended approaches for addressing those gaps and assess the impact of relevant funding sources on building and sustaining capabilities.

   b. The THIRA is a statewide three-step risk assessment completed every three years. The THIRA assessment steps include:

      1) **Identifying threats and hazards of concern:** Based on a combination of experience, forecasting, subject matter expertise, and other available resources, a list of threats and hazards is developed that could affect the community.

      2) **Giving threats and hazards context:** The threats and hazards identified in Step 1 are described and analyzed to show how they may affect the community and create challenges in performing the core capabilities.

---

[6] FEMA, *THIRSA and SPR Guide, 3rd Edition,* 2018. https://www.fema.gov/sites/default/files/2020-07/threat-hazard-identification-risk-assessment-stakeholder-preparedness-review-guide.pdf

3) **Establishing capability targets:** Using the impacts described in Step 2, the level of capability that the community plans to achieve overtime to manage the threats and hazards it faces is determined.

c. The SPR is a three-step self-assessment of a community's capability levels based on the capability targets identified in the THIRA:

1) **Assess capabilities:** Based on the language from the capability targets set in THIRA Step 3, the community's current capability is identified, the additional information includes how that capability has changed over the last year, including capabilities lost, sustained, and built. Additional context is provided to explain the reported data and its sources.

2) **Identify capability gaps and intended approaches to address them:** The causes of the capability gap are determined between the capability target and the current capability identified in SPR Step 1. Actions and investments needed to close the capability gap or sustain the capability are also outlined.

3) **Describe the impacts of funding sources**: Relevant funding sources, including but not limited to grant programs and the community's own resources that helped to build or sustain the capabilities assessed by the capability targets, are outlined. How those capabilities were used in a real-world incident(s) over the past year is also included.

2. As a part of the Hazard Mitigation Program, the state and each of the counties maintain an up-to-date Mitigation Plan. In compliance with FEMA regulations, each Mitigation Plan has its own Risk Assessment section and is re-assessed as a part of the Hazard Mitigation Plan updates.

3. In addition to this Annex, The State of Hawaii Office of Homeland Security (OHS) coordinates several efforts aimed at characterizing and communicating threats to Hawaii. These initiatives are intended to be complementary to one another.

a. **Threat Team Hawaii**: An ongoing initiative to improve the Level 1 Threat Assessment Team's capability to identify and assess threats, including violent extremism reported by the community, and incorporate the work of trained Level 1 teams to identify and assess threats as part of OHS's all-threats program. Applicable activities of Threat Team Hawaii include:

1) Providing violent extremism training, workshops, exercises, and assistance in developing County-specific Threat Teams.

2) Developing an all-threats reporting and analysis system.

b. **School assessments**: The STOP School Violence Threat Assessment and Technology Reporting Program helps reduce security risks and safety threats in schools by supporting the development of threat assessment teams and implementing electronic reporting tools to help mitigate school violence threats and risks.

c. **Local Prevention Framework Track:** The Local Prevention Framework Track helps and supports partners at the local level to better understand the evolving terrorism and targeted violence threat

environment by identifying potential actions, partners, training, and resources. Currently, the Local Prevention Framework Track is available in the Counties of Kauai, Maui, and Honolulu.

2.2.2 TERRORISM

1. This section provides case studies that illustrate the threat of terrorism by highlighting events both within Hawaii and nationwide. Although terrorism events are not common in Hawaii, it is critical not to confound a lack of historical examples as a lack of risk. As threats increase nationally and worldwide, Hawaii can expect to see an increase in threats in the state.

   a. **U.S. Capitol Hill Riots:** In January 2021, the U.S. Capitol Building in Washington, D.C., was breached by thousands of armed from far-right extremist organizations demanding entrance into the House of Representatives and Senate Congressional chambers. The protestors had marched down the National Mall after attending a rally held by President Donald J. Trump, in which he encouraged the group to attend and possibly overthrow the certification of the 2020 presidential election results. After overwhelming police and security forces, the thousands of supporters entered the Capitol Building, looting and vandalizing the building and Congressional offices, while others came to an armed standoff with Capitol Police forces. After deploying the D.C., Maryland, and Virginia National Guard, the building was cleared, and several rioters were arrested. By the end of the day, five individuals, including a Capitol Police officer, were killed as a result of injuries sustained during the incident. As of January 2021, the FBI is actively investigating the incident, with many lawmakers demanding the insurrection be labeled as domestic terrorism.

   b. **Hawaii-Based Islamic Sympathizer:** In summer 2018, a U.S. Army soldier, stationed at Schofield Barracks in Wahiawa and residing in Waipahu, met numerous times with undercover Federal Bureau of Investigation (FBI) agents whom he believed had connections to the Islamic State of Iraq and Levant (ISIL). He provided them with sensitive, non-public, military documents which he intended later be provided to ISIL. He also provided the agents with a commercially purchased small aerial drone, a military chest rig, and other military-style clothing and gear. The soldier then met two additional undercover FBI personnel, one who purported to be a high-ranking ISIL leader, or "sheikh," and another who played the role of an ISIL fighter. Kang led them in a two-hour, step-by-step military combative training session in order to train the purported ISIL member in hand-to-hand fighting techniques and marksmanship. The soldier was given numerous opportunities by the undercover agents to return the classified military documents and to stop and leave the training, which he did not do. Instead, he swore an oath of loyalty to ISIL and its leader in a ceremony conducted by the purported ISIL sheikh. After the ceremony, Kang said that he wanted to get his rifle and go to

downtown Honolulu and Waikiki strip and start shooting. Kang was subsequently arrested and taken into custody. In December 2018, the soldier was sentenced to 25 years in prison for attempting to provide material support to ISIL.

c. **New York-Based Islamic Sympathizer and Recruiter:** Between 2013 and 2014, a man from Rochester, New York actively recruited and attempted to send two individuals – both of whom were cooperating with the FBI at the time – to Syria to join and fight on behalf of ISIL. The perpetrator sent anti-American ISIL propaganda videos to one of the individuals and arranged for an English-speaking ISIL contact in Iraq to communicate with the individual over social media. He also provided guidance about traveling internationally while avoiding detection, supported the coordination of travel logistics, and coordinated the admission of both individuals into ISIL-controlled territory in Syria. In March 2016, the perpetrator was sentenced to over 22 years in prison for attempting to provide material support to ISIL.

2.2.3 COMPLEX COORDINATED TERRORIST ATTACK

1. Much like terrorism events in the state, Hawaii has largely been spared acts of complex, coordinated multi-incident acts of mass violence. It remains critical not to look at a lack of examples as a lack of risk. As threats increase nationally and worldwide, Hawaii can expect to see an increase in threats in the state. While not classified as terrorist incidents, several Hawaii-based incidents in the recent past have exhibited characteristics of a CCTA.

   a. **Diamond Head ("Hibiscus Drive") Stabbing, Shooting, and Fire:** On January 19, 2020, a 69-year-old suspect stabbed his landlord in a Diamond Head neighborhood and began opening fire on three responding police officers, killing two from the Honolulu Police Department (HPD). During the incident, the suspect started a fire that destroyed five homes and damaged several others. Ammunition stored inside the home was ignited by the fire, causing a significant blast and initially rendering the area unsafe for first responders. The suspect, who died in the fire, had a history of paranoia and believed the FBI and Secret Service were tracking him.

   b. **Kehalani Foodland Stabbing:** On July 24, 2016, an individual entered the Foodland grocery store to stalk his estranged wife and started an argument with the man she was shopping with. After a brief struggle with the man, the assailant sliced his estranged wife's throat and stabbed two additional people who tried to intervene. The assailant then attempted to attack another individual before fleeing the scene and being arrested shortly thereafter.

2. The following case studies from around the world provide context and help illustrate the nature of incidents that are classified as CCTAs:

   a. **Sri Lanka Easter Bombings:** On Easter Sunday on April 21, 2019, three churches and three hotels in Sri Lanka were targeted in a series of coordinated Islamic terrorist suicide bombings. The churches, packed with Christians attending Easter Sunday services, were targeted first, followed by attacks at the three hotels. Later that day, an Inn and housing complex were also attacked. In total, 259 people were killed and at least 500 people were injured. In total, nine bombers were identified and up to 70

suspects were held on charges. The attack was associated with a Sri Lanka-based jihadist group with ties to ISIL. The attacks were purported to be retaliation for the New Zealand attacks that occurred in two mosques in New Zealand a month earlier.

b. **Brussels Bombings:** On March 22, 2016, three coordinated suicide bombings occurred across Belgium. Two suicide bombings occurred at the Brussels Airport, followed by a separate bombing at the Maalbeek Metro Station in central Brussels. A total of 35 people, including the three suicide bombers, were killed, and over 300 were reported injured. In addition to the three suicide bombers, two other individuals were arrested weeks after the incident. All the attackers were involved in the planning and organizing of the Paris attacks, described below, and ISIL claimed responsibility.

c. **Paris Attacks:** On November 13, 2015, a series of coordinated terrorist attacks took place in Paris. Three suicide bombers struck outside the Stade de France during a soccer match, followed by several mass shootings and suicide bombings at different restaurants and cafes throughout the city. Shortly thereafter, perpetrators executed another mass shooting leading to a hostage situation standoff with police. In total, the attacks killed 130 people and caused over 400 injuries. The attacks were planned in Syria and organized by a terrorist cell, with ISIL taking responsibility, listing the motive as retaliation for French airstrikes.

d. **Mumbai Attacks:** Between November 26 and November 29, 2008, a series of terrorist attacks took place in various locations in Mumbai, India, where 10 members of an extremist Islamist terrorist organization based in Pakistan carried out 12 coordinated shooting and bombing attacks at various locations across the city. At least 174 people died, including 9 attackers, and more than 300 were wounded.

e. **London Bombings:** On July 7, 2005, a series of coordinated terrorist/suicide attacks occurred across London's public transportation system. Three Islamic terrorists detonated three homemade bombs in quick succession on three different London Underground trains, with a fourth bomb denoted shortly after on a double-decker bus. In addition to the bomber, 55 were killed, and more than 700 were injured. The bombers were Islamic extremists who claimed they were soldiers and had been motivated by al-Qaeda.

f. **Madrid Train Bombings:** On March 11, 2004, 10 coordinated bombings of improvised explosive devices (IEDs) occurred against four commuter trains within the early morning in Madrid, three days
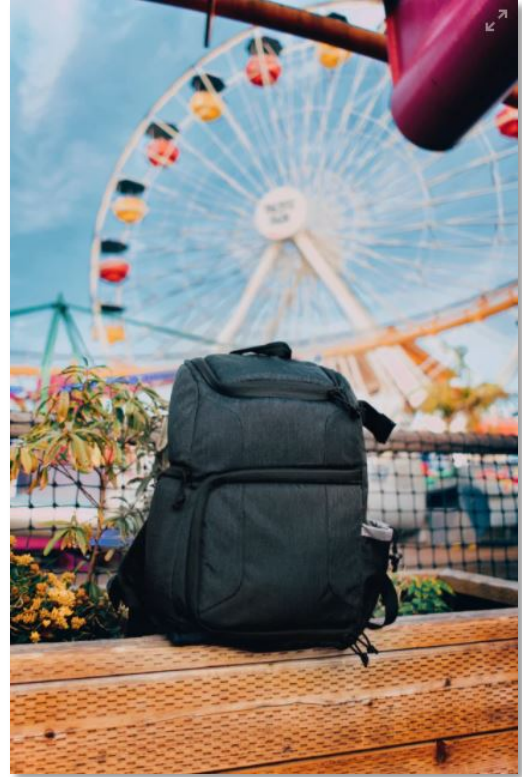
before Spain's general elections. The explosions killed 191 people and injured over 1,800. Initially, the attacks were blamed on a separatist organization. However, the attacks were later concluded to be conducted by an al-Qaeda terrorist cell.

2.2.4 ACTIVE ASSAILANT/SHOOTER/OTHER MASS VIOLENCE

1. This section provides case studies that illustrate the threat of active assailant, active shooter, and other acts of non-terrorism mass violence within Hawaii. The case studies are not meant to be a comprehensive list of incidents; rather, they are intended to show that threats and incidents are not uncommon in the state. This list also includes credible and non-credible threats received and investigated by intelligence agencies throughout the state.

   a. **Maui Police Department Threat:** On July 21, 2020, a man contacted the Maui Police Department multiple times, threatening to bomb the Kihei Police Station. The suspect later trespassed at the Kihei Police Station and attempted to strike a police officer with his vehicle before fleeing the scene. The individual was apprehended and arrested shortly thereafter.

   b. **Hauula Barricaded Gunman:** On April 14, 2020, police responded to a gunman barricaded in a home in Hauula. The gunman exchanged fire with officers and was later arrested.

   c. **Waiakea High School:** On March 4, 2020, police investigated a message threatening a school shooting that was written on a bathroom wall at Waiakea High School. The threat indicated a school shooting would occur on March 5, 2020, but it was a general message that did not name anyone in particular. The threat was investigated, but school operations were uninterrupted.

   d. **Mililani High School Stabbing:** On the morning of February 24, 2020, two 16-year-old students were stabbed at Mililani High School, ultimately surviving their injuries. The school was placed in lockdown after police responded to the report of a stabbing around 10:15 am. Shortly after the incident, students were released from school early and parents were directed to the school's gymnasium and Meheula Parkway for police-facilitated pickups. The perpetrator was taken into custody and school resumed the following day.

   e. **Mililani High School Threat:** On Friday, February 28, 2020, Mililani High School remained open after a threat circulating over social media was deemed not credible. The threat came in the form of images of text messages. The perpetrators were not publicly identified due to being minors.

   f. **Pearl Harbor Shooting:** On December 4, 2019, a 22-year-old U.S. Navy sailor fatally shot two individuals at the Pearl Harbor Naval Shipyard, wounding a third, using his service weapons (an M4 rifle and M9 pistol). The military base was subsequently placed on lockdown. While a motive was not clear, the suspected reportedly has disciplinary problems at work, had been enrolled in anger management courses, and had an upcoming military criminal disciplinary proceeding. The suspect was killed by suicide during the incident.

   g. **Kauai School Threat Cluster:** On October 17, 2019, Kapaa and Kauai High Schools, Kapaa Elementary, and St. Catherine School, all on Kauai, were locked down for approximately one hour while police investigated threats made to both high schools. This came after several prior threats of violence were

made to Kauai schools. On September 30, 2019, threats were made to Kauai and Waimea High Schools. On September 25, 2019, a threat toward Kauai High School was reported; the threat was investigated, and classes continued as usual. On September 19, 2019, threats were made to Chiefess Kamakahelei Middle School, causing an investigation and increased security presence the following day.

h. **Pearl City Barricaded Gunman:** On September 12, 2019, a gunman in Pearl City created a standoff with police that lasted 14 hours. During this time, the gunman fired shots both into his Pacific Palisades neighborhood and directly at officers. The gunman was arrested and was identified as an individual who was recently released from a 20-year prison sentence for a similar 22-hour standoff with police.

i. **Harbor Lights Barricaded Assailant:** On February 11, 2019, police responded to an apartment complex in Kahului after a woman made a 911 call that a male acquaintance had assaulted her in her home. After police arrived, the suspect barricaded himself and the woman inside the apartment for approximately nine hours overnight before he was arrested. Due to the proximity to the University of Hawaii Maui campus, an emergency alert was issued to all students and staff, and the campus was temporarily locked down.

j. **Kekaha Barricaded Assailant:** On August 29, 2018, police responded to the home of a man who threatened to harm himself and had barricaded himself in his home with another individual. After a four-hour standoff with the Crisis Negotiations Team, police entered the home to find the two individuals dead in an apparent murder-suicide.

2. Although targeted and mass violence events are not common in Hawaii, it is critical not to confound a lack of historical examples as a lack of risk. As threats increase nationally and worldwide, Hawaii can expect to see an increase in threats in the state. Some recent examples of nationwide incidents are as follows.

a. **Nashville, TN Bombing:** On December 25, 2020, a suicide bomber detonated an RV bomb in downtown Nashville, injuring eight people and damaging dozens of buildings. After being parked for several hours, residents of nearby apartments reported hearing gunfire and an automated warning message broadcasting evacuation warnings to the nearby area. Police were able to successfully evacuate most of the area before the bomb detonated, injuring eight and causing significant damage to at least 40 businesses. The perpetrator was killed in the explosion, and his motive remains unknown. It was later found that the perpetrator's girlfriend had contacted police in 2019 reporting that he had been building bombs for more than a year at his residence.

b. **El Paso, TX Walmart Shooting:** In August 2019, a gunman began firing at civilians in the parking lot of a Walmart Supercenter before entering the crowded store and continuing to fire indiscriminately with a semi-automatic rifle. The perpetrator surrendered to the police after killing 23 people and injuring 23 others. The perpetrator had written a manifesto with white nationalist and anti-immigrant themes, citing a previous terror attack in New Zealand as a partial motive.

c. **Parkland, FL School Shooting:** In February 2018, a lone gunman entered Marjory Stoneman Douglas High School in southeast Florida and opened fire with a semi-automatic rifle, killing 17 people and

injuring 17 others. The perpetrator then fled the scene on foot by blending in with fleeing students before being arrested later in the day. The assailant was identified as a former student of the high school with a history of disciplinary problems. He was indicted on multiple counts of premeditated murder and is currently awaiting trial.

d. **Sutherland Springs, TX Church Shooting:** In November 2017, a lone gunman killed two individuals outside a Baptist church in southern Texas before entering the church and opened fire with a semi-automatic rifle, killing 26 and injuring 20 others. A former NRA firearms instructor who was worshipping in the church returned fire, causing the perpetrator to flee. The worshipper, along with another individual, pursued the assailant in a vehicle chase until the suspect lost control and crashed. When police arrived on-scene, they found the individual dead from a self-inflicted gunshot wound. Investigators reported that the incident was motivated by a dispute with the perpetrator's mother-in-law.

e. **New York City, NY Vehicle Ramming Attack:** On October 31, 2017, a man drove a rented pickup truck directly into cyclists and pedestrians along the Hudson River Park bike path in Manhattan, New York City, killing eight and injuring 11 others. The individual drove into victims for approximately one mile before crashing into a school bus, exiting his vehicle wielding two guns, and being apprehended by police. The perpetrator was a self-radicalized supporter of ISIL who followed the group's social media advice on how to carry out vehicular attacks. A federal grand jury indicted the assailant with multiple and attempted murders in aid of racketeering, destruction of a motor vehicle, and providing material support to ISIL.

f. **Portland, OR Train Knife Attack:** In May 2017, a self-described white nationalist harassed two teenage girls on the Portland light-rail system with hate speech toward a variety of ethnicities and religions before stabbing three men who attempted to de-escalate the situation. Two of the men were killed, and the third man was seriously injured. The perpetrator was apprehended by police and later tried and convicted of multiple counts of aggravated murder and one count of attempted murder.

g. **Dallas, TX Police Shooting:** In July 2016, a man opened fire at groups of police officers patrolling and protestors attending a Black Lives Matter protest in Dallas. The perpetrator then continued to a nearby community college building, during which he encountered and killed another officer. He encountered several other officers as he attempted to make his way into the building, eventually succeeding and barricading himself while firing indiscriminately at police. Police negotiated with the individual for several hours before utilizing a bomb disposal remote control vehicle to detonate near the assailant, killing him. During negotiations, the perpetrator claimed to have placed several explosives around downtown Dallas. A sweep was conducted by police, and no explosives were found. Throughout the incident, five police officers were killed, and nine other officers and two civilians were injured.

h. **Orlando, FL Pulse Nightclub Shooting:** In June 2016, an ISIL sympathizer opened fire inside the Pulse Nightclub in Orlando with a semi-automatic rifle and semi-automatic pistol. After shooting indiscriminately for several minutes, the assailant began a hostage situation in one of the club's bathrooms. After an hours-long standoff, the police breached the building and engaged in fire with the assailant, killing him. A total of 49 people were killed and 53 were injured. During the standoff,

the perpetrator called 911 to swear allegiance to the leader of ISIL and claimed the recent killing of high-level ISIL officers by the U.S. in a military airstrike the previous month was the motivation for the incident.

2.2.5 VULNERABILITY ANALYSIS

1. This section provides an overview of key geographic, demographic, and infrastructure vulnerabilities that may have significant consequences for how the state is affected by, responds to, and recovers from a terrorism or targeted violence incident. This is not a complete vulnerability analysis and should be looked at in conjunction with the HI-EOP.

   a. **High Tourism Locations:** The Hawaii economy remains heavily reliant on both domestic and international tourism; in 2019, tourism generated approximately 23% of local economic activity in Hawaii. [7] Several iconic locations throughout the state with year-round tourism industries create clear targets for terrorist attacks or other active assailant situations, as evidenced by worldwide terror attacks in recent years. Many sites across the state can be considered a high threat for terrorist or targeted violence actions.

   b. **Government Facilities:** Due to recent political and racial unrest, government facilities have become an elevated target for protests, both peaceful and violent. In Spring 2020, a protest at the Michigan State Capitol was attended by armed militias, and weeks later, the Chamber of the House of Representatives was mobbed by the same protestors carrying semiautomatic rifles and demanding entrance. In January 2021, the U.S. Capitol Building in Washington, D.C. was breached by thousands of armed protestors also demanding entrance into the Congressional chambers, as described in section 2.2.2 Terrorism. Hawaii government facilities, such as Washington Place, the State Capitol, Honolulu Hale, and other state legislature buildings, have the potential to become the target of similar demonstrations locally.

   c. **Extremist Organizations with Geographic Connections to Hawaii**: Since 2016, extremist political organizations have been growing in popularity nationwide. The goal of these organizations is often to engage in political violence as they promote far-right, neo-fascist views. In January 2021, several members of these groups were involved in the violent siege of the U.S. Capitol Building in Washington, D.C. Many of these organizations have known ties to Hawaii, including the Knights of Aloha, Proud Boys, and Young Americans for Freedom. Notably, the leader of the Oahu chapter of the Proud Boys (a former University of Hawaii Manoa student) was arrested by federal authorities due to his involvement in the Capitol unrest. The individual had also started the Oahu chapter of Young

---

[7] The Economic Research Organization at the University of Hawai'i, *How to Control Hawaii's Coronavirus Epidemic and Bring Back the Economy: The Next Steps,* April 2020. https://uhero.hawaii.edu/wp-content/uploads/2020/04/HowToControlHawaiisCoronavirusEpidemic.pdf

Americans for Freedom in an attempt to bring more conservative speakers and views to the University of Hawaii Manoa campus to counter "rampant liberalism" in Hawaii.[8]

d. **Race-Related Protests:** While the statewide threat in Hawaii related to race relations is generally low, 2020 brought nationwide high-profile racial tension and the subsequently increasing threat of escalating violence and domestic terrorism. Threat analysis across Hawaii on this vulnerability remains low; however, the race-based inequities in Hawaii leave native Hawaiian and the Pacific Islander populations at a great disadvantage[9] and may therefore be easier to radicalize.

e. **Military and Law Enforcement Facilities:** There are 15 U.S. military bases located throughout Hawaii, including the headquarters for the U.S. Indo-Pacific Command. Military bases have become an increasingly popular target for targeted violence incidents committed by civilians and service members alike. Recent high-profile incidents at the Pearl Harbor Naval Shipyard, Naval Air Station Pensacola, and Naval Air Station Corpus Christi highlight the potential ease of attacking a military facility. There are also multiple federal, state, and local law enforcement facilities located across Hawaii, with a similar level of threat.

f. **Educational Institutions:** While no active shooter or active assailant attacks have occurred in Hawaii since 2011, public and private K-12 schools, colleges, and universities are a popular target for targeted violence events. Between 2010 and 2018, schools and institutes of higher education made up for almost 21% of all active shooter incidents.[10]

g. **Maritime Activities:** With over a thousand miles of coastline and ten commercial harbors, the movement of persons and supplies on/off vessels provides additional opportunities for terrorism or targeted violence attacks. Between the high volume of cruise ships, commercial fishing boats, and the two inter-island ferries, several unique preparedness and response challenges arise for maritime activities.

h. **Cyberthreats:** While this plan does not cover cyberattacks or other cyber threats, many CCTAs may include cross-cutting methodologies that could include a cyber component. A well-executed cyberattack would likely include impacts on vulnerabilities of critical infrastructure and the public. Currently, cyberattack planning and critical infrastructure hardening is the responsibility of each department. In the future, coordinated state-wide cyber recommendations will be critical.

2.3 ASSUMPTIONS

1. The State of Hawaii and persons within, including both residents and visitors, are potentially at risk from an act of terrorism or targeted violence.

2. A terrorist threat or incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas, and may result in mass casualties.

---

[8] Hawaii Public Radio, https://www.hawaiipublicradio.org/post/proud-boys-hawai-i#stream/0
[9] Demographic, Social, Economic, and Housing Characteristics for Selected Race Groups in Hawaii, March 2018, State of Hawaii: DBEDT - Research and Economic Analysis Division https://files.hawaii.gov/dbedt/economic/reports/SelectedRacesCharacteristics_HawaiiReport.pdf
[10] FBI. Quick Look Active Shooter Incidents. https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics

3. Targets may include physical infrastructure or individuals and groups.

4. Coordination between law enforcement, public safety, and emergency management personnel is vital to ensure appropriate readiness actions are taken while still protecting law enforcement sources and methods.

5. The consequences (or cascading effects) of terrorism could outlast or surpass an initiating event. Effects may include long-term health and medical problems, extended economic issues, or political and social concerns.

6. A terrorist or targeted violence incident may be readily apparent to a responding organization or may be very difficult to initially detect and identify because of uncertainty about the cause or extent of the situation.

7. Prevention methods are implemented in an attempt to keep a terrorist attack or targeted violence incident from occurring. Prevention consists of those activities that serve to prevent, avoid, or stop an imminent, threatened, or actual act of terrorism against Hawaii, its population, and its interests. These activities decrease the perpetrators' chance of success, mitigate attack impact, minimize attack visibility, increase the chance of apprehension or detection, and obstruct perpetrators' access to resources.

8. First responder entities have situational awareness of potential threats and potential threat elements.

9. The SEOC will be activated for any act of terrorism and some acts of targeted violence.

10. The resources and/or expertise of local agencies could be quickly depleted by a response to a major terrorist incident and its consequences.

11. A terrorist event may create a level of disaster requiring federal assistance.

12. No single agency at the local, state, federal, or private level possesses the authority and the expertise to act unilaterally on many difficult issues that may arise in response to threats or acts of terrorism. Terrorism requires law enforcement, public safety, public health, and emergency management coordination.

13. The response to a threat or actual incident involves law enforcement and investigative activity as an integrated element.

14. Virtually all terrorist acts involve violations of laws. Therefore, law enforcement agencies gather and analyze intelligence on terrorists and may develop estimates of their intentions. Access to this criminal intelligence information may be limited, but significant threats must be communicated by law enforcement agencies to those local officials who can implement protective measures and alert the public.

15. The suspected or actual involvement of terrorists adds an additional dimension to incident management.

16. There are often competing needs in the aftermath of a terrorist act - law enforcement agencies want to protect the crime scene to gather evidence, while emergency responders may need to bring in extensive equipment and personnel to conduct search and rescue operations. It is essential for the incident command team to establish operating areas and formulate a plan of action which considers the needs of both groups.

17. Injuries from a terrorist attack may be both physical and psychological.

18. Recovery from a terrorist attack can be complicated by the presence of additional threats, extensive physical damages, and mass casualties.

19. Although this Annex takes into consideration the most probable scenarios relating to the primary categories of terrorism incidents, no assumptions should be made to the Annex being all-inclusive of every possible situation that a terrorism incident could create. Emergency responders will assess the situation and determine the best course of action based on their training and prescribed policies, plans, and procedures.

This page intentionally left blank.

3. CONCEPT OF OPERATIONS

3.1 GENERAL

1. This section provides an overview of how the State of Hawaii will coordinate the response to an actual or threatened act of terrorism or targeted violence, as defined in Section 1.2, including plan activation and the anticipated sequence of emergency events and priorities during each phase.

2. This section builds upon the Concept of Operations listed in the HI-EOP.

3. The Department of Homeland Security *Strategy for Countering Terrorism and Targeted Violence* outlines four goals that are aimed at enhancing prevention, protection, mitigation, response, and recovery from acts of terrorism and targeted violence. [11] The State of Hawaii subscribes to these goals as the foundation for its own efforts:

    a. **Goal 1:** Understand the evolving terrorism and targeted violence threat environment, and support partners in the homeland security enterprise through this specialized knowledge.

    b. **Goal 2:** Prevent terrorists and other hostile actors from entering the U.S. and deny them the opportunity to exploit the Nation's trade, immigration, and domestic and international travel systems.

    c. **Goal 3:** Prevent terrorism and targeted violence.

    d. **Goal 4:** Enhance U.S. infrastructure protections and community preparedness.

---

[11] DHS, *Strategic Framework for Countering Terrorism and Targeted Violence,* September 2019.
https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

3.2 RESPONSE ACTIONS

3.2.1 PLAN ACTIVATION

1. This document is an integrated part of the HI-EOP which outlines basic response practices. This plan provides an additional set of procedures that will be activated due to a suspected terrorism or targeted violence threat or actual event within the State of Hawaii.

2. The activation of this plan will be at the discretion of the OHS with a recommendation by the Hawaii Emergency Management Agency (HI-EMA). This plan will be activated if there is a potential for an event to be terroristic or targeted violence in nature, even if it is not definitively determined to be a terroristic event. Law enforcement entities determine if a threat or incident may potentially be terrorism or targeted violence or if there is intelligence connecting the incident to a known entity as a part of the initial situation assessment. Law enforcement threat findings will influence plan activation.

3.2.2 INITIAL RESPONSE

1. Any actualized threat situation will likely be identified at the local level through a law enforcement entity. During/after an incident, 911 is typically notified through public reaction and local law enforcement is dispatched to the incident location. Law enforcement will alert dispatch, who also acts as the County Warning Point of the situation, and if necessary, the local Emergency Operations Center (EOC) will be activated.

   a. Local EOC staffing will include the local Emergency Management or Civil Defense Agency (CDA) along with all relevant EOC positions and partners.

   b. The local EOC will notify the State Warning Point (SWP) of activation, and the SEOC may be activated if necessary. The state and local EOCs will determine the need for further escalation for federal assets.

2. Early official communications regarding an incident will be limited based on the details known. Only verified facts should be disseminated, and rumors or speculations should not be communicated. Type of information communicated may include:

   a. Facts that are known about the incident.

   b. Location of the incident.

   c. Time/date of the incident.

SEOC activated if necessary

State Warning Point

Local EOC

Local EOC Activation Notification Flow to SEOC
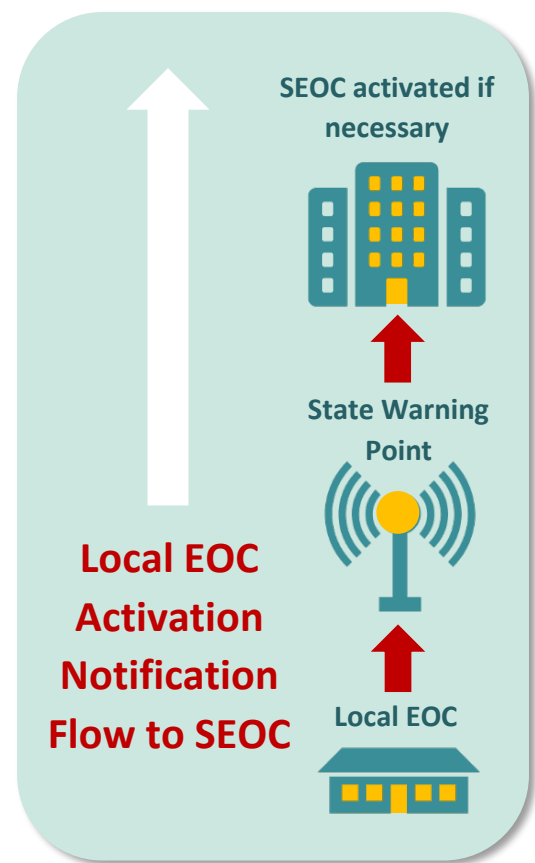
    d.   Populations affected by the incident.

    e.   The incident perpetrator(s) if known.

3. Initial response objectives for all jurisdictions should be in support of life safety, incident stabilization, protection of property and the economy, and preservation of culture and the environment. This will likely include a focus on:

    a.   Initial law enforcement response.

    b.   Threat neutralization actions.

    c.   Emergency medical services (EMS) response.

    d.   Implementing lifeline stabilization targets.

    e.   Initial targeted information distribution to the public, responders, and government entities.

    f.   Intelligence and investigation activities.

    g.   Healthcare surge capacity and stabilization.

4. The locally affected county or jurisdiction is designated as the initial primary responder. Key responsibilities of the affected county or jurisdiction include:

    a.   Save lives.

    b.   Establish response operations.

    c.   Protect property.

    d.   Incident scene management.

    e.   Threat identification and neutralization.

    f.   Establish initial communications.

    g.   Establish EOC operations.

    h.   Activate responders and auxiliary support.

    i.   Enact processes to request additional support as necessary.

    j.   Establish medical procedures and surge capacity at the hospital level.

    k.   Establish vertical communication including with HI-EMA and OHS.

    l.   Declare county-level emergency, if necessary.

5. Other counties that are unaffected by the event may support the primary response jurisdiction. Key responsibilities of support jurisdictions unaffected by the event include:

    a.   EOC activation at a minimum level to support resource coordination and mutual aid to impacted jurisdictions.

b. Enact protective measures within the jurisdiction to reduce the risk of secondary threats.

c. Establish resource and personnel support protocol dependent on the situation and the risk of further attacks.

6. If necessary, the state will support response as needed by the local or affected jurisdiction. All state agencies are responsible for coordinated response efforts through key tasks including:

a. Activate the SEOC.

b. Resource coordination and mutual aid in support of the affected local jurisdictions.

c. Declare state-level emergency, if necessary.

d. Request federal level assets in support of the response.

e. Request for a federal emergency declaration, if necessary.

7. If an incident is assumed to be tied to a terrorism event, additional protective measures may be put into place starting from the local level and potentially including statewide assets. Protective measures may be focused to include similar targets, facilities, or other known vulnerabilities.

8. Any suspected threat should produce law enforcement searches for additional threats. It is the responsibility of the local jurisdiction to identify additional potential threats at the incident site, as well as potential secondary targets in the jurisdiction.

3.2.3 SUSTAINED RESPONSE

1. Sustained response objectives for all jurisdictions continue to be in support of life safety, incident stabilization, protection of property and the economy, and preservation of culture and the environment. The sustained response will likely include a focus on:

a. Media and public information coordination.

b. Maintaining lifeline stabilization targets.

c. Increased information management needs.

d. Sustained law enforcement response.

e. Ongoing intelligence and investigation activities.

f. Management of healthcare surge capacity and stabilization plans.

g. Witness management including interviews, personal effects management, and returns.

h. Support services for witnesses, responders, and the general public, including mental and behavioral health as well as spiritual care.

i. Development and operations of family assistance centers (FAC).

j. Fatality management services including victim identification, processing, storage, and family notifications.

3.2.4 TRANSITION TO RECOVERY

1. Recovery transition may be a slow process depending on the type and the size of the incident. This process will be determined at the time of the incident. The State of Hawaii is following the National Fire Protection Association (NFPA) 3000 recommendations of organizing recovery into three major subcategories:[12]

   a. Immediate Recovery.

   b. Early Recovery.

   c. Continued Recovery.

3.2.4.1 IMMEDIATE RECOVERY

1. Immediate recovery may include a focus on:

   a. Media and public information coordination.

   b. Finalizing lifeline stabilization targets.

   c. Event response documentation consolidation and evaluation.

   d. Sustained witness management and support services.

   e. Sustained family assistance center operations, including victim assistance protocols.

   f. Reestablishing normal municipal operational standards and expectations.

   g. Operational security and public safety protocols.

   h. Damage assessment.

2. Damage assessment protocols will follow recommendations of the NFPA 3000 and include:[13]

   a. Civilian and responder casualties.

   b. Bystander and witness effects.

   c. Damage to infrastructure.

   d. Damage to responding organizations.

   e. Geographical area closures.

   f. Business impact.

   g. Victim populations affected, which may include:

---

[12] NFPA 3000 20.1.1.1
[13] NFPA 3000 20.2.2.5

- Children and youth.

- First responders.

- Native Hawaiian communities.

- Elderly (kupuna) populations.

- Individuals with disabilities or other access and functional needs.

- Individuals who are deaf or hard of hearing.

- Individuals with limited English proficiency.

- High-risk populations.

- Lesbian, gay, bisexual, transgender, and queer populations.

- Military veterans.

- Underserved and socially isolated populations, including those historically underserved due to race, socio-economic status, disability, or sexual orientation.

- Undocumented populations.

- Other specialized populations.

3.2.4.2   EARLY RECOVERY

1. Early recovery is defined as the operational period after immediate recovery where processes for agency coordination, meeting protocols, accountability, initial damage assessment, and primary victim assistance, including reunification and notifications, are actively being managed.[14]

2. Early recovery may include a focus on:

   a. Operational security.

   b. Damage assessment.

   c. Public information coordination.

   d. Resource needs analysis.

   e. Analysis of event consequences.

   f. Cascading event threats.

   g. Volunteer management.

   h. Donations management.

   i. Victim advocacy, assistance, and services.

---

[14] NFPA 3000 20.3

    j.   Federal emergency funding opportunities and grants.

3. A resource needs analysis will be conducted to plan for ongoing recovery operations. Resource needs analysis will include:

    a.   Potential deaths and injuries.

    b.   Business impact.

    c.   Mental and emotional requirements.

    d.   Property damage.

    e.   System or geographical area disruptions.

    f.   Investigation and scene control management.

3.2.4.3   CONTINUING RECOVERY

1. Continuing recovery is defined as the operational periods after early recovery when previous recovery efforts have been stabilized.[15]

2. Continuing recovery may include a focus on:

    a.   Business impact evaluation.

    b.   Coordination of the restoration, rebuilding, and replacement of facilities, infrastructure, materials, equipment, tools, vendors, and suppliers.

    c.   Restoration of the supply chain.

    d.   Reopening or relocation of vital facilities.

    e.   Continuation of communications with stakeholders and the public.

    f.   Roles and responsibilities of the individuals implementing the recovery strategies.

    g.   Internal and external (vendors and contractor) personnel.

    h.   Adequate controls to prevent corruption or unlawful access to data during recovery.

    i.   Investigation of fraud associated with disaster assistance and assurances of consumer protection.

    j.   Maintenance of pre-incident controls.

    k.   Long-term community resiliency.

    l.   Volunteer and donation management.

    m. Identification of gaps that requires supplemental state or federal assistance.

    n.   Cost recovery.

---

[15] NFPA 3000 2.4.1.1

3.3 DIRECTION, CONTROL, AND COORDINATION

1. The Governor has primary direction, control, and coordination of all state resources and is responsible for the safety and welfare of Hawaii's residents and visitors, as well as the continuity of state government and requesting federal assistance.

2. The Incident Commander, assisted by a staff sufficient for the tasks to be performed, will manage the emergency response at the incident site from an Incident Command Post (ICP). If multiple incident locations are involved, multiple incident command operations may be established.

3. All threats and acts of terrorism are criminal events. The FBI is the lead agency for criminal investigations of terrorist acts or terrorist threats and intelligence collection activities within the U.S., including in the state of Hawaii.

4. Local and state authorities always maintain control of their response resources and continue to operate while the FBI integrates into the on-scene emergency management system.

3.3.1 IMPLEMENTATION OF THE INCIDENT COMMAND SYSTEM (ICS)

1. Use of the Incident Command System (ICS) is required by all emergency response agencies when responding to actual or suspected terrorist events.

2. If there is a local incident site, an ICP will be established to manage emergency operations at that site. The ranking official from the agency with primary responsibility for the incident will establish incident command and assume the position of Incident Commander.

3. The ICP is responsible for the coordination and deployment of scene response activities. Incident response priorities will include:

    a. Life safety.

    b. Scene stabilization.

    c. Conservation of property and resources.

4. The Incident Commander will direct and control responding resources and designate emergency operating areas. Typical operating area boundaries established for a terrorist or targeted violence incident may include:

    a. **Crime Scene Boundary:** Defines the crime scene area. The crime scene may also be referred to as the "red zone" or "working point." Access to the crime scene may be restricted by state, federal, or local law enforcement personnel. Response activities within the crime scene may require special care to protect evidence.

    b. **Hazardous Materials (Hazmat) Boundary:** Defines the hazmat site, which may also be referred to as the "hot zone," "isolation area," or "exclusion zone." The hazmat area may also include the upwind "warm zone" utilized for contamination control and rescue staging. Depending on the spread of contaminants, the hazmat site may include some of (or the entire) crime scene. Entry into the hazmat boundary is normally restricted to response personnel equipped with personal protective equipment and using decontamination procedures.

    c. **Incident Boundary:** Includes the crime scene, the hazmat area, and the "cool zone" or "support zone" used for incident support operations such a resource staging and casualty collection. Additionally, areas where protective actions (such as shelter-in-place or evacuation) may be recommended, or mandatory measures (such as quarantine) may be imposed inside the incident boundary. Access to this area is normally controlled. If a quarantine is implemented, egress may also be restricted.

5. As other response disciplines and/or state and federal responders arrive at the ICP to support field operations and incident management, the Incident Commander will transition to a unified command.

6. The Incident Commander and the EOC/SEOC will divide the responsibilities of incident management.

    a. The Incident Commander will manage field operations at the incident site and in adjacent areas.

    b. The EOC will mobilize and provide local resources, disseminate emergency public information, organize and implement large-scale evacuation, coordinate care for casualties, coordinate shelter and mass care for evacuees, arrange mortuary support, and request assistance from other jurisdictions or state/federal partners, if necessary.

7. Representation of fire, law enforcement, and medical responders is necessary at the ICP to allow for the transition from threat neutralization and lifesaving measures to crime scene investigation.

8. With the arrival of state and federal responders, the FBI may establish a Joint Field Office (JFO) for overall coordination and management of response operations between government agencies and response partners from the private sector.

9. The need for a State Disaster Recovery Coordinator shall be determined and, if activated, placed inside UC until the command is disbanded.[16]

---

[16] NFPA 3000 20.2.2.4.1:

3.3.2 STATE EMERGENCY RESPONSE OPERATIONS

3.3.2.1 ACTIVATION OF THE STATE EMERGENCY OPERATIONS CENTER (SEOC)

1. The SEOC may be fully or partially activated by HI-EMA for any terrorist or targeted violence threat or actualized incident. Local EOCs will notify the SEOC for activation.

2. SEOC activation enables representatives from key state agencies to coordinate information with local, federal, and supporting state agencies as dictated by the situation. Responsibilities of the SEOC include but are not limited to:

   a. Assess the potential threat or impact of a similar event elsewhere in Hawaii.

   b. Coordinate and manage resources and mutual aid.

   c. Coordinate communications between responders.

   d. Coordinate public information, which may include establishing a Joint Information System (JIS) or Joint Information Center (JIC).

   e. Share information with key state and local government officials regarding the situation.

   f. Compile information regarding state and local preparedness status or needs.

   g. Conduct briefings.

   h. Issue alerts, notifications, and advisories consistent with federal levels or formats.

3.3.2.2 ORGANIZATIONAL STRUCTURE

1. SEOC organization is based upon grouping of assigned primary functions. Depending on the specific threat or actualized incident, Command and General Staff positions and SESFs are staffed at various levels either in person or remotely.

2. The specifics of an event may cause various agencies representing critical services to shift assignments from technical support to primary or lead agency positions.

3.3.2.3 MOBILIZATION AND DEPLOYMENT OF STATE RESOURCES

1. Several emergency operations facilities may be established for the management of the incident. HI-EMA, through the SEOC, may deploy liaison personnel to any or all of the following locations:

a. Local ICPs.

b. Local EOCs.

c. JIC.

d. Department Operations Center (DOC).

e. State Emergency Response Team (SERT).

f. Policy Group.

g. JFO.

2. Other State resources requested by local jurisdictions will be mobilized through the SEOC and/or the appropriate SESF in accordance with the provisions of the HI-EOP.

3.3.2.4 DEACTIVATION OF STATE RESPONSE

1. When an incident no longer requires the support and coordination functions provided by the SEOC, or those functions can be effectively managed by individual agencies using regular coordination mechanisms, deactivation occurs.

2. Deactivation of the state's response and demobilization of deployed state personnel will be at the direction of the Director of Emergency Management after coordination with the affected local jurisdictions. Deactivation of specific assets, operations, or facilities may be staged as conditions warrant.

3. After-action review and improvement planning is arranged as part of deactivation planning.

4. HI-EMA will support long-term recovery by coordinating participation from state departments, private sector agencies, and non-governmental organizations (NGOs).

3.3.3 COORDINATION OF INCIDENT CONSEQUENCE MANAGEMENT ACTIVITIES

1. Consequence management includes measures to protect public health and safety, restore essential services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.

2. Consequence management will be coordinated by both the local affected jurisdiction and the state through unified command. The state may seek federal assistance if needed.

3. Law enforcement agencies involved in consequence management will inform response and recovery agencies of decisions made that may have implications for resource management.

4. Until crisis management activities have been concluded, law enforcement will participate in unified command or EOC operations to support consequence management activities involving the protection of the crime scene, evidence collection, and investigative processes.

This page intentionally left blank.

4. ROLES AND RESPONSIBILITIES

4.1 LOCAL GOVERNMENTS

1. Maintain regular preparedness activities, including developing and maintaining an up-to-date emergency operations plan (EOP) and supporting Annexes.

2. Local jurisdictions maintain primary responsibility for coordinating initial response activities.

3. County jurisdictions will follow policies and procedures as outlined in respective EOP and Annexes.

4. The primary responsibility of county governments is to provide an initial response to save lives and protect public health, safety, property, and the environment.

4.1.1 LAW ENFORCEMENT

1. Conduct anti-terrorist operations and maintain terrorist profile information. Advise emergency management staff and state and federal agencies of significant terrorist threats.

2. Conduct terrorism response training programs for law enforcement personnel and support public education and awareness activities.

3. Establish an incident command post (ICP) at the scene to manage on-scene incident response and transition responsibility to state or federal agency, if necessary. The Incident Commander will:

    a. Determine and implement immediate protective actions for emergency responders and the public in the vicinity of the incident site.

    b. Establish communications.

    c. Provide an initial incident assessment, request additional resources if needed, and provide periodic updates to the emergency operations center (EOC).

    d. Request a liaison officer from each participating agency is present at the ICP, if necessary.

    e. Establish a specific division of responsibilities between the incident command operation and the EOC.

    f. Alert the EOC of the need for additional resources or mutual aid.

    g. Transition the incident command operation to a unified command operation when external resources arrive.

4. Establish and maintain the perimeter around the incident site and neutralize the threat.

5. Alert the County Warning Point of the situation.

6. Manage traffic and crowd control measures and conduct evacuation measures, if necessary.

7. Brief emergency response personnel on crime scene protection.

8. Assign personnel to the Joint Information Center (JIC).

9. Notify state and federal authorities of terrorism (if suspected) and:

    a. Coordinate the deployment and operation of counter-terrorist response elements.

    b. Coordinate and conduct reconnaissance in the vicinity of the incident site to identify threats from secondary attacks of cascading effects.

    c. Coordinate to investigate the incident and identify and apprehend suspects.

10. Coordinate and conduct improvised explosive device (IED) operations during incidents, including:

    a. Conducting an initial assessment of IED or suspicious device and requesting appropriate assets.

    b. Rendering IED safe.

    c. Establishing "safety zones" for emergency responders and victims, if needed.

4.1.2 FIRE, HAZMAT, AND EMS

1. Conduct terrorism response training programs and participate in training drills and activities.

2. Assign personnel to the ICP and establish a unified command.

3. Assign personnel to the JIC.

4. Coordinate and conduct all fire and rescue operations during incidents, including:

    a. Dispatching and deploying fire personnel and equipment during an emergency.

    b. Identifying requirements for debris clearance to expedite fire response and search and rescue.

    c. Controlling fires, if necessary.

    d. Conducting search and rescue operations as needed.

    e. Identifying unsafe structures and restricting access pending further evaluation by the Public Works or Engineering staff.
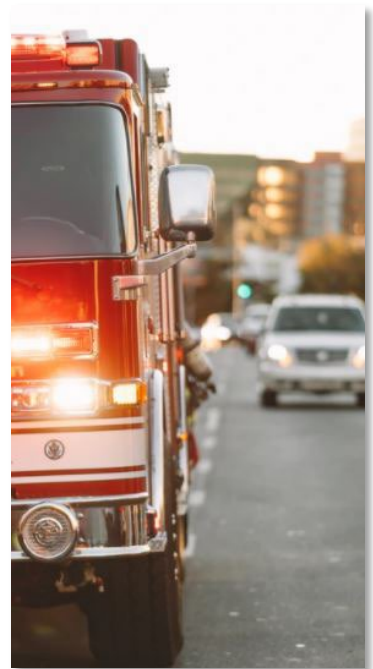
f. Providing support for evacuation operations if requested.

5. Coordinate and conduct hazardous materials (Hazmat) operations during incidents, including:

   a. Establishing "safety zones" and decontamination area for emergency responders and victims, if needed.

   b. Carrying out initial decontamination of victims, if required. Procedures must be available for emergency decontamination of large numbers of people.

   c. Coordinating with medical facilities to ensure monitoring and decontamination of victim intake.

6. Coordinate and conduct emergency medical operations during incidents, including:

   a. Responding to medical emergency calls and providing emergency medical care to the injured.

   b. Establishing a triage area, if necessary.

   c. Managing and conducting timely patient transport to appropriate medical facilities.

4.1.3 EMERGENCY MANAGEMENT

1. Coordinate regularly with law enforcement and other response agencies with respect to the terrorist threat to:

   a. Determine appropriate readiness actions during periods of increased threat.

   b. Develop common communication procedures.

   c. Conduct terrorism response training programs and participate in training drills and activities.

   d. Maintain countywide plans and procedures.

2. Activate and staff local EOC(s). Responsibilities of EOC personnel include but are not limited to:

   a. Notifying the SWP.

   b. Requesting and managing mutual aid.

   c. Developing and transmitting situation reports to the SEOC as the emergency unfolds and changes.

3. Notify, brief, and advise elected officials.

4. Assign personnel to the JIC.

5. Notify state and federal agencies as appropriate.

6. Coordinate Family Assistance Center (FAC) and Victim Identification Center (VIC) operations with law enforcement, state agencies, and NGO partners.

4.1.4 ELECTED OFFICIALS

1. Provide policy guidance with a response to anti-terrorism and counter-terrorism programs.

2. Declare a countywide emergency.

3. Request assistance from the state.

4. Assign personnel to the JIC.

4.1.5 OTHER COUNTY DEPARTMENTS

1. Provide personnel, equipment, and supply support for emergency operations upon request from the EOC.

2. Assign personnel to the EOC.

3. Activate the Department Operations Center (DOC).

4.2 STATE GOVERNMENT

4.2.1 OFFICE OF HOMELAND SECURITY (OHS)

1. Prepare comprehensive plans and programs for homeland security and facilitate the implementation and maintenance of these plans.

2. Develop and maintain this Annex; ensure its consistency with State and Federal guidelines and regulations.

3. Facilitate the processes needed to respond to and recover from a homeland security-related incident including a coordinated comprehensive planning program.

4. Ensure coordination and cooperation among all partner organizations for homeland security; public agencies, including county, state, and federal agencies; and private organizations.

5. Develop and maintain lists of critical infrastructure and conduct studies and surveys of the vulnerabilities of same. Participate in planning efforts to mitigate identified critical infrastructure risks.

6. Develop and maintain a capability to process security clearance applications.

7. Foster coordination on security matters within the Pacific region, such as coordinating planning efforts and sponsoring discussions, seminars, and conferences.

8. Support coordination across federal, state, and local agencies during after-action reporting and recovery.

9. Manage the intelligence and information monitoring of a terrorism or targeted violence incident on the state level.

10. Assign personnel to imbed at critical incident response or coordination sites to ensure critical intelligence sharing.

11. Share intelligence with limited key federal, state, and local government officials in accordance with protected information sharing protocols and the needs of the decision makers.

4.2.2 HAWAII EMERGENCY MANAGEMENT AGENCY (HI-EMA)

1. Manage the response of a terrorism or targeted violence incident at the state level through facilitating the incident management at a statewide level.

2. Maintain SWP to receive notification from local EOCs and take immediate and appropriate actions.

3. Activate and staff the SEOC as appropriate based on the incident and coordinate the response from the state level. Responsibilities of SEOC personnel include but are not limited to:

    a. Serving as the point of contact for communications between state and local responding agencies.

    b. Coordinating and managing resource management and mutual aid.

    c. Compiling information regarding state and local preparedness status or needs.

12. Assign personnel to any or all of the following locations:

    a. Local ICPs.

    b. Local EOCs.

    c. JIC.

    d. DOCs.

    e. State Emergency Response Team (SERT).

    f. Policy Group.

    g. Joint Field Office (JFO).

13. Establish the process for information sharing with key state and local government officials regarding the situation.

14. Provide support to all ongoing response operations as needed.

15. Coordinate FAC and VIC operations with local jurisdictions, other state agencies, and NGO partners.

16. Notify the Crime Victims Compensation Commission (CVCC) of the incident.

4.2.3 OFFICE OF THE GOVERNOR

1. Provide policy guidance with response to anti-terrorism and counter-terrorism programs.

2. Provide general direction for response and recovery operations in the aftermath of a terrorism incident.

3. Review and coordinate public release of information related to emergency activities.

4. Establish a Policy Group at the SEOC.

5. Assign personnel to the JIC and/or JFO.

6. Declare a state-level emergency.

7. Request federal level assets in support of the response.

8. Request a federal emergency declaration.

4.2.4 DEPARTMENT OF PUBLIC SAFETY (DPS)

1. Provide technical assistance and advice to state departments, agencies, and local jurisdictions in counter- and anti-terrorism planning, training, and exercises, when requested.

2. Serve as the primary state agency for law enforcement operations, intelligence, and traffic and crowd control.

3. Provide technical response assistance to local jurisdictions at the scene of a terrorist incident.

4. Evaluate the nature, credibility, and implications of the threat.

5. Coordinate investigative efforts with appropriate local and state law enforcement agencies.

6. Share information with the State Law Enforcement Coalition (SLEC) members regarding the situation.

7. Direct the Crime Victim Compensation Commission (CVCC) to provide services including:

    a. Deploy to response locations as directed by the SEOC.

    b. Mobilize mass violence response team and mass violence incident response notification system.

    c. Provide victim assistance services as outlined in the CVCC Mass Violence Victim Response Plan.[17] Victim services may include physical, mental, and behavioral health support, victim compensation, and financial assistance.

---
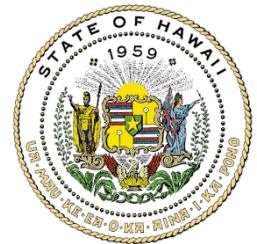
[17] CVCC Mass Violence Victim Response Plan

d. Prepare needs assessment of immediate, short-term, and long-term victim needs specific to the terrorism or targeted violence incident.

e. Support long-term recovery operations for victims.

4.2.5 NATIONAL GUARD

1. Prepare and conduct force protection training for state and local agencies, as requested.

2. Provide logistics support, as requested.

3. Provide support by ensuring that the Civil Support Team (CST) is prepared for emergency response. To request CST support, local jurisdictions should submit a request for assistance through the local EOC.

4.2.6 STATE EMERGENCY SUPPORT FUNCTION (SESF) LEAD AGENCIES

1. Update policies, procedures, and emergency notification procedures to reflect organizational changes or additions.

2. Ensure development of any specialized procedures necessary to implement any applicable responsibilities of this Annex.

3. Assign personnel to the SEOC and coordinate required actions involved in SESF response as outlined in the HI-EOP.

4.3 FEDERAL GOVERNMENT

4.3.1 FEDERAL BUREAU OF INVESTIGATION (FBI)

1. Provide technical assistance and advice to state departments, agencies, and local jurisdictions in counter- and anti-terrorism planning, training, and exercises, when requested.

2. Serve as the lead federal agency for crisis management during a terrorism or targeted violence event, including serving as the lead law enforcement authority for investigation and recovery of evidence.

3. Provide technical response assistance to local jurisdictions at the scene of a terrorist incident.

4. Notify other federal agencies, including DHS, FEMA, and members of the National Intelligence Council, of a significant threat.

4.3.2 FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

1. Serve as the lead federal agency for consequence management and operate as defined in the National Response Framework (NRF).

2. Assign personnel to the JFO or near the projected incident location if requested by the FBI.

3. The FEMA Region IX Administrator will activate the Regional Response Coordination Center to support federal regional response coordination when deemed necessary based on potential consequences of the incident.

4. Provide assistance, as requested from local jurisdictions and/or state agencies. The NRF provides an outline for the coordination of federal support agencies.

4.3.3 OTHER DEPARTMENT OF HOMELAND SECURITY (DHS) AGENCIES

1. Review and analyze intelligence and threat information as requested by the FBI.

2. Decide, in coordination with other federal entities, whether a National Terrorism Advisory System (NTAS) Alert should be issued. NTAS Alerts will only be issued when intelligence has been deemed credible.

3. Assign personnel to the JFO or near the projected incident location if requested by the FBI.

4. Support investigative actions as requested by the FBI.

4.3.4 DEPARTMENT OF DEFENSE

1. Maintain equipment to support OHS or other partners during a homeland security-related incident.,

2. Utilize intelligence and information monitoring capabilities for situational awareness and operational readiness.

3. Serve as the lead response agency for any incident on military property, including any military bases or housing.

4. Serve as a support agency for any incident involving military personnel.

5. Assign personnel to the JOC as requested by the FBI.

6. Provide logistics support in accordance with federal laws and operational capabilities.

7. Maintain responsibility for military assets, including potentially executing lockdown procedures on military property, if necessary.

4.4 NON-GOVERNMENTAL ORGANIZATIONS (NGOS) AND PRIVATE SECTOR

1. NGOs, voluntary organizations, and private sector partners with disaster response missions and/or programs that support the state's emergency planning and response efforts are assigned to SESFs as outlined in the HI-EOP.

2. Provide information, resources, or disaster relief services as defined in this plan and annexes, and/or as outlined in their respective charters, bylaws, or agreements with state agencies.

3. Provide support with FAC and VIC operations as well as long-term recovery operations.

4.4.1 TOURISM/VISITOR INDUSTRY

1. The Hawaii Tourism Authority (HTA) maintains a support role in emergency response.

2. During a terrorism or targeted violence incident, HTA will activate the agency's DOC and staff the SEOC. Typically, HTA personnel will staff SESF #15 positions.

3. Provide public safety information to visitors and tourists.

4. Support visitor evacuation, if necessary.

5. Support recovery actions and combat public misinformation and rumor control.

This page intentionally left blank.

5. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION

5.1 OVERVIEW

1. Developing a Common Operation Picture (COP) for response partners is essential in ensuring effective and coordinated response and recovery operations.

2. Potential and actualized threat information will be collected, evaluated, and disseminated to critical stakeholders to provide a COP.

3. Information storage and handling will be carried out in accordance with procedures outlined in the HI-EOP.

5.2 MONITORING

5.2.1 OVERVIEW

1. Although all people in the State of Hawaii have some responsibility for monitoring and reporting observed threats, the responsibility of coordinating threat concerns falls onto the Hawaii State Fusion Center (HSFC), which is under the direction of OHS.

2. The HSFC is tasked with gathering information and intelligence, providing analysis, and advising on threats, including notifying individuals, agencies, and organizations as necessary.

3. The HSFC monitors statewide threat indicators and trends, including terrorism, cybersecurity, and drug trafficking. Additionally, the HSFC works in conjunction with partner agencies and coalitions to monitor additional topics such as child abductions and school threats.

4. The HSFC monitors threat indicators and trends to gain worldwide situational awareness in the context of application to Hawaii. Monitoring activities focus on identifying and screening for potential high threat situations, locations, and groups statewide by analyzing nationwide/worldwide threats along with local intelligence. Threats may be economic, physical, or climate-related, all of which may leave Hawaii vulnerable to terrorism or targeted violence events.

5. The primary jurisdiction of HSFC responsibility is limited to Hawaii; however, the HSFC monitors situations outside of the state, including international and domestic threats for situational awareness and insight on threats to Hawaii.

6. Specific concerns of the HSFC may arise through both routine passive monitoring and focused monitoring requests. Focused monitoring requests may come from either local law enforcement entities or other fusion centers via a request for assistance process. The results of these inquiries help to re-focus efforts or concerns both in Hawaii and nationwide.

7. The HSFC has documented procedures highlighting responsibilities and specific policies and protocols. External stakeholders, including individual agencies that coordinate with the HSFC, also have organization-specific processes and procedures. All available procedural documentation should be consulted for complete protocol understanding.

5.2.2 KEY AGENCIES

1. The HSFC is designed to be a coordinated element of many different partners, both governmental and nongovernmental. The following agencies are habitually involved in HSFC activity:

   a. DHS.

   b. FBI.

   c. U.S. Indo-Pacific Command Joint Operations Center.

2. Additional personnel are often tasked to participate but not always represented. These agencies may vary depending on the type and scope of the incident. Support agencies may include:

   a. Local law enforcement agencies.

   b. Hawaii Army National Guard.

   c. Hawaii Attorney General.

   d. Hawaii Department of Land and Natural Resources.

   e. Hawaii Department of Transportation.

   f. Hawaii Department of Health.

3. Relationships with partners help build a network of monitoring capabilities. Regular meetings support relationship building and monitoring capabilities. Partner agencies may include:

   a. DHS, including Homeland Security Information Network (HSIN) members.

   b. FBI.

   c. Joint Terrorism Task Force members.

   d. U.S. Immigration and Customs Enforcement.

e. U.S. Customs and Border Protection.

f. Local law enforcement agencies.

g. Local officials.

h. U.S. Secret Service.

i. High-Intensity Drug Trafficking Area agencies, including the Drug Enforcement Administration and other Department of Justice components.

5.2.3 KEY LOCATIONS

1. The HSFC is located on Oahu.

2. The existing HSFC sites are under expansion to include satellite sites at the county level. Until expansion is completed, all counties participate in HSFC activity remotely, with direct communications between the law enforcement entities statewide.

3. If the HSFC location is compromised, there is no predetermined location for backup activation sites. A Continuity of Operations Plan exists for HSFC activity and will be enacted in the case of a compromised location. The HSFC building site is physically hardened to reduce the opportunity of compromise.

5.2.4 SYSTEMS/MONITORING TOOLS

1. Monitoring can include an array of different sources, including but not limited to:

    a. Media sources.

    b. Fusion centers (local and national).

    c. News media including television news and print media.

    d. Law enforcement intelligence.

    e. Social media monitoring.

    f. Dark web monitoring.

    g. Coordination meetings with statewide partners.

2. Social media is monitored in compliance with state and federal regulations. Targeting specific individuals without a warrant is not permissible; however, general monitoring remains allowed.[18]

---

[18] NFPA 3000 17. 5 Social media shall be permitted to serve as an information and intelligence platform for Unified Command.

5.3 DETECTION

5.3.1 OVERVIEW

1. Detection is the process by which a threat is identified, validated, and the information about that threat is disseminated.

2. Detection, like monitoring, is a shared responsibility across the State of Hawaii, with the responsibility of coordinating detection efforts being one of the roles of the HSFC, under the direction of the OHS.

3. The HSFC is responsible for screening and monitoring intelligence and beginning threat interpretations.

4. Unlike some other fusion centers, the HSFC is not a law enforcement fusion center. The HSFC should be used as an intel source and not as an investigative tool. Local and state law enforcement hold investigative and enforcement responsibilities in the State of Hawaii.

5. Intelligence is validated before any notifications take place. Information will be disseminated once it is validated.

6. Most intelligence will be validated through law enforcement agencies, including local, federal, or law enforcement from another state. Intelligence may also be validated through another fusion center or the private sector.
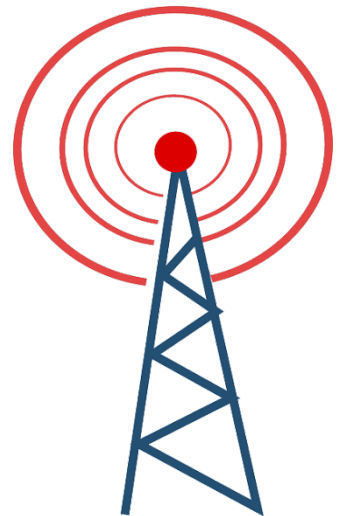
5.3.2 KEY AGENCIES

1. Agencies that will support threat intelligence validation may include:

    a. Fusion centers.

    b. Local or state law enforcement.

    c. Federal law enforcement.

    d. Other sectors that can provide validations as needed.

5.4 NOTIFICATION

5.4.1 OVERVIEW

1. After threat information is validated, initial threat information is immediately disseminated to relevant partner agencies. Dissemination methods and recipients will depend on the specific threat information as well as potential impacts.

2. The recipients of intelligence notifications are situation dependent. Notifications may be immediate or may take time depending on the situation. It is important that information is shared in a way that delivers crucial messages but does not escalate public fear.

3. Threat reporting is not standardized; rather, it is at the discretion of OHS and the fusion center to identify recipients of a potential threat or intelligence information.

4. All state-level threats are communicated to the Director of Emergency Management, or Adjutant General, and the Governor, who will then decide processes for statewide dissemination.

5. Terrorism events, like all disasters, start and end at the local level. Recipients of threat notifications or intelligence must include County Warning Points (CWPs) and local Emergency Operations Centers (EOCs) to ensure operational readiness. Should a potential threat escalate past the county level, the local EOC will notify the SEOC for activation.

6. Reference the statewide terrorism response checklist as a playbook.

7. At the time of a tangible threat, the Fusion Center will set up an HSIN room to coordinate information needs. The HSFC, under the direction of OHS, will grant permissions based on the threat and will include relevant partners such as:

    a. Other fusion centers.

    b. OHS.

    c. County partners.

8. WebEOC will be used for tracking information that can be broadly disseminated, while sensitive information is managed through HSIN.

    a. WebEOC is accessible only during an EOC activation and may not be available for potential threats that have not yet occurred.

    b. HSIN is a secure platform with a specified audience and can be accessed at any time after the creation of a secure room.

5.4.2 KEY AGENCIES

1. The SWP is the communication warning center for the state. The SWP may be notified of an actualized threat via the National Warning System (NAWAS) and should be updated on the situation for record-keeping for anything beyond normal operational activities.

2. After notification, SWP is responsible for sharing disseminated information with relevant state partners, including HI-EMA and OHS leadership for activation and coordination via the Hawaii Warning System (HAWAS). HAWAS is used to transmit and receive emergency messages from the local EOC and CWPs.

3. Additional horizontal information sharing through OHS may include agencies such as (depending on the identified threat or specific situation):

    a. HI-EMA.

    b. National Guard.

    c. State military outposts.

4. Vertical information sharing through OHS may include (depending on the identified threat):

    a. Governor.

    b. Director of Emergency Management.

    c. FBI.

    d. DHS, including Homeland Security Investigations and Cybersecurity and Infrastructure Security Agency.

    e. National Intelligence Council.

    f. Other federal partners as necessary.

5. Any intelligence shared with the Governor must also be shared with the federal National Intelligence Council, which maintains continuous monitoring of potential and actualized threats.

5.4.3 SYSTEMS/NOTIFICATION TOOLS

1. Systems that can be utilized to share information about a potential or actualized threat include:

    a. Phone.

    b. Official paper or memo.

    c. Email.

    d. In-person meetings.

    e. Notification of Emergency Management Director or Governor for dissemination to critical partners.

2. The National Terrorism Advisory System (NTAS) issues alerts through state and local partners and the media directly to the public. NTAS utilizes the following channels to disseminate information:[19]

   a. The official DHS NTAS webpage.

   b. Email signup.

   c. Social media including Facebook and Twitter.

3. Providing state support in disseminating threat information from NTAS may include publishing information on official state websites and re-tweeting or re-posting information on social media.

---

[19] National Terrorism Advisory System, *NTAS Guide: National Terrorism Advisory System Public Guide*, April 2011. https://www.dhs.gov/xlibrary/assets/ntas/ntas-public-guide.pdf

6. COMMUNICATIONS

6.1 OVERVIEW

1. Deployment of communications resources shall be made to facilitate command and control in the field and augment communication with the County Emergency Operations Center (EOC).

2. SESF #2 – Communications will assist responders with local communications needs as well as establish and maintain communications with State, local, and federal agencies.

6.2 RESPONDER COMMUNICATIONS

1. To be compliant with ICS protocols, all communications will be in plain language and free of acronyms and abbreviations.

2. Hawaii maintains a statewide network that supports state and federal communications systems. Additionally, each county maintains its own disparate radio system for communications within its local jurisdiction.

6.2.1 911 AND DISPATCH

1. Public Safety Answering Point (PSAP) dispatch protocols are managed at the county level through County Warning Points (CWPs). PSAPS and CWPs are responsible for managing initial 911 calls for police, fire, and EMS.

2. The SWP is the designated hub to direct or redirect emergency communications to the appropriate organization. The SWP effectively operates as a state-wide 911 function by collecting information from various sources and distributing it to the necessary state-level leadership for situational awareness or decision points.

3. If an incident requires state support, the local EOC will notify the SEOC through SWP.

6.2.2 ON-SCENE COMMUNICATIONS

1. Incident command/unified command is responsible for all on-scene communications.

2. There are several radio systems throughout Hawaii, including both systems with a statewide footprint and others that are locally operated at the county level.[20]

---

[20] FEMA, *Hawaii Emergency Communications Annex to the Region IX Regional Emergency Communications Plan,* 2019.

3. The Anuenue Interisland Digital Microwave Network is a statewide system that supports first responders, search and rescue, law enforcement, emergency services, and critical government throughout the Hawaiian Islands.

   a. Each county and several state agencies are equipped with a Transportable Repeater Interoperable Communications (TRIC) unit programmed with the respective regional and national shared channels to provide interim communications during the on-scene response.

4. State response radio channels are available on local response radios to provide interoperability among responding organizations. Specifics of tactical interoperable communications can be seen in SESF #2 Communications (Attachment 1: Emergency Communications Appendix), the State and Regional Tactical Interoperable Communications Plan (TICP), individual county-level TICPs, and the Hawaii Emergency Communications Annex to the FEMA Region IX Regional Emergency Communications Plan.

5. In addition to interoperable radios, the state maintains a cache of satellite phones and iPads to augment on-scene communications as necessary.

6. The Statewide Interoperability Coordinator (SWIC) should be familiar with and aware of all communications equipment utilized in the response.

6.2.3 SUPPORT AGENCY COMMUNICATIONS

1. Both the SEOC and local EOCs communicate using public and VoIP telephone and via government-supplied data networks, such as WebEOC.

2. The SEOC is equipped with multiple redundant communication networks comprised of local, state, and federal emergency communication systems.

3. Each county EOC has a state-supplied satellite data system to provide backup communications during emergency response.

4. The HSFC uses traditional communications and has no redundant methods of communications. The HSFC often uses the Homeland Security Information Network (HSIN) Situation Rooms in response to and preparation for planned events and can access secure voice data capabilities through relationships with the FBI and other federal partners.

5. Federal partners maintain radio networks throughout Hawaii that can be utilized to support tactical-level response communications.[21] These systems' availability is reliant on an emergency declaration or other National recognition of DoD support to the State prior to activation.

   a. FEMA has established a small communications cache on Oahu that can provide continuity communications and tactical-level communications.

---

[21] Ibid.

b. DHS operates a multi-site radio network with a statewide footprint to support tactical disaster communications.

c. U.S. Indo-Pacific Command owns an encrypted radio network with sites on Oahu, Maui, Kauai, and the Big Island, which can be utilized in support of a terrorism or targeted violence incident.

d. U.S. Coast Guard (USCG) maintains a maritime distress radio system that uses 10 Anuenue Interisland Digital Microwave Network radio links which can be utilized in support of a terrorism or targeted violence incident.

6.3 JOINT INFORMATION SYSTEM (JIS)/JOINT INFORMATION CENTER (JIC)

1. The lead jurisdiction's Public Information Officer (PIO) will provide official public information on behalf of the state. Other state and local PIOs will support the lead PIO as requested.

2. Depending upon the circumstances, senior state officials may become the designated spokesperson(s) to provide routine updates to the public.

3. Should it be necessary, a Joint Information System (JIS) will be activated and staffed by agency PIOs. The JIS provides the mechanism to organize, integrate, and coordinate information to ensure timely, accurate, accessible, and consistent messaging across multiple jurisdictions and/or disciplines, including the public, private sector, and NGOs.

4. Key responsibilities of the JIS include but are not limited to:

    a. Gathering, verifying, coordinating, and disseminating consistent, unified messaging.

    b. Managing rumor control.

    c. Providing support for decision-makers.

    d. Hosting briefings or special events.

    e. Managing public inquiries.

5. Individual agencies may still release their own messages in accordance with specific policies and procedures after crafting and verifying the unified message through the JIS.

6. To ensure coordination of public information during incidents that involve multiple agencies or jurisdictions, the Incident Commander may choose to establish and staff a Joint Information Center (JIC) with agency PIOs. A JIC is a central location that facilitates operations of the JIS.

7. In all JIC operations, the staff reports to the Lead PIO, who may delegate responsibility for specific functions to an assistant or JIC staff member.

8. The JIC may be a physical location near the incident site or hosted virtually through WebEOC or other communication platforms.

6.3.1 KEY AGENCIES

1. When a JIS or JIC is activated, it is staffed by PIOs from responding agencies. A JIC may also include agencies such as:

   a. Local law enforcement.

   b. Local fire departments.

   c. Local emergency management agencies/EOCs.

   d. Local and state officials.

   e. Homeland security officials.

   f. Federal officials.

   g. Non-governmental organization (NGO) representatives.

   h. Private sector representatives.

6.4 PUBLIC ALERT AND WARNING

1. When threat information must be communicated to the public to prevent future damage or loss of life, local warning systems will be activated.

2. Initial public information will be the responsibility of the local law enforcement agency or the local jurisdiction and is shared by other entities as appropriate.

3. Initial immediate information released will focus on public safety needs and may be limited in nature. Secondary messages may provide additional details and clarity of the incident and expected public actions; however, all information will be released on a limited "need-to-know" basis.

4. The Office of the Governor may wish to manage all public information releases.

5. Public information and warning include a network of systems that should be enacted in coordination to ensure information is widely disseminated. Any of the following systems may be utilized to widely disseminate safety information to the public.

   a. Activation of the Emergency Alert System (EAS) to disseminate urgent information.

   b. Activation of Wireless Emergency Alerts (WEA) in areas directly adjacent to a threat with direct safety information.

    c.   Activation of the WEA in a wider area with more generalized information.

    d.   Activation of the National Warning System (NAWAS) or Hawaii Warning System (HAWAS) to distribute telephonic warnings or alerts.

    e.   Activation of the statewide Outdoor Warning System (sirens).

    f.   Activation of a public mass communications platform such as Everbridge or Nixle.

    g.   Activation of internal notification systems such as the Hawaii Department of Education parent notification systems.

6. Additional public notification methods may include:

    a.   Activating call response centers in the EOC or SEOC.

    b.   Traditional media including regional television and radio stations.

    c.   Official website updates and social media posts.

    d.   Subscription-based public mass notification alerts.

    e.   Community meetings and town halls.

7. A JIC may be established to collect and disseminate warning and general information. The JIC will be conducted in support of the local jurisdiction.

8. State PIOs should be made available to support local messaging, either through the JIC or the local jurisdiction. State PIOs should amplify locally generated messaging focusing on safety or factual information.

9. During a statewide emergency or major event, SESF #15 at the SEOC will coordinate messaging from all the affected counties and provide one consistent unified message to the press and public.

10. Modern public notification must include some social media planning and monitoring. The state has access to Virtual Operations Support Teams (VOST) to support social media monitoring and management during a crisis. To activate a VOST, the local EOC should submit a request for assistance to the SEOC.

This page intentionally left blank.

7. PLAN DEVELOPMENT AND MAINTENANCE

7.1 RESPONSIBILITIES FOR ANNEX DEVELOPMENT AND MAINTENANCE

1. Under the Hawaii Revised Statutes, Title 10, Chapter 128A, OHS is responsible for preparing comprehensive plans for homeland security and defense that ingrate with related plans at all levels of government. This Annex falls under that mandate.

2. The Terrorism and Targeted Violence Annex was developed with input from:

    a. OHS.

    b. HI-EMA.

3. OHS is responsible for coordinating all revisions of the Terrorism and Targeted Violence Annex. Plan maintenance responsibilities include:

    a. Maintaining a plan review cycle as described in the next section.

    b. Reviewing all plan components and proposed changes for accuracy and consistency.

    c. Obtaining approvals for any changes that directly impact any agency other than OHS.

    d. Ensuring notifications of approved changes are made and maintaining a record of changes.

    e. Submitting all revisions to HI-EMA, which has overall responsibility for the HI-EOP Basic Plan, to which this document is an annex.

4. All plan updates must be approved by the OHS Administrator.

7.2 REVIEW CYCLE

7.2.1 REGULAR REVIEW

1. OHS will complete periodic updates to the Terrorism and Targeted Violence Annex no less than every year. Along with the same guidance as for the review of the HI-EOP Basic Plan, regular updates are likely to include any of the following:

    a. Minor administrative revisions needed to update terminology, titles, or agency names.

    b. Changes to the current realities of risk and vulnerability analyses, planning assumptions, and the overall homeland security situation.

    c. Additions of relevant case studies as they occur throughout Hawaii, the U.S., and worldwide.

d. Changes in federal or state laws, policies, structures, capabilities, or other changes to emergency management standards or best practices.

e. Incorporate substantive lessons learned from exercises, incident analysis, or program evaluations.

2. OHS will document any regular review of the Terrorism and Targeted Violence Annex as part of the record of changes, even if no changes are made to the document as a result of the review. In such cases, OHS will note in the record of changes the date of the review and that all information was validated as remaining accurate and current.

7.2.2 OFF-SCHEDULE REVIEW

1. In addition to the regular review cycle, OHS commits to reviewing the Terrorism and Targeted Violence Plan regularly. OHS will be responsible for identifying when an update is warranted. It is recommended that the considerations for updating the plan should be made after:

a. Any real-world incident that activates the plan.

b. Any exercise that uses or references the plan.

c. As a part of the annual plans review.

7.2.3 REVIEW AGENCIES

1. In addition to OHS, the following agencies should be involved in the review of the Terrorism and Targeted Violence Annex:

a. HI-EMA.

b. Office of the Governor.

c. DPS.

d. National Guard.

e. SESF lead agencies.

f. HTA.

g. County partners including local emergency management agencies, police, and fire departments.

h. Other governments and NGOs that are listed with responsibilities in this Annex.

2. Federal partners, including the FBI, FEMA, DHS, and DOD, should be made aware of any revisions or changes to this Annex.

3. It is recommended that County partners host a collaborative Annex review with emergency management, police, and fire departments.

7.3 CAPABILITY MAINTENANCE

1. Maintaining and growing the capabilities described in this Terrorism and Targeted Violence Annex is a priority for OHS.

2. OHS facilitates capability maintenance and growth by providing training and exercise opportunities to agencies identified in this Annex, as well as by participating in training and exercise opportunities sponsored by other organizations.

7.3.1.1 TRAINING AND EXERCISE PROGRAM DEVELOPMENT AND IMPLEMENTATION

1. Training and exercise of the Terrorism and Targeted Violence Annex will be integrated with and conducted as part of the statewide training and exercise program, which is compliant with the requirements of the Homeland Security Exercise and Evaluation Program (HSEEP).

2. The Terrorism and Targeted Violence Annex will be included in the Integrated Preparedness Planning Workshop (IPPW). The purpose of the IPPW is to identify and set training and exercise program priorities by compiling stakeholder training and exercise plans and soliciting leadership input. The IPPW also supports the coordination of statewide training and exercise schedules.

3. OHS will develop an annual training or exercise activity to test response capabilities as they relate to this document.

7.4 PLAN DISTRIBUTION AND ACCESS

1. The primary means of distribution for the Terrorism and Targeted Violence Annex will be electronic.

2. Portions of the Terrorism and Targeted Violence Annex deemed by the OHS and HI-EMA Administrators to be free of sensitive or confidential information will be publicly available online. Any version of this Annex containing sensitive information will be treated as a controlled document and hosted on the state's WebEOC system, where it will be accessible to State Emergency Response Team (SERT)[22] members, county emergency management agencies, and other state, local, and federal partners with access to the system.

---

[22] https://dod.hawaii.gov/hiema/files/2019/08/SERT-Member-Selection-and-Roles.pdf

3. Notifications of Annex revisions will be sent to:

   a. County emergency management agencies, police, and fire departments.

   b. State department directors.

   c. SERT members, which includes HI-EMA staff, EMOs, and SESF representatives.

   d. Federal response partners.

This page intentionally left blank.

8. AUTHORITIES AND REFERENCES

8.1 STATE LAWS, REGULATIONS, AND DIRECTIVES

1. Administrative Directive No. 15-01: *Emergency Management Preparedness Policies for Departments.*

2. 2017 Hawaii Revised Statutes. *Title 10. Chapter 127A: Emergency Management.*

3. 2017 Hawaii Revised Statutes. *Title 10. Chapter 128A: Homeland Security.*

8.2 FEDERAL LAWS, REGULATIONS, DIRECTIVES, AND REFERENCES

1. DHS. *Mass Attacks in Public Spaces.*

2. DHS. *Planning Considerations: Complex Coordinated Terrorist Attacks.*

3. DHS. *Strategic Framework for Countering Terrorism and Targeted Violence.*

4. FEMA. *National Response Framework: Terrorism Incident Law Enforcement and Investigation Annex.*

5. Homeland Security Presidential Directive (HSPD-7). *Critical Infrastructure, Prioritization, and Protection.*

6. Public Law 104-201. *Defense Against Weapons of Mass Destruction Act.*

8.3 OTHER REFERENCES

1. Crime Victims Compensation Commission, *Mass Violence Victim Response Plan.*

2. DHS, *Planning Considerations: Complex Coordinated Terrorist Attacks*, July 2018.

3. DHS, *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019.

4. FBI, *Active Shooter Incidents in the United States in 2019*, April 2020.

5. FBI, *Active Shooter Resources.*

6. FBI, *Countering Violence Extremism.*

7. FBI. *Quick Look Active Shooter Incidents.*

8. Economic Research Organization at the University of Hawai'i, *How to Control Hawaii's Coronavirus Epidemic and Bring Back the Economy: The Next Steps,* April 2020.

9. EMA, *Emergency Management Institute Glossary.*

10. FEMA, *Basic Guidance for Public Information Officers, 2015.*

11. FEMA, *Emergency Management Institute Glossary.*

12. FEMA, *Hawaii Emergency Communications Annex to the Region IX Regional Emergency Communications Plan,* 2019.

13. FEMA, *Ready.gov.*

14. FEMA, *THIRA, and SPR Guide, 3rd Edition,* 2018.

15. GAO, *Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies,* December 2018.

16. Hawaii Public Radio, https://www.hawaiipublicradio.org/post/proud-boys-hawai-i#stream/0

17. National Fire Protection Association 3000. *Standard for an Active Shooter/Hostile Event Response (ASHER) Program.*

18. National Terrorism Advisory System, *NTAS Guide: National Terrorism Advisory System Public Guide*, April 2011.

19. Pew Research Center*, Social media outpaces print newspapers in the U.S. as a news source*, December 2018.

20. State of Hawaii DBEDT - *Research and Economic Analysis Division, Demographic, Social, Economic, and Housing Characteristics for Selected Race Groups in Hawaii*, March 2018.

21. Texas Department of Public Safety*, Texas Domestic Terrorism Threat Assessment*, January 2020.

22. University of South Florida, Emergency Management.

9. LIST OF ATTACHMENTS

Attachments are items that are built for and maintained with this Annex. Supporting documents are maintained separately—both by other agencies and potentially on a different review schedule than this Annex—but help convey the overall posture of terrorism and targeted violence preparedness in the State of Hawaii.

9.1 ATTACHMENTS TO THIS ANNEX

Attachment 1   Acronyms and Abbreviations

Attachment 2   Definitions

9.2 SUPPORTING DOCUMENTS

Hawaii Emergency Communications Annex to the Region IX Regional Emergency Communications Plan, 2019

Mass Violence Victim Response Plan, Crime Victim Compensation Commission, State of Hawaii, DRAFT November 2019

State Emergency Support Function #2, Communications, 2018

State Emergency Support Function #13, Public Safety and Security Annex, 2021

Visitor Coordination Annex, August 2019

Kauai Tactical Interoperable Communications Plan, August 2014

Maui Tactical Interoperable Communications Plan, August 2014

Oahu Tactical Interoperable Communications Plan, August 2014

Hawaii Tactical Interoperable Communications Plan, October 2010

This page intentionally left blank.

ATTACHMENT 1: ACRONYMS AND ABBREVIATIONS

This section contains acronyms and abbreviations related to the topics of terrorism and targeted violence. In some cases, the terms do not appear elsewhere in this Annex but are included here to facilitate an overall understanding of the terminology that might be used when discussing threats and incidents.

CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CCTA	Complex Coordinated Terrorist Attack
CDA	Civil Defense Agency
CERT	Community Emergency Response Teams
COP	Common Operating Picture
CPG	Comprehensive Preparedness Guide
CST	Civil Support Team
CVCC	Crime Victims Compensation Commission
CWP	County Warning Point
DHS	US Department of Homeland Security
DOC	Department Operations Center
DOD	US Department of Defense
DPS	Department of Public Safety
EMS	Emergency Medical Services
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FAC	Family Assistance Center
FEMA	Federal Emergency Management Agency
GAO	US Government Accountability Office
HAWAS	Hawaii Warning System
HAZMAT	Hazardous Materials
HI-EMA	Hawaii Emergency Management Agency
HI-EOP	Hawaii Emergency Operations Plan
HTA	Hawaii Tourism Authority
HPD	Honolulu Police Department
HSEEP	Homeland Security Exercise Evaluation Program
HSFC	Hawaii State Fusion Center
HSIN	Homeland Security Information Network
IC	Incident Command
ICP	Incident Command Post
ICS	Incident Command System
IED	Improvised Explosive Device
IPPW	Integrated Preparedness Planning Workshop
ISIL	Islamic State of Iraq and Levant
JIC	Joint Information Center

JIS	Joint Information System
JFO	Joint Field Office
MCI	Mass Casualty Incident
NAWAS	National Warning System
NFPA	National Fire Protection Association
NGO	Non-Governmental Organization
NRF	National Response Framework
NTAS	National Terrorism Advisory System
ODNI	US Office of the Director of National Intelligence
OHS	Hawaii Office of Homeland Security
PIO	Public Information Officer
PSAP	Public Safety Answering Point
SEOC	State Emergency Operations Center
SERT	State Emergency Response Team
SESF	State Emergency Support Function
SPR	Stakeholder Preparedness Review
SWIC	Statewide Interoperability Coordinator
SWP	State Warning Point
THIRA	Threat and Hazard Identification and Risk Assessment
TICP	Tactical Interoperable Communications Plan
TRIC	Transportable Repeater Interoperable Communications
UC	Unified Command
US	United States
USINDOPACOM	US Indo-Pacific Command
VIC	Victim Identification Center
VoIP	Voice Over Internet Protocol
VOST	Virtual Operations Support Teams
WEA	Wireless Emergency Alerts

ATTACHMENT 2: DEFINITIONS

This section contains definitions related to the topics of terrorism and targeted violence. In some cases, the terms do not appear elsewhere in this Annex but are included here to facilitate an overall understanding of the terminology that might be used when discussing threats and incidents.

Active Assailant	An active assailant is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, there is no pattern or method to their selection of victims. The event is unpredictable and evolves quickly.[23] An active assailant differs from an active shooter in that the perpetrator may be utilizing modes of attack other than firearms. An incident caused by an active assailant may be referred to as an act of **targeted violence, active violence, active attack, or active threat**.
Active Shooter	An individual actively engaged in killing or attempting to kill people in a confined and populated area[24]; in most cases, active shooters use firearms, and there is no pattern or method to their selection of victims.[25]
Biological Agents	Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of the material. Biological agents may be used as liquid droplets, aerosols, or dry powders.
Capability	Training that has prepared an individual to follow through on his or her intentions. The individual's capability also includes his or her educational training and skill set acquired through life experiences.
Chemical Agent	A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by the severity of effect: lethal, blister, and incapacitating.
Command and General Staff	The staff who report directly to the Incident Commander, including the Public Information Officer, Safety Officer, Liaison Officer, and other positions as required. They may have an assistant or assistants, as needed.
Complex Coordinated Terrorist Attack	Act of terrorism that involves synchronized and independent team(s) at multiple locations, sequentially or in close succession, initiated with little or no warning, and employing one or more weapon systems: firearms, explosives, fire as a weapon,

---

[23] University of South Florida, Emergency Management. https://www.usf.edu/administrative-services/emergency-management/hazards/active-shooter.aspx

[24] Federal Bureau of Investigation, *Active Shooter Resources.* https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources

[25] Federal Emergency Management Agency. https://www.ready.gov/sites/default/files/2020-03/active-shooter_information-sheet.pdf

	and other nontraditional attack methodologies that are intended to result in large numbers of casualties. [26]
Comprehensive Preparedness Guide (CPG) 101	A guide designed to assist jurisdictions with developing emergency operations plans. It promotes a common understanding of the fundamentals of planning and decision making to help emergency planners examine a hazard and produce integrated, coordinated, and synchronized plans.
Concept of Operations	A component of the basic plan that clarifies the school's overall approach to an emergency (i.e., what should happen, when, and at whose direction) and identifies specialized response teams and/or unique resources needed to respond to an incident.
Continuity of Operations Plan	A functional annex providing procedures to follow in the wake of an incident where the normal operations of the school are severely disrupted.
Critical Infrastructure	Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Cyber Attack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Cyber Terrorism	Malicious conduct in cyberspace to commit or threaten to commit acts dangerous to human life, or against a nation's critical infrastructures, such as energy, transportation, or government operations in order to intimidate or coerce a government or civilian population, or any sequence thereof, in furtherance of political or social objectives.
Decontamination	The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.
Domestic Terrorism	Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.
Elevated Threat	A verified terrorist threat. An elevated threat alert warns the public and officials of a credible terrorist threat. [27]
Emergency Operations Center (EOC)	The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. [28]

---

[26] DHS, *Planning Considerations: Complex Coordinated Terrorist Attacks*, July 2018. https://www.fema.gov/media-library-data/1532550673102-c4846f270150682decbda99b37524ca6/Planning_Considerations-Complex_Coordinated_Terrorist_Attacks.pdf

[27] National Terrorism Advisory System (NTAS), 2011. https://www.dhs.gov/national-terrorism-advisory-system

[28] FEMA, *Emergency Management Institute Glossary*. https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm#:~:text=Unified%20Command%20(UC)%3A%20In,responsibilities%20to%20work%20together%20effectively

Emergency Operations Plan	An ongoing plan for responding to a wide variety of potential hazards. An EOP describes how people and property will be protected; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available; and outlines how all actions will be coordinated.
Emergency Support Functions	ESFs provide the structure for coordinating federal interagency support for a federal response to an incident. they are mechanisms for grouping functions most frequently used to provide federal support to states and federal-to-federal support, both for declared disasters and emergencies under the Stafford Act and for non-Stafford Act incidents.
Emerging Threat	As defined by the U.S. Government Accountability Office (GAO), long-range emerging threats to the U.S. include adversaries' political and military advancements, dual-use technologies, weapons, and events and demographic changes. Please see the full GAO report for further threat identification and descriptions within these four categories. [29]
Evacuation	The organized, phased, and supervised withdrawal, dispersal, or removal of students, personnel, and visitors from dangerous or potentially dangerous areas.
Exercise	An instrument to train for, assess, practice, and improve performance in *prevention, protection, response,* and *recovery capabilities* in a risk-free environment. Exercises can be used for: testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement. Note: Exercises are also an excellent way to demonstrate school resolve to prepare for disastrous events.
Imminent Threat	An imminent threat warns of a verified, credible, specific, and impending terrorist threat. [30]
Incident Command	The Incident Command System (ICS) organizational element responsible for the overall management of the incident and consisting of the Incident Commander (either single or unified command structure) and any assigned supporting staff.[31]
Integrated Response	A coordinated emergency management strategy that integrates law enforcement, fire, tele-communicator, and emergency medical services (EMS) in an active threat incident to stop the killing by neutralizing the threat and saving lives.

---

[29] U.S. Government Accountability Office (GAO), *Long Range Emerging Threats Facing the United States as Identified by Federal Agencies,* December 2018. https://www.gao.gov/assets/700/695981.pdf
[30] NTAS, 2011. https://www.dhs.gov/national-terrorism-advisory-system
[31] FEMA, *Emergency Management Institute Glossary.* https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm#:~:text=Unified%20Command%20(UC)%3A%20In,responsibilities%20to%20work%20together%20effectively

Fusion Center	Defined as a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing the ability to detect, prevent, investigate, and respond to criminal and terrorism activity.
General Staff	A group of incident management personnel organized according to function and reporting to the Incident Commander. The General Staff normally consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief. An Intelligence/Investigations Chief may be established, if required, to meet incident management needs.
Hazardous Material(s)	Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.
International Terrorism	Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).
Joint Information Center (JIC)	A facility established to coordinate critical emergency information, crisis communications, and public affairs functions. The Joint Information Center is the central point of contact for all news media. The Public Information Officer may activate the JIC to better manage external communication. [32]
Joint Information System (JIS)	A structure that integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely, and complete information during crisis or incident operations. The mission of the Joint Information System is to provide a structure and system for developing and delivering coordinated interagency messages; developing, recommending, and executing public information plans and strategies on behalf of the Incident Commander (IC); advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort. [33]
Joint Terrorism Task Force	Serve as the coordinated "action arms" for federal, state, and local government response to terrorism threats in specific US geographic regions. The FBI is the lead agency that oversees JTTFs.
Lone Offender/Lone Wolf	Terrorist threats have evolved from large-group conspiracies toward lone-offender attacks. These individuals often radicalize online and mobilize to violence quickly. Without a clear group affiliation or guidance, lone offenders are challenging to identify, investigate, and disrupt. The FBI relies on partnerships and tips from the public to identify and thwart these attacks.

[32] FEMA, *Basic Guidance for Public Information Officers, 2015.* https://www.fema.gov/media-library-data/20130726-1623-20490-0276/basic_guidance_for_pios_final_draft_12_06_07.pdf
[33] Ibid.

National Response Framework	A guide establishing a comprehensive, national, all-hazards approach to domestic incident response. It intends to capture specific authorities and best practices for managing incidents ranging from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters.
Preparedness	A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response. Within the National Incident Management System (NIMS), preparedness focuses on the following elements: planning, procedures and protocols, training and exercises, personnel qualification and certification, and equipment certification. Examples: Conducting drills, preparing homework packages to allow continuity of learning if school closures are necessary, etc.
Prevention	Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. Examples include cyberbullying prevention, pandemic influenza sanitation measures, building access control procedures, security systems, and cameras, etc.
Recovery	Encompasses both short-term and long-term efforts for the rebuilding and revitalization of affected communities. Examples: Short-term recovery focuses on crisis counseling and restoration of lifelines such as water and electric supply and critical facilities. Long-term recovery includes more permanent rebuilding.
Response	Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population.
State Emergency Operations Center (SEOC)	The physical location at which the coordination of information and resources to support state incident management (on-scene operations) activities take place.
State Emergency Response Team (SERT)	The team of people assigned to support emergency preparedness and response efforts that includes HI-EMA staff, Emergency Management Officers (EMOs) and State Emergency Support Functions (SESFs) to include: Ensuring all departments have identified a primary, secondary and tertiary Emergency Management Officer (EMO) to serve as the liaison between their agency and HI-EMA and Assigning appropriate agencies to SESFs. [34]
Targeted Violence	Any incident of violence that implicates homeland security activities and in which a known or knowable attacker selects a particular target prior to the violent attack. [35]
Terrorism	Any activity involving a criminally unlawful act that is dangerous to human life or potentially destructive of critical infrastructure or key resources, that appears intended to intimidate or coerce a civilian population; to influence government

---

[34] HI-EMA, *State of Hawaii Emergency Operations Plan,* November 2019. https://dod.hawaii.gov/hiema/files/2020/02/Hawaii-State-EOP-Fall-2019-Published.pdf

[35] DHS, *Strategic Framework for Countering Terrorism and Targeted Violence,* September 2019. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

	policy by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping.[36]
Unified Command	In incidents involving multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement, unified command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.[37]
Violent Extremism	Encouraging, condoning, justifying, or supporting the commission of a violent act to achieve political, ideological, religious, social, or economic goals.[38]

---

[36] Ibid.
[37] FEMA, *Emergency Management Institute Glossary.*
https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm#:~:text=Unified%20Command%20(UC)%3A%20In,responsibilities%20to%20work%20together%20effectively
[38] Federal Bureau of Investigation (FBI). https://cve.fbi.gov/whatis/