OREGON DEPARTMENT OF EMERGENCY MANAGEMENT

STATE HOMELAND SECURITY GRANT PROGRAM

FY24

Investment Justifications (IJ)

Mailing address:
P.O. Box 14370
Salem, OR 97309-5062

Applications Due:
Monday, July 1, 2024 by 10pm Pacific Time

All projects must meet the investment justification (IJ) criteria established in this document regardless of whether you are seeking formula-based funding or competitive funding. For FY24, there are seven (7) investment justifications, five (5) of which are also federal priority areas.

All the FY24 investment justifications focus on priority core capability areas and minimizing gaps identified at the state and local level which were identified through the annual state capability assessment and the Integrated Prepared Planning (IPP) process and the THIRA/SPR assessments.

Federal Priority Areas are recognized by DHS/FEMA as national priorities and reflect capability gaps shared across the nation. For those seeking competitive funding, priority will be given to projects that address at least one of the five federal priority areas.

As you build your projects, applicants are required to demonstrate how the project will:

- Support terrorism preparedness; and
- Support building capability and/or closing capability gaps or sustaining capabilities identified in the community's THIRA/SPR process.

Each project must also explain how the proposed project will support the applicant's efforts to:

- Prevent a threatened or an actual act of terrorism;
- Prepare for all hazards and threats, while explaining the nexus to terrorism preparedness;
- Protect citizens, residents, visitors, and assets against the greatest threats and hazards, relating to acts of terrorism; ***and/or***
- Respond quickly and equitably to save lives, protect property and the environment, and meet basic human needs in the aftermath of an act of terrorism.

If you have questions about your capability assessment priorities and gaps aligning with the IJs, please reach out to the grant's coordinator for advice and clarification. This may help you avoid disqualification.

FY24 Core Capability Focus:
Based on the capability assessments submitted to OEM, FY24 SHSP projects must address one of the 12 core capabilities which stood out as high priority and medium to low capability throughout the state. Those Core Capabilities are:

- Access Controls and Identity verification
- Intelligence and Information Sharing
- Interdiction and Disruption
- Logistics and Supply Chain Managment
- Mass Care Services
- On-scene Security, Protection, Law Enforcement
- Operational Coordination
- Operational Communications
- Physical Security Protection Measures
- Planning

- Public Information and Warning
- Screening, Search and Detection

FY24 Investment Justifications

- Domestic Violent Extremism*
- Community Preparedness and Resilience
- Information and Intelligence Sharing*
- Soft Target/Crowded Places Hardening*
- Election Security*
- EOC / NIMS / NQS
- Emergency Communications

*Denotes an IJ that aligns with a Federal Priority Area.

As you build your projects, applicants are required to demonstrate how the project will:

- Support terrorism preparedness; and
- Support building capability and/or closing capability gaps or sustaining capabilities identified in the community's THIRA/SPR process.

Each project must also explain how the proposed project will support the applicant's efforts to:

- Prevent a threatened or an actual act of terrorism;
- Prepare for all hazards and threats, while explaining the nexus to terrorism preparedness;
- Protect citizens, residents, visitors, and assets against the greatest threats and hazards, relating to acts of terrorism; and/or
- Respond quickly and equitably to save lives, protect property and the environment, and meet basic human needs in the aftermath of an act of terrorism or other catastrophic incidents.

Seven Investment Justifications

1) Domestic Violent Extremism Prevention

As stated in the Homeland Threat Assessment 2024, terrorism, including domestic violent extremism, remains a top threat to the Homeland. Domestic violent extremists capitalize on social and political tensions, which have resulted in an elevated threat environment. They utilize social media platforms and other technologies to spread violent extremist ideologies that encourage violence and influence action within the United States.

Applicants are encouraged to submit an investment related to combatting the rise, influence, and spread of domestic violent extremism. Investments under this priority may include the development, implementation, and execution of prevention-focused program and initiatives, such as threat assessment and management programs to identify, evaluate, and analyze indicators and behaviors indicative of terrorism and targeted violence.

Examples of holistic approaches to this IJ could include:

- Contracting with community-based conflict mediation organizations
- Mental health service
- Social media monitoring programs
- See Something Say Something™ campaigns
- Social service activities which could prevent or identify lone-wolf radicalization
- Multidisciplinary behavioral health assessment teams

Additional resources and information regarding domestic violent extremism are available through Center for Prevention Programs and Partnerships | Homeland Security (dhs.gov).

2) **Community Resilience**

This investment will encourage whole community involvement in a community's preparedness efforts by allowing enhancement and sustainment of:

- CERT volunteer programs
- public/private partnerships activities encouraging whole community involvement in a community's preparedness efforts
- mass care and casualty projects
- public information and alerts, including overcoming cultural or language barriers.

This investment justification **will not pay** for:

- The purchase of first responder equipment or supplies. All requests for equipment or supplies should be appropriate for trained volunteers or the community at large.

- Any overtime and/or backfill for trained first responders or jurisdiction employees to instruct CERT or community preparedness trainings or outreach.

Mass Care/Casualty type projects
Projects addressing mass care and mass casualty may reference plans written by communities for response to all hazards events but must reference acts of terrorism as one of those hazards.

For mass care-related equipment projects, jurisdictions must have a viable inventory management plan before applying to purchase shelf-stable food and/or water. The inventory management plan must be referenced in the body of the application. The entire plan must be included in the project application.

The state cannot, according to federal guidance, spend more than $100,000 in aggregate, for this grant program, on shelf-stable food and water.

3) Information and Intelligence Sharing with Federal, State, and Local Partners

Effective homeland security operations rely on access to, analysis of, and the timely sharing of open source, unclassified, and classified information, suspicious activity reports, tips/leads, and actionable intelligence on indicators and behaviors to accurately identify, assess, and mitigate a wide array of threats against the United States, including terrorism, threats to life, targeted violence, and other threats within the DHS mission space.

Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, tribal, and territorial governments and private sector partners.

Cooperation and information sharing among state, local, tribal, territorial, and federal partners across all areas of the homeland security enterprise, including counterterrorism, while upholding privacy, civil rights, and civil liberties protections, is critical to homeland security operations and the prevention of, preparation for, protection against, and response to acts of terrorism, and other threats to life and criminal acts of targeted violence. Counterterrorism includes both international and domestic terrorism, cybersecurity, border security, transnational organized crime, immigration enforcement, economic security, and other areas.

Applicants must justify persuasively how they will contribute to the information sharing and collaboration purposes of the investment and a culture of national preparedness.

Additional resources and information regarding collaboration and information sharing are available through the Department's Office of Intelligence and Analysis.

4) Soft Target Hardening

Soft targets and crowded places are increasingly appealing to terrorists and other violent extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other violent extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, polling places, and similar facilities.

Additionally, it is important that personnel responding to incidents at these locations are trained on key operational systems, such as ICS, to ensure proper command, control, and coordination of on-scene incident management.

The malicious use of unmanned aircraft systems poses a threat to the safety and security of the American people, communities, and institutions. Technologies to detect or mitigate unmanned aircraft systems are an allowable use under the HSGP in accordance with the

Domestic Counter-Unmanned Aircraft Systems (UAS) National Action Plan. Recipients should ensure that, prior to the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, they seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws which may apply to the use of such technologies.

Additional resources and information regarding securing soft targets and crowded places are available through the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology.

Projects seeking competitive funding under this IJ will receive priority during the grant review process.

5) Elections Security

Violent protests, intimidation, misinformation, and attempts to tamper with elections equipment have become all too common in resent elections. This IJ supports projects that address these threats and support and sustain our foundational principles of democracy; free and fair elections.

In January 2017, DHS designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Additionally, the Homeland Threat Assessment 2024 indicates that electoral processes remain an attractive target for many adversaries.

Securing election infrastructure, ensuring its continued operation in the face of threats and harassment, advancing the safety of election officials, and ensuring an election free from foreign interference are national security priorities. Threats to election systems are constantly evolving, so defending these systems requires constant vigilance, innovation, and adaptation.

ALL Applicants **must** coordinate with ODEM for all projects and matters related to the election security National Priority Area, prior to submitting your application. **Any activities proposed that could be used to suppress voter registration or turnout will not be approved.*

Emergency Operations Centers / NIMS / NQS

This IJ provides funding for projects which support Emergency Operations Centers (EOC) including activities to advance your agency's National Incident Management System (NIMS) and National Qualification System (NQS).

All gaps addressed through this investment must be identified in an EOC assessment, through the after-action report/improvement plan (AAR/IP), or through your THIRA/SPR process.

Upon completion of any training, subrecipients will be required to complete an exercise (use of the Homeland Security Exercise and Evaluation Program (HSEEP) is recommended) and develop an after-action report and associated improvement plan that identifies successes and addresses any shortcomings.

This IJ will also support the purchase of equipment to build capabilities and resiliency of the EOC. For physical improvements to your EOC, you must provide your plan language which describes the location as your primary or secondary EOC.

7) Emergency Communications

This IJ supports all POETE type projects that support voice/data operability/interoperability, with a primary focus on infrastructure development, particularly where regional/multi-jurisdictional projects are the solution. For FY24 priority will be given to Communication Plan updates, as this has been identified as a local need, which has been overshadowed by equipment purchases.

There will not be a local match requirement for this IJ in FY24.

Requested equipment must align with these authorized equipment list (AEL) categories: 4 – information technology; 6 – interoperable communications; 10 – power; 14-SW-01 – physical security enhancements; 21-GN-00-INST – installation.

To apply for equipment that is not aligned with the above AEL categories, written approval from OEM must be obtained before application submission. Any approvals given must be included with the application package.

Communications towers and related equipment are eligible expenses. Applications for work at communications sites must provide proof that all permits are approved, and agreements are in place to allow the project to move forward if funded. Applicants interested in pursuing tower site projects are highly encouraged to attend grant workshops and work directly with the OEM grants team to ensure success.

All emergency communications equipment purchased with SHSP funds must align with SAFECOM, the Oregon Statewide Communication Interoperability Plan (SCIP) and a promulgated local communications plan and/or strategy, and, when applicable, be P25 compliant. If you think your project does not align with SAFECOM or the SCIP, you must seek approval from OEM before submitting your application. More information about these requirements is provided at https://www.cisa.gov/publication/emergency-communications-grant-guidance-documents.

Applicants are encouraged to coordinate with OEM's communications officer, Oregon's statewide interoperability coordinator (SWIC) and/or the State Interoperability Executive Council (SIEC) Technical Committee when developing an emergency communications project. This coordination will ensure the project supports the statewide strategy to improve emergency communications and is compatible and interoperable with surrounding systems. Competitive

funding projects that are developed in coordination with these entities may receive priority by the grant review committee.

Restrictions under this Investment Justification

Federal prohibitions on expending FEMA award funds for covered telecommunications equipment or services must be followed. Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or
iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

The following page contains the Investment Justification Alignment Table which will assist you in selecting the proper mission area, core capability, and POETE for your project. Your project must align with the options established on this table. Deviations from this table may result in your project being disqualified.

F*or more information regarding allowable projects, project examples, and Federal Priorities, please see the FY24 HSGP NOFO. Pages 8 through 12*

Any questions regarding this document and its guidance should be directed to:

Kevin Jeffries
Grants Coordinator
Oregon Department of Emergency Management
Mobile: 971-719-0740
Kevin.jeffries@oem.oregon.gov

FY24 IJ to POETE Crosswalk

Investment Justification	Mission Area	Core Capability	POETE	Project Types/Examples
Domestic Violent Extremism Prevention	Prevention Protection	Planning Intelligence and Information Sharing Screening Search Interdiction and Disruption Operation Coordination	Planning Organization Equipment Training Exercise	Planning, Bomb Teams, LETPA activities, Community Coordination Councils, Titian Fusion Centers, Public Health/Mental Health Interventions, FTE-Analyst
Community Resilience	Prevention Protection Response Recovery	Planning Public Information and Warning Supply Chain integrity and Security Physical Protective Measures Mass Care Services	Planning Organization Equipment Training Exercise	Mass Care, CERT Teams, Housing, Planning, FTE-Outreach Coordinators, Evacuations and Shelters Supply/Equipment, SAR, Active Shooter,
Intelligence Sharing with State, local, and Federal Partners	Prevention Protection Response Recovery	Planning Intelligence and Information Sharing Operations Coordination On-scene Security, Protection, Law Enforcement	Planning Organization Equipment Training Exercise	Planning, Titian Fusin Center, Community Coordination Councils, OpsCenter-Training/Exercise, FTE-Analyst
Soft Target Hardening	Prevention Protection	Interdiction and Disruption Screening, Search and Detection Access Controls and Identity verification Physical Protective Measures Public Information and Warning	Planning Organization Equipment Training Exercise	Planning/Assessments, Gates, Lights, Locks, ID-Card Reader, Anti-vehicle Ballard, P.A. Warning Systems, Surveillance Cameras,
Elections Security	Prevention Protections	Planning Intelligence and information Sharing Screening, Search and Detection Access Controls and Identity verification Physical Security Protection Measures	Planning Organization Equipment Training Exercise	Planning/Assessments, Camaras, Lights, Locks, ID-Card Readers, Cybersecurity, physical security enhancements, LETPA,
EOC / NIMS / NQS	Response Recovery	Planning Public information and Warning Infrastructure Systems Operational Coordination Logistics and Supply Chain and Security Intelligence and Information Sharing	Planning Organization Equipment Training Exercise	Planning/Assessments, Equipment/Supplies, Training, Go-Bags, Exercises,
Emergency Communications	Prevention Protection Response Recovery	Planning Operational Communications Public Information and Warning	Planning Organization Equipment Training Exercise	Planning/Assessments, Trainings, Exercises, AuxComm/Aminture Radio teams, Tactical LETPA equipment, Communications Equipment