Emergency Management Division
Unmanned Aerial Systems (UAS)
Threats and Hazards Preparedness Framework

Contents

Promulgation & Signatories

This document is approved for implementation by the following authorities as of October 20, 2025. This plan supersedes all previous plans and directives.

Robert Ezelle

Director, Emergency Management Division

Washington Military Department

Record of Changes

Change Number: YR-XXX	Date of Change: MM/YYYY	Change Summary/Sections Affected

Introduction

Purpose

The Washington Emergency Management Division's (EMD) Unmanned Aerial Systems (UAS) Threats and Hazards Framework defines the operational-level strategies necessary to address the safety and security risks associated with hazardous UAS. This framework meets the purpose by documenting policies, responsibilities, procedures, personnel, equipment, and other capabilities necessary to respond to a UAS-related incident. These UAS hazard-specific considerations supplement the State's Comprehensive Emergency Management Plan (CEMP), State Emergency Operations Center (SEOC) Standard Operating Procedures (SOPs), and other established emergency response coordination structures. Note that this framework does not replace, replicate, or supersede the broader all-hazards approach to structuring a state response.

This framework's whole-of-government approach outlines a response structure that supports the development of local jurisdictions' capabilities and sustains public trust by strengthening the State's preparedness to counter potential UAS threats.

This plan provides specific considerations for coordinating a state response to UAS threats and incidents affecting organizations, infrastructure, and individuals within the State of Washington. It does not replace, replicate, or supersede the broader all-hazards approach to structuring a state response but does provide state leadership and responding organizations with hazard-specific information to effectively respond to UAS incidents within the emergency management context.

Scope

The UAS Threats and Hazards Preparedness Framework applies to all UAS incidents that are deemed significant (as defined below), including those that threaten public safety or impact critical infrastructure.

Washington State's CEMP supports all-hazards emergency management activities in the State, while this UAS threat specific framework addresses unique UAS threat-related activities. EMD is the coordinating agency for Washington State's whole-of-government efforts to address UAS-related hazards.

This framework does:

- Apply broadly to the threat of UAS and counter-UAS within Washington State.
- Identify response considerations for significant UAS-related incidents (see Definitions section).
- Identify unique SEOC activation considerations.

- Establish a flexible and scalable operational environment for addressing UAS-related risks.
- Provide guidance to state government agencies on how the state enterprise will organize itself to respond to a significant UAS-related incident.
- Align with roles, responsibilities, and response actions taken at the federal, tribal, and local levels of government.
- Provide a common foundation to support whole-of-government coordination.
- Leverage established incident management structures, such as the National Incident Management System (NIMS).

This framework does not:

- Develop security plans for specific locations, infrastructure, events, or activities.
- Direct critical infrastructure protection planning (though it may help inform such efforts).
- Discuss law enforcement actions of protection, prevention, and mitigation (law enforcement considers "mitigation" as acts against the UAS to disrupt the operator's control or destroy, all or part of, the system).
- Provide tactical-level response planning.
- Address UAS-related espionage.

Definitions

Unmanned Aircraft System (UAS): An unmanned aircraft system is an aircraft operated without the possibility of direct human intervention onboard combined with the associated elements required for safe and efficient operation. These elements may include control stations, communication links, support equipment, payloads, and launch or recovery systems (FAA, 49 U.S.C. § 44801).

Counter-Unmanned Aircraft System (cUAS): A counter-unmanned aircraft system refers to devices designed to detect, identify, monitor, and, when authorized by law, mitigate unmanned aircraft systems that pose a potential threat. These measures may include lawful means of disabling, disrupting, or seizing control of a UAS (FAA, 49 U.S.C. § 44801; DHS C-UAS Guidance).

Unidentified Anomalous Phenomena (UAP): Airborne objects that are not immediately identifiable; trans-medium objects or devices; and submerged objects or devices that are not immediately identifiable and that display behavior or performance characteristics suggesting that the objects or devices may be related to airborne or trans-medium objects or devices. (Per the NDAA FY23 Section 1673(d)(8).) DOD's All-domain Anomaly Resolution Office (AARO) considers UAPs as sources of anomalous detections in one or more domain (i.e., airborne, seaborne, spaceborne, and/or trans-medium that are not yet attributable to known actors and that demonstrate behaviors that sensors or observers do not readily understand).

Significant UAS-related incident: A distinguishable sized incident that necessitates a coordinated state response through SEOC activation and/or a Governor's Emergency Proclamation. Triggers of an activation or proclamation for a UAS-related incident include a mass casualty incident (MCI), a significant public safety concern, critical infrastructure service disruptions, or leadership's discretion. See the Washington Response Plan (WRP) for details on SEOC activation.

UAS-related incident of concern: Does not meet the "significant" threshold of SEOC activation or Governor's proclamation but still requires subject matter expertise beyond the capabilities of first responders, local jurisdictions, or state agencies.

Situation Overview

The threat landscape associated with UAS is continuously evolving. While the increasing use of UAS across various applications establishes this technology as a routine part of daily life, these advancements introduce new risks, including the potential for hazardous or malicious applications of UAS. In addition to the rise in criminal applications of UAS, there is an escalating threat of weaponization associated with terrorism and nation-state military technologies. UAS threats are, and will intensify, risks to large events, critical infrastructure, and government functions as these remain prime targets for adversaries seeking to incite terror, undermine the economy, or compromise vital systems. Alongside these physical concerns, there is also a cyber element. Weaknesses in GPS navigation or remote-control software could be taken advantage of by a hostile actor, giving them the ability to interfere with or even seize control of a drone in flight. If successful, this type of attack could disrupt emergency operations, compromise aviation safety, or cause problems for other systems that rely on wireless and satellite signals.

Public safety professionals must implement preparedness measures, such as counter-UAS training, public messaging, and risk assessments, to address potential hazards and elevated risks. Yet UAS threats remain difficult to counter due to civil rights protections, federal aviation restrictions, and the ease with which operators can evade law enforcement. While commercial mitigation tools exist, only four federal agencies (DHS, DOJ, DOD, FAA) are currently authorized to employ them. (6 USC 124n: Protection of certain facilities and assets from unmanned aircraft). The rapidly evolving regulatory environment further complicates access to counter-UAS options. FAA regulations over the air domain mean that the use of countermeasures against a UAS (even for "self-defense") is not currently an authority the state or locals can exercise outside of federal coordination. Policy-based countermeasures, such as flight rules, temporary flight restrictions (TFRs), and notices to airmen (NOTAMs), all rely on voluntary compliance. Low compliance, weak penalties, and enforcement challenges make policy-based countermeasures largely ineffective. As a result, threats persist despite the existence of laws and regulations.

Questionable UAS incursions or incidents occur regularly. Therefore, it is important to characterize incidents according to their scope and severity of impact. While a UAS attack on a single organization may be catastrophic for that entity, it may not necessitate a coordinated state response unless it generates (or has the potential to generate) impacts that require a governor's emergency proclamation.

Sources of UAS risk

Non-Malicious Incidents occur when an unintended action results in a significant UAS-related incident. Such incidents happen for numerous reasons, including:

- Human error;
- System malfunctions or failures; and

Operations arising from either unintentional or intentional disregard of laws and regulations, including deliberate but non-malicious violations (e.g., acts intended to draw attention or challenge authority rather than cause harm).

Malicious Incidents are caused by threat actors with the intent to commit a crime, inflict harm or damage, incite terror, or wage conflict. Perpetrators of malicious incidents include the following:

- Criminals – The use of UAS to commit crimes.
- Violent extremists – The weaponization of UAS to achieve ideological, political, or religious goals, encompassing advocating, preparing, and engaging in violent acts. This threat source may be communicated through a Bulletin or Alert from the National Terrorist Advisory System (NTAS)
- Nation-state actors – Sponsored or directed by a government to conduct an attack. This may pose a threat to U.S. national security, potentially resulting in armed conflict and the threat of military-grade systems.

Unidentified Anomalous Phenomena (UAP) is a unique UAS-related risk in that the presence or thought of a UAS can incite public safety concerns, panic, or fear that harm may be intended.

It is important to note that consequence management, the aspect of emergency management that focuses on responding to an incident, remains the same regardless of the hazard or delivery method. This aligns with the framework outlined in the Washington State Significant Cyber Incident Response Plan, which can provide guidance on incident management and partner coordination when cyber-enabled UAS threats occur. **Recommendation:** Establish performance measures and evaluation criteria aligned with the **Homeland Security Exercise and Evaluation Program (HSEEP)**. Using HSEEP tools—such as Exercise Evaluation Guides (EEGs), After-Action Reports (AARs), and Improvement Plans (IPs)—would provide a consistent method to evaluate UAS preparedness and response. Integrating these tools into post-incident reviews and training cycles will support continuous improvement and accountability across agencies.

Examples of UAS Threats

The following examples represent a continuum of potential UAS threats—ranging from clearly defined and immediate risks to those that are uncertain or under investigation:

- Confirmed threat of an attack on a specific location or event;
- Hostile Surveillance – The use of surveillance capabilities that pose a threat to public safety, individual rights, critical infrastructure, or economy;
- Confirmed existence of a UAP – Authorities have acknowledged an unknown technology that could be a threat but cannot yet determine what it is; and
- Unconfirmed UAP – The reports of an abnormality are irregular, inconstant, or lacking reputable sources.

Concept of Operational Framework

The State's role in addressing UAS threats depends on local jurisdiction's varying capacities to manage complex incidents. In general, the State will function as a coordinating entity for state and federal resources to facilitate relationships between jurisdictions, state agencies, and private organizations.

As with any disaster, the SEOC serves as a central coordination point. The SEOC facilitates resource requests, coordinates with local, tribal, and federal governments, and coordinates a Joint Information System (JIS) to ensure unified messaging. Participation in SEOC operations can occur in person or virtually, depending on the nature of the incident and the requirements necessary to meet the activation and operational period goals. During a significant UAS-related incident, the SEOC can coordinate the State's response efforts and act as a conduit between the affected jurisdictions and the federal government. The SEOC will be primarily concerned with:

- Identifying and responding to any consequences resulting from the significant UAS-related incident.
- Coordinating information sharing and threat intelligence between impacted entities and the federal government.
- Facilitating resource requests and fulfillment to affected entities; and
- Centralizing and disseminating information through a JIS

State-level coordination of significant UAS-related incidents is triggered when the SEOC activates following a request for assistance related to the incident, at the mandate of a governor's emergency proclamation, or based on other triggers as defined in the SEOC SOPs. At that point, the significant UAS-related incident will be monitored and coordinated through the SEOC under the guidance of the Unified Coordination Group (UCG).

Unified Coordination Group (UCG): The UCG functions as a multiagency coordination entity (as defined by the NIMS) and works to establish joint priorities (single or multiple incidents) and allocate resources, resolve agency policy issues, and provide strategic guidance to support

incident management activities. The UCG is comprised of senior leaders representing significant jurisdictional responsibility, financial or resource commitment, and relevant functional authority depending on the scope of the incident. The UCG provides strategic guidance and initial resolution to any conflicts in priorities for allocation of critical resources. If policy issue resolution cannot be achieved among UCG members, issues can be raised to the Policy Group. Based on the incident priorities and policy direction provided by the Policy Group, the UCG, in coordination with SEOC Command and General Staff, sets operational objectives for the SEOC.

Policy Group: The State Policy Group is comprised of cabinet level executives and subject matter experts who provide high level strategic and policy guidance to support the incident. The Policy Group provides incident priorities and policy direction to the UCG, supports prioritization and allocation of resources, and enables decision-making among elected and appointed officials and senior executives.

Washington's SEOC Emergency Support Functions (ESFs) streamline the mobilization of essential resources and expertise to address specific needs. The ESFs activated will depend on the specific impacts of an incident. During a UAS-related incident, the ESFs anticipated to be the focus of operations are ESF 13 – Public Safety, Law Enforcement, and Security, and ESF 15 – External Affairs.

ESF 13 – Public Safety, Law Enforcement, and Security: Coordinates with local jurisdictions and federal authorities to design and implement unique actions to prevent, protect, and mitigate a UAS hazard. The scope of responsibility of ESF 13 includes facility and resource security, security planning and technical resource assistance, and public safety and security support.

ESF 15 – External Affairs: The core purpose of ESF 15, "to communicate accurate, accessible, and timely information to the public and various stakeholders during emergencies and declared disasters for external affairs," remains unchanged during a UAS-related incident. However, the unique aspects of a UAS-related incident may necessitate a hazard-specific public messaging plan. (See Annex A)

State Emergency Operations Center (SEOC)

The SEOC is the primary platform for coordinating operational response activities for issues arising due to a significant UAS-related incident including incident prioritization, critical resource allocation, and shared situational awareness. This coordination includes communicating UAS incident situational awareness and related activities to SEOC partners, the Governor's office, private sector partners, and local, tribal, and federal coordination centers. The SEOC maintains the capability to physically or virtually add federal, state, local, tribal, territorial, and private sector partners, including international stakeholders as appropriate, to the coordinated SEOC effort. Initial activation and the organizational structure for the SEOC will follow the guidance provided by the WRP.

SEOC Activation during a UAS-related Incident

Responding to a significant UAS-related incident involves a timely, coordinated effort across state government to prioritize resources, minimize impacts, and set conditions for a timely recovery. The Emergency Management Division may partially or fully activate the SEOC to coordinate and manage response efforts. The SEOC provides a central location for state agencies to coordinate the State's response with federal, tribal, local, and private sector organizations that are impacted by the incident or are contributing to response operations.

Because of the unique nature of UAS incidents, the SEOC may need to involve organizations and individuals not typically engaged in other hazard activations such as subject matter experts (SMEs) and agency representatives such as the FAA, FBI, U.S. Marshals, and private industry representatives. These additional personnel may be organized within the Policy Group, Unified Command Group, SEOC Command and General Staff, or an Emergency Support Function (ESF). Examples of significant UAS-related incidents that may trigger state-level coordination include those that pose an imminent threat to critical infrastructure services, government stability, or the lives of residents or those that are likely to create significant impacts to public health or safety, national security, economic security, foreign relations, or civil liberties. The severity of an incident may depend on the scope and scale of the incident, as well as the potential for cascading impacts. The following table provides decision makers with factors to consider in determining the State's initial response level. Note that the SEOC may alter its initial activation level based on the evolving situation, including its complexity, impacts and other factors, especially if the UAS incident is occurring simultaneously with other incidents.

The SEOC may increase activation levels in response to several types of incidents. These include major disasters or emergencies, or situations in which state, local, or tribal government agencies need assistance. An increase may also be triggered when multiagency coordination is needed to address complex problems.

The need for extensive joint emergency planning and coordination may elevate the SEOC activation level. Indicators of this need include resource support for local governments, federally recognized tribes, or state agencies, critical infrastructure impacts (i.e., disruptions to power, roads, water, communication, or other essential systems), response to public safety threats, and major planned events (e.g., FIFA World Cup 2026). The activation level may also change due to the need for extensive joint emergency planning where coordination is essential.

Washington State Emergency Operations Center (SEOC) Activation Levels
Level 1 Full Activation

• Major Incident • In a Full Activation, all primary SEOC functions activate to support the incident or the impacted jurisdictions from the SEOC or JFO. Supplemental staffing may be utilized for the SEOC and ESFs as dictated by the incidents.
Level 2 Partial Activation
• Significant Event • When an incident exceeds the capability or capacity of the AWC or requires specialized incident support, the SEOC activates to a level 2 Partial Activation. In a Partial Activation, one or more of the SEOC functions activate to support the incident or the impacted jurisdictions from the SEOC or JFO. State agencies activate to fill SEOC positions and ESFs as dictated by the incident.
Level 3 Enhanced Monitoring Activation
• Routine Activation Level • The routine activation level in which state agencies conduct their daily emergency management responsibilities. The State Emergency Operations Officers (SEOOs) in the SEOC AWC manage and coordinate incidents in cooperation with local, state, and federal agencies. The AWC operates 24 hours a day, including weekends and holidays.
A detailed description of the SEOC activation process and phases or response can be found in the Washington State Emergency Management Response Plan

Vertical Integration

This framework vertically aligns with federal response structures at the national and regional level, as well as county and city plans at the local level. EMD accomplishes this through coordination with federal and local jurisdictions to provide counter-UAS capabilities and an aligned understanding of authorities and responsibilities.

The SEOC integrates information collected from all levels of government and maintains situational awareness through a common operating picture (COP). The COP enables federal entities to work from the same information as those at the local level.

Federal Integration: In accordance with The National Response Framework, response coordination with the federal government will occur through the FEMA Region 10 Regional Response Coordination Center (RRCC).

Local Integration: Local government UAS incident response structures and capabilities vary. In general, the State will coordinate with county Emergency Operations Centers (EOCs). Additional coordination may arise depending on the nature of the incident and the impacted entities. Local

jurisdictions responding to a "UAS incident of concern" can reference guidance materials from the DOJ, FAA, and DHS. (See Annex B Resources).

Horizontal Integration

This framework is a state-level interagency plan that provides direction to state government entities responsible for responding to a significant UAS-related incident and its potential consequences to citizens and physical infrastructure following a disaster. State agencies' planning efforts span pre-incident preparedness, response, and post-incident recovery. Horizontal integration in the context of a UAS response plan for an emergency management agency refers to the coordination and collaboration among various state agencies at the same level of government for effective response.

The SEOC horizontally integrates by cross-leveling resources among state agencies, gathering situational awareness, and leveraging agency-specific authorities to support a whole-of-government effort. Much of this coordination is through the state ESFs. For example, an essential action during a UAS related incident is ESF 15 – External Affair's timely synchronization of public messaging to prevent dissemination of conflicting information.

Tribal Government Integration

Tribal government UAS incident response structures and capabilities vary. If tribes choose, they may coordinate government-to-government with the State and/or federal agencies. The level of integration and coordination between the State and the involved tribe(s) depends on the nature of the incident, the entities impacted, and the level of support desired by the tribe(s). Tribal governments may also choose not to coordinate with the State in any capacity during a significant UAS-related incident.

Academia Integration

Academic institutions across Washington State represent a critical partner in the development, evaluation, and refinement of cUAS incident response strategies. Universities and research centers contribute subject matter expertise in emerging technologies, threat modeling, and policy analysis, and may support operational planning through simulation, data analytics, and risk assessment. During a significant UAS-related incident, academic partners may assist with post-incident evaluation, public communication strategies, and the development of evidence-based recommendations for future mitigation.

Private Sector Integration

Depending on the nature of a significant UAS-related incident, private sector organizations may be directly affected. Private corporations may integrate into statewide response when a significant UAS-related incident impacts the critical infrastructure they own/operate, the employment of a considerable number of Washington residents, if they are significant

contributors to the state's economy, or are crucial partners during any emergency response. The SEOC will coordinate response activities with impacted private sector entities to:

- Align response priorities; and
- Share information and resources.

This coordination may occur through the policy group, UCG, or the relevant (ESF), within the State's Business Emergency Operations Center (BEOC), and/or through a partner state or federal agency with a direct relationship to the affected business.

Governor's Emergency Proclamation

The governor may proclaim a state of emergency in the area affected by a significant UAS-related incident. A proclamation by the governor is a prerequisite for access to the full range of federal disaster recovery programs available to the state, as well as interstate mutual aid requests through the Emergency Management Assistance Compact (EMAC). Sources of governor's proclamation authority and to issue related orders are found in RCW Chapters 38.08, 38.52, and 43.06. An emergency proclamation provides a host of tools to help manage the incident, including:

- Deploying the National Guard and State Guard.
- Allowing emergency contracting and procurement.
- Prohibiting activities to help preserve and maintain life, health, property, or public peace.
- Waiving or suspending certain state laws, rules, and regulations to facilitate operations.
- Assistance to incident survivors, including state programs that provide support to specific subsections of the population.

A governor's proclamation is not required to activate the SEOC, coordinate response efforts, or utilize the interstate and international mutual aid agreement (Pacific Northwest Emergency Management Arrangement (PNEMA).

Additional details on the governor's proclamation process can be found in the WRP.

Requesting a Presidential Emergency or Major Disaster Declaration and Damage Assessments

Pursuant to Title 44, Code of Federal Regulations (CFR), Part 206, Subpart B, the governor may request the President of the United States issue an emergency or a major disaster declaration. Before making a request, the governor must proclaim a State of emergency and ensure all appropriate state and local actions have been taken.

To determine if a request for a disaster declaration is warranted, the Recovery Lead for ESF 21 – Recovery, if activated, works closely with the EMD Recovery Section to identify if the known incident impacts have met the state and local indicators that necessitate a joint FEMA-State

Agreement. This determination is made through the conduct of damage assessments on homes, businesses, and public infrastructure.

If the governor's request results in the President declaring an emergency or major disaster, the governor and the FEMA Regional Administrator will execute a FEMA-State Agreement that states the understandings, commitments, and conditions for federal assistance, and describes:

- The incident and incident period for which assistance will be made available.
- The areas eligible for federal assistance.
- The type and extent of federal assistance provided.
- The commitment of the state and local governments with respect to the amount of funds to be expended in alleviating damage and suffering caused by the major disaster or emergency.

With a Presidential Major Disaster Declaration, FEMA's Public Assistance (PA) grant program provides federal assistance grants to state, tribal, territorial, and local governments, and certain types of private nonprofit organizations so that communities can quickly respond to and recover from major disasters or emergencies. Additionally, Other Needs Assistance (ONA) awards are available under FEMA Individual Assistance (IA) to qualified individuals and families to meet serious, disaster-related needs and necessary expenses for which assistance from other federal, state, or voluntary agency disaster assistance programs is unavailable or inadequate.

Further details on the process for requesting a Presidential Disaster Declaration and PA and IA funding are outlined in the WRP.

UAS Threat Intelligence and Information Sharing

Timely access to accurate information is essential for managing UAS incidents. While some intelligence on malicious UAS activity originates from classified sources, much of the information needed for effective response and coordination can be shared through unclassified or appropriately sanitized channels. When feasible, it may be beneficial for personnel involved in strategic and operational UAS planning to hold security clearances to help integrate classified intelligence into training, planning, and operations. Additionally, these personnel should have ready access to a facility in which classified information can be stored, discussed, and accessed. Installing a sensitive compartmented information facility (SCIF) for the Emergency Management Division would close this capability gap. Closing intelligence gaps could require access through established channels such as the State Fusion Center, Joint Terrorism Task Forces (JTTFs), and federal partners.

During incidents, the priority is rapid sharing at the lowest classification level possible. Whenever practical, intelligence should be translated into unclassified advisories, situational updates, or technical guidance so all stakeholders, emergency managers, first responders, and infrastructure operators, have the awareness needed to protect the public and maintain continuity of operations.

The SEOC, UCG, and Policy Group utilize non-sensitive information channels to manage the response to a significant UAS-related incident. This includes:

- Information Sharing: Ensure timely dissemination of information to all relevant stakeholders, including public and private sector partners, to facilitate coordinate response efforts. Private sector engagement will occur through normal, previously established lines of communication through the ESF associated with/that covers the specific sector being impacted. For example, if wireless carrier coverage is disrupted by a UAS-related incident, direct engagement with the carriers will be carried out through ESF 2 – Communications.
- Operational Coordination: Use information to align and synchronize the actions of the SEOC, UCG, and Policy Group with on-the-ground response activities, ensuring a unified approach to incident management.
- Situational Awareness: Maintain a common operating picture by continuously updating relevant groups with the latest information about the incident's status, impacts, and response progress.
- Emergency Public Information: Develop and distribute clear, accurate, and consistent public messages to inform and guide the public, helping to mitigate panic, and provide instructions for safety.
- Resource Allocation: Utilize information to prioritize and allocate resources effectively, ensuring that the most critical needs are addressed promptly.
- Interagency Collaboration: Foster partnerships among various agencies by sharing information that can help identify collaborative opportunities and avoid duplication of efforts.

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a standardized framework for designing, conducting, and evaluating exercises that test preparedness and response capabilities. Using HSEEP ensures that exercises are consistent, repeatable, and measurable across all participating agencies. Key elements include Exercise Evaluation Guides (EEGs), After-Action Reports (AARs), and Improvement Plans (IPs), which collectively allow agencies to identify capability gaps, track progress, and prioritize corrective actions. By integrating HSEEP into UAS preparedness planning, Washington State can systematically assess the effectiveness of its training, interagency coordination, public messaging, and incident response, while fostering continuous improvement through lessons learned and documented improvements.

By following these procedures, the SEOC, UCG, and Policy Group can ensure an effective and coordinated response to significant UAS-related incidents, enhancing overall incident management and public communication.

Washington State Fusion Center (WSFC): The fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel,

training, technical assistance, exercise support, security clearances, and connectivity to federal systems. A fusion center plays a crucial role in UAS threat and risk assessment by serving as a centralized hub for collecting, analyzing, and disseminating information related to UAS. The WSFC is Washington State's single fusion center and concurrently supports federal, state, and tribal agencies, and regional and local law enforcement to maintain public safety and homeland security. The WSFC is a unified counterterrorism, "all crimes," fusion center, incorporating agencies with intelligence, critical infrastructure, public safety and preparedness, resiliency, response and recovery missions. WSFC provides information and updates on UAS and potential threats directly to all affected partners.

Public Messaging and Risk Communication

(See Annex A – Messaging for more information)

UAS and UAP incidents create special challenges for public communication. Their complexity and uncertainty often spark rumors and misinformation, which can heighten public concern and reduce trust in official updates.

To address this, the State uses the JIS to deliver accurate, timely, and clear information. Messaging will emphasize safety guidance, operational updates, and reassurance by sharing both confirmed and unknown details. Communication is coordinated with State, federal, local, tribal, and private partners, using pre-developed templates to ensure consistence and rapid release during an incident.

Authorities and Legal Framework

(See Annex C – Laws and Regulations for more details)

The management of UAS incidents takes place in a highly regulated environment. Federal law gives the FAA exclusive control of U.S. airspace, which limits what states and local jurisdictions can do on their own. Washington's emergency management responsibilities are defined in RCW 38.52, which guides coordination, response, and support to local partners. While only certain federal agencies are authorized to employ active counter-UAS measures, the State plays a critical role in preparedness, information sharing, public messaging, and consequence management.

Roles and Responsibilities

The possibility of a significant UAS-related incident occurring within the State of Washington is an ever-present threat, and effective planning and coordination activities that support unity of effort across the whole state government are essential. The ability to respond to UAS incidents is not the responsibility of any single office and requires collaboration across multiple state and local agencies.

Homeland Security Advisor (HSA)

The Adjutant General (TAG) of the Washington Military Department serves on the governor's cabinet and is the governor's Homeland Security Advisor (HSA). The HSA has responsibility for coordinating significant UAS-related incident related activities for the State of Washington.

Local Law Enforcement Coordination and Reporting

Local law enforcement plays a critical role in responding to reports of UAS activity. While the Federal Aviation Administration (FAA) regulates airspace, local officers are often the first to receive public reports and can enforce state and local laws related to privacy, trespassing, harassment, obstruction of emergency services, and other criminal activity.
When a concerning UAS incident is reported, local law enforcement should follow their jurisdiction's notification protocol, then notify and coordinate with the following entities as appropriate:

- FAA Law Enforcement Assistance Program (LEAP) – Western Regional Operations Center
    - Report unsafe UAS operations or suspected federal airspace violations.
- Washington State Fusion Center (WSFC)
    - Share information on suspicious or criminal UAS activity for statewide situational awareness.
- Local County Emergency Management
    - Contact the appropriate local emergency management agency for assistance, recommend state-level coordination with the SEOC, especially if the incident has broader public safety impacts or extends beyond jurisdictional lines.

This coordination ensures that UAS incidents are addressed within the appropriate jurisdictional authority, while enhancing information sharing between local, state, tribal, and federal partners.

Office of the Governor (GOV)

In accordance with RCW 38.52.030(2) and (3) and RCW 38.52.050, the governor provides overall direction and control for the preparation and carrying out of all emergency actions authorized under chapter 38.52 RCW, the Emergency Management Act, including development and carrying out of the State's comprehensive emergency management program. This includes preparation for and carrying out all emergency functions to mitigate, prepare for, respond to, and recover from emergencies and disasters from all hazards, whether natural, technological, or human caused, resulting from an event or set of circumstances that either (1) demand immediate action to preserve public health, protect life and public property, or to provide relief to any stricken community overtaken by such occurrences, or (2) have resulted in the governor proclaiming a state of emergency pursuant to RCW 43.06.010(12).
Under RCW 38.08.040, the governor is also authorized to activate the National Guard to perform such duty as deemed proper in the event of a public disaster; when required for public health, safety or welfare; or to prepare for or recover from such events.

Washington Military Department (MIL)

Emergency Management Department (EMD) The Director of EMD ensures the State is prepared to handle any disaster or emergency by administering the program for emergency management delineated by the HSA. The EMD Director is also responsible for coordinating the State's response in any disaster or emergency.

National Guard activation under Title 32 (United States Code) Under Title 32 (USC), the National Guard operates under the direction of its state chain of command but is funded by federal appropriations. Guard members serving in a Title 32 status can be requested to provide support to federal missions (such as Counter-UAS operations) subject to the approval of its state leadership as facilitated by the Joint Operations Center (JOC).

State Active Duty and State Guard (SAD) When activated under State Active Duty, the National Guard serves solely under state authority and funding. Personnel may be deployed to assist local or state response efforts, providing specialized expertise or operational support, as requested and coordinated through the JOC.

Washington State Department of Agriculture (WSDA)

The WSDA uses UAS to support its mission through activities such as aerial photography, pest tracking, site inspections, aerial mapping, sample collection, and 3D mapping. UAS operations are within FAA regulations and department policies.

Washington State Department of Commerce (COM)

During normal energy sector operations, owners/operators use UAS technology for various purposes, including major storm damage survey, line repair, substation/switching station and line inspections, power plant inspections, wind farm, gas pipeline inspections, and security. However, for malicious use cases, UAS can be utilized for hostile surveillance or pose direct threats to energy critical infrastructure.

Located within the Department of Commerce's Energy Division, the Energy Resilience and Emergency Management Office (EREMO) has the responsibility to prepare and update contingency plans for securing energy infrastructure against all hazard threats including physical and cybersecurity vulnerabilities, and for implementation in the event of energy shortages or emergencies. This office coordinates the state's Emergency Support Function (ESF) 12 – Energy which includes the electric, petroleum, natural gas, and alternative fuel sectors within the SEOC during state activations and is the primary coordinator for all energy infrastructure organizations within the state.

Washington State Department of Corrections (DOC)

Utilizes UAS for security, search, apprehension, and infrastructure inspections. UAS operations are within FAA regulations and department policies. Prisons are seeing an increase in the criminal use of UAS in attempts to introduce contraband.

Washington State Department of Enterprises (DES)

Although DES does not operate UAS as part of its mission, agency policy prohibits UAS use on the Capitol Campus except by law enforcement or first responders during an emergency, or with prior written approval from the DES Director for authorized campus care and maintenance purposes.

Washington State Department of Natural Resources (DNR)

DNR utilizes UAS on wildland firefighting incidents to provide reconnaissance, enhance situational awareness, and enable incident commanders to make the most efficient use of their resources. UAS operations are within FAA regulations and department policies.

Washington State Department of Transportation (WSDOT)

Employs UAS to conduct infrastructure inspections, project scoping, capture video and photographic imagery, assist in emergency response, and facilitate public engagement. UAS also supports a wide range of additional duties and responsibilities related to the management and preservation of WSDOT-owned and managed infrastructure. UAS operations are within FAA regulations and department policies.

Washington State Patrol (WSP)

The WSP utilizes UAS for a variety of applications related to public safety, including crime scene and collision scene mapping, tactical use for de-escalation and clearing buildings or spaces for officers, disaster recovery, and search and rescue. WSP's UAS operations are guided by FAA regulations, state, and internal policies. If a crime involves the use of this technology, WSP may take primary investigative role or support the jurisdiction with their investigation if needed.

Annexes

Annex A: Guidance for Public Messaging

Contents

Introduction

Unmanned Aircraft Systems (UAS) and Unidentified Anomalous Phenomena (UAP) present unique challenges that may not be addressed in all hazards messaging plans. This annex provides suggestions to use in conjunction with the WA state's CEMP and the Emergency Support Function (ESF) 15 External Affairs Annex.

Clear, consistent, and coordinated public messaging is essential to gain and maintain public trust and ensure safety during UAS-related incidents. Public Information Officers (PIOs) across state agencies and local jurisdictions play a critical role in delivering accurate information, correcting misinformation, and providing clear guidance to the public.

This annex provides statewide guidance for public messaging related to UAS incidents. It outlines responsibilities, principles, and a PIO Quick Reference to support local and state partners in communicating effectively during preparedness, response, and recovery activities. The Washington Emergency Management Division (WA EMD) serves as the coordinating entity for statewide UAS public messaging, ensuring alignment with federal partners and local jurisdictions.

Purpose

This annex provides guidance for consistent, coordinated public messaging related to UAS incidents in Washington state. The goal is to sustain public trust by ensuring that information released during preparedness, response, and recovery efforts is timely, accurate, and consistent across jurisdictions.

Scope

This annex can be used by all state agencies and local jurisdictions engaged in UAS-related operations. It addresses public messaging in preparedness, response, and recovery phases of incidents involving UAS, including potential counter-UAS (cUAS) actions authorized under state or federal law.

Roles and Responsibilities

Washington Emergency Management Division (WA EMD)

- In partnership with the Governor's communications office, coordinate statewide UAS public messaging during incidents.
- Ensure consistency with federal partners (FAA, DHS, FBI) and other state agencies.
- Provide templates, talking points, and messaging guidance to local jurisdictions.
- Compile statewide situational awareness on UAS incidents for distribution.

State Agencies and Local Jurisdictions

- Provide timely situational updates to WA EMD Joint Information Center (JIC)/Joint Information System (JIS) when activated.

- Use provided talking points and templates to ensure message consistency.
- Amplify WA EMD messaging through local communication channels.
- Engage community partners to reach priority populations.

Federal Partners (FAA, DHS, FBI, etc.)

- Provide technical information and federal-level public messaging guidance.
- Coordinate with WA EMD prior to release of incident-specific messaging when possible.

Messaging Principles

- **Accuracy First:** Release only confirmed information; avoid speculation.
- **Timeliness:** Provide early acknowledgment of incidents with updates as information develops.
- **Consistency:** Ensure alignment of state, local, and federal messaging.
- **Transparency:** Clearly communicate known risks and protective actions.
- **Reassurance:** Emphasize ongoing efforts by state and local agencies to safeguard the public.

Core Messaging Themes

Preparedness & Awareness

- Drones (UAS) are increasingly common and have many beneficial uses.
- Washington state has plans and partnerships in place to address UAS safety and security.
- The public plays a role in reporting suspicious or unsafe drone activity.

Incident Response

- Authorities are aware of the situation and are actively responding.
- There may be temporary disruptions (e.g., airspace restrictions, event security measures).
- Public safety is the top priority, and protective actions are being taken.

Public Safety Guidance

- Stay clear of incident areas and follow instructions from local officials.
- Do not attempt to interfere with UAS or suspected malicious activity.
- Report concerns about unsafe or suspicious drone operations to local law enforcement or the FAA hotline.

Recovery and Reassurance

- Emphasize restoration of normal operations as soon as possible.
- Share lessons learned and planned improvements for future preparedness.
- Reinforce continued coordination between state, local, and federal partners.

Communication Tools and Channels

- **Joint Information Center (JIC)/Joint Information System (JIS):** Central coordination platform for state and local messaging.
- **Press Releases and Media Briefings:** For major incidents or public safety advisories.
- **Social Media:** Rapid updates, rumor control, and amplification of official messages.
- **Websites and Alert Systems:** WA EMD and local jurisdiction platforms for situational updates.
- **Community Partners:** Trusted messengers (e.g., Tribal governments, local leaders, NGOs) to reach diverse populations.

PIO Quick Reference – UAS Incidents Washington State Emergency Management Division (WA EMD)

Immediate Priorities

■ Confirm facts before release.
■ Coordinate with WA EMD JIC (if activated).
■ Use approved templates/talking points.
■ Align with federal partners (FAA, DHS, FBI).
■ Do NOT speculate or release unverified info.

Core Messages

- Preparedness
  - Drones are widely used and often beneficial.
  - WA State has plans and partnerships to address UAS safety and security.
- Incident Response
  - Authorities are aware and actively responding.
  - Public safety is the top priority.
  - Temporary disruptions (airspace, events, travel) may occur.
- Public Guidance
  - Stay clear of the area.
  - Do not interfere with drones.
  - Report unsafe or suspicious activity to law enforcement or FAA hotline.
- Recovery / Reassurance
  - Normal operations will be restored quickly.
  - Lessons learned will strengthen future preparedness.

Topics to Avoid

- Operational Security (OPSEC) details
  - Do not describe detection capabilities (range, locations, or tools used).
  - Avoid discussing vulnerabilities or system limitations.
- Attribution and Speculation
  - Do not speculate on the intent, identity, or affiliations of a drone operator.
  - Do not confirm criminal or terrorist involvement until validated by law enforcement.

- Sensitive Law Enforcement/Federal Investigations
    - Do not share investigative details handled by FBI, FAA, DHS, or DoD.
    - Do not confirm surveillance or evidence collection techniques.
- Technical Specifications
    - Avoid detailed discussion of drone countermeasures, jamming capabilities, or interception methods.
    - Do not list brands/models of counter-UAS systems in use.
- Unverified Information
    - Do not release casualty figures, damage estimates, or disruption impacts until confirmed.
    - Avoid repeating rumors or circulating unverified images/videos.
- Overly Alarmist or Dismissive Tone
    - Do not exaggerate risks in ways that create panic.
    - Conversely, do not minimize credible threats that could undermine public trust.

Sample Holding Statement

"Authorities are aware of reports of drone activity near [location]. WA EMD is coordinating with local and federal partners to ensure public safety. Updates will be provided through official channels as more information becomes available."

Communication Channels

- WA EMD and local websites
- Social media (for rapid updates + rumor control)
- Press releases/media briefings
- Community partners/Tribal governments

Key Reminders

- Accuracy > speed
- Use plain language.
- Reassure: agencies are coordinating and prepared.
- Refer technical/legal questions to FAA or DHS as appropriate.

Point of Contact:

WA EMD Joint Information Center (JIC) – SEOC.PIO@mil.wa.gov

Annex B: Planning Resources

Documents

Cybersecurity and Infrastructure Administration (CISA):

- "Protect Critical Infrastructure and Public Gatherings"
- "Recognize Suspicious Unmanned Aircraft Systems (UAS)"
- "RESPONDING TO DRONE CALLS: Guidance for Emergency Communications Centers"

Department of Homeland Security (DHS):

- Counter-UAS Information
- National Terrorism Advisory System (NTAS)
- "Counter Unmanned Aircraft Systems Legal Authorities"
- "Safe Handling and Collection of Electronics (SHAKE) Factsheet"
- "Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges"

Federal Aviation Administration (FAA):

- "Drone Safety Day Playbook"
- "Public Safety Small Drone Playbook"
- UAS Operations

Federal Interagency:

- "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems"

U.S. Department of Justice (DOJ):

- "Community Policing & Unmanned Aircraft Systems (UAS) Guidelines to Enhance Community Trust"
- "Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program"
- "Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks"

U.S. House of Representatives. Subcommittee on Transportation and Maritime Security.

- "Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home"

U.S. Office of the Attorney General:

- "Guidance regarding "Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems"

Washington State

- Washington State Drone Laws
- WSDOT Unmanned Aircraft Systems

Professional Organizations

- Law Enforcement Drone Association (LEDA)

Annex C: Laws and Regulations

Federal

Presidential Executive Order: UNLEASHING AMERICAN DRONE DOMINANCE
UAS, otherwise known as drones, offer the potential to enhance public safety as well as cement America's leadership in global innovation. But criminals, terrorists, and hostile foreign actors have intensified their weaponization of these technologies, creating new and serious threats to our homeland. Drug cartels use UAS to smuggle fentanyl across our borders, deliver contraband into prisons, surveil law enforcement, and otherwise endanger the public. Mass gatherings are vulnerable to disruptions and threats by unauthorized UAS flights. Critical infrastructure, including military bases, is subject to frequent — and often unidentified — UAS incursions. Immediate action is needed to ensure American sovereignty over its skies and that its airspace remains safe and secure.

10 USC 130i: Protection of Certain Facilities and Assets from Unmanned Aircraft
Authorizes the Department of Defense (DOD) to detect, identify, monitor, track, and mitigate threats posed by UAS, or drones, to specified covered facilities and assets within the United States. This authority allows the DOD to take actions that might otherwise be restricted by law, such as intercepting communications to disrupt drone control, disable, or destroy a UAS threat.

50 USC 2661: Protection of Certain Nuclear Facilities and Assets from Unmanned Aircraft
Grants the Secretary of Energy (with consultation from the Secretary of Transportation) the authority to take action to protect certain nuclear facilities and assets from threats posed by unmanned aircraft systems or unmanned aircraft.

6 USC 124n: Protection of Certain Facilities and Assets from Unmanned Aircraft
Grants the Secretary of Homeland Security and the Attorney General the authority to take actions to mitigate a credible threat (as defined by the Secretary or the Attorney General, in consultation with the Secretary of Transportation) that an UAS poses to the safety or security of a covered facility or asset.

USC Title 32- National Guard
Defines the organization, personnel, training, procurement, and homeland defense activities of the National Guard.

FY2025 National Defense Authorization Act (NDAA): Countering Uncrewed Aircraft Systems
Strengthens Department of Defense (DOD) authority and resources to counter threats from UAS.

Federal Legal Concerns to Mitigating UAS Threats

18 USC 32: Destruction of Aircraft or Aircraft Facilities
Establishes the destruction of aircraft or aircraft facilities as a crime.

18 USC 1030: Fraud and Related Activity in Connection with Computers
Makes it a crime to intentionally access a computer without authorization, or beyond authorized access, to obtain information, commit fraud, cause damage, or conduct further other unlawful activity.

18 USC 1367: Interference with the Operation of a Satellite
Makes it an offense to intentionally or maliciously interfere with the authorized operation of a communications or weather satellite, or to hinder any satellite transmission.

State

RCW 47.68.250: Registration of Aircraft
Every aircraft, inclusive of commercial UAS, must be registered with the department for each calendar year in which the aircraft is operated or is based within this state. A fee of fifteen dollars is charged for each such registration and each annual renewal.

WAC 200-250-030: Use of Unmanned Aircraft is Prohibited
Launching, landing, or operating an unmanned aircraft from or on lands and waters within the boundaries of the state capitol campus is prohibited except for the exclusions listed under WAC 200-250-040.

WAC 352-32-130: Aircraft
Defines the legal use of UAS in Washington State parks.

Annex D: Law Enforcement Quick Reference — UAS Coordination Contacts

This Annex is intended to serve as a quick reference guide for law enforcement agencies in responding to incidents involving Unmanned Aircraft Systems (UAS). It does not in any way supersede or replace the authority of existing laws, regulations, and jurisdictional protocols.
Local law enforcement agencies encountering UAS incidents may use the following points of contact for reporting and coordination. Agencies are encouraged to add specific local contact details in the spaces provided.

Agency/Entity	**Role**	**Contact Information (fill in locally)**
Local Dispatch/Communications Center (Computer-Aided Dispatch – CAD)	Always notify dispatch and ensure the incident is officially entered into the CAD system. Dispatch can relay to aviation units, and other agencies as needed.	
Local Emergency Management Director/Duty Officer	Report UAS activity that may affect public safety, critical infrastructure, or require coordination with local and state resources.	
Local Prosecutor/City/County Legal Contact	Case-specific coordination for charging, local ordinances, and enforcement actions.	
FAA Law Enforcement Assistance Program (LEAP) – Western Regional Operations Center	Report unsafe UAS operations, airspace violations, or hazardous flight near airports/aircraft.	206-231-2089
Washington State Fusion Center (WSFC)	State-level intelligence and information sharing. Report suspicious UAS activity, surveillance, or emerging threats.	877-843-9522
Washington State Emergency Operations Center (SEOC) Duty Officer	24/7 state coordination for significant incidents requiring resources, situational awareness, or escalation.	800-258-5990

Washington State Department of Transportation – Aviation Division	How to register a commercial UAS, information about the State UAS Coordinator, and drone program.	564-999-1040

Notification and Reporting

1. **Local Notification (First Priority):** Notify the dispatch/communications center (CAD), agency supervisors, and the appropriate county or city emergency management department, according to department procedure.
2. **State and Federal Notification (As Applicable):** Following local notification, escalate to state and federal partners, including the Washington State Fusion Center (WSFC), FAA Law Enforcement Assistance Program (LEAP), and the State Emergency Operations Center (SEOC) Duty Officer, as appropriate.
3. **Documentation and Recordkeeping:** Ensure all actions and observations are documented. Enter reports into the CAD system and maintain incident records to support future coordination, investigation, or potential prosecution in accordance with department procedure.