

**FY21**

---

**Investment Justifications**

**STATE HOMELAND SECURITY  
GRANT PROGRAM**

**OREGON OFFICE OF EMERGENCY MANAGEMENT**

[www.oregon.gov/OMD/OEM](http://www.oregon.gov/OMD/OEM)



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

**Physical address:  
3225 State Street  
Salem, OR 97301**

**Application Deadline:  
April 18, 2021, 11:59 p.m. PDT**

Please review changes to the allocation model, application process, state investment justifications and federal priority areas carefully. Documents that describe changes implemented in FY21 are available at

<https://www.oregon.gov/oem/emresources/Grants/Pages/HSGP.aspx>.

All projects must meet the Investment Justification criteria established in this document. Additionally, if you seeking a competitive award, priority will be given to projects that address at least one of the five federal priority areas described on pages 7 through 9 of this document.

State Investment Justifications focus on minimizing gaps identified at the state and local levels through the State Threat and Hazard Identification and Risk Assessment (THIRA) and State Preparedness Report (SPR) process. By using SHSP funds to prepare for a terrorist or catastrophic event, Oregon communities will be better prepared for all levels and types of threats and hazards.

Oregon's THIRA evaluates state and local gaps based on three scenarios: a multiple location/IED event, a Cascadia Subduction Zone earthquake, and a coordinated cyberattack on critical systems. All scenarios are realistic, probable, and catastrophic for residents in affected jurisdictions.

The application for each project must describe how the project is related to the THIRA, how it addresses one more capability gaps, and how it is related to one more of the following investment justifications.

## **1) Planning**

This investment addresses identified gaps, with a focus on assessing and surveying capabilities, creating or enhancing emergency operations planning throughout the state, and supporting the training, implementation and exercising/validation of developed plans.

Oregon has implemented a statewide emergency operations and management planning format that has been institutionalized at state, tribal, county, and city levels. This planning format incorporates the National Incident Management System (NIMS), National Response Framework (NRF), and the Comprehensive Preparedness Guide (CPG) planning requirements and guidance.

Examples of projects this investment can address include but are not limited to: assessments, maintenance and enhancement of plans related to NIMS, communications, critical infrastructure, all hazards, cyber security, vulnerable

FY21 State Homeland Security Program Oregon Investment Justifications  
populations, catastrophic events, emergency operations centers, continuity of operations (COOP), and the implementation of the THIRA process.

In addition to plan development, this investment will require subrecipients to address the training and exercise components necessary for effective implementation of the developed plan. In accordance with the Homeland Security Exercise and Evaluation Program (HSEEP), upon completion of training, subrecipients will be required to complete an exercise, then develop an after-action report and associated improvement plan that addresses any shortcomings identified in the plan. For all approved projects, subrecipients are required to promulgate the plan and update the plan every five years at a minimum.

**Projects that support the Cascadia Rising 2022 (CR22) exercise are eligible under this investment justification. The CR22 exercise is a high priority for Oregon. Projects related to the exercise will receive a 10-point bonus during competitive award review.**

## **2) Communications**

This investment addresses communications equipment, training and exercising activities which include: projects that support voice/data operability/interoperability, with a primary focus on infrastructure development particularly where regional/multi-jurisdictional projects are the solution.

**Projects requesting end-user units will not be considered eligible unless the requesting agency is providing a minimum of a 10 percent match.**

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 prior to 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 the Grants Roadshow Training and work directly with the OEM grants team to ensure success.

All equipment purchases 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.

**Restrictions under this Investment Justification:**

See the page 33 of the FY21 Notice of Funding Opportunity (NOFO) regarding *Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services*.

*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.*

**3) Chemical, Biological, Radiological, Nuclear and high-yield Explosives (CBRNE) Detection and Response**

This Investment will provide support to overarching activities the State has identified as priorities, with an emphasis on maintaining existing capabilities:

- improving the capabilities of existing special teams and first responders to detect and respond to CBRNE incidents, through the acquisition of discipline appropriate, CBRNE detection and response equipment; and
- training and exercises to further improve the ability of first responders and special teams to detect and respond to CBRNE incidents.

This investment directly addresses the listed targets from the State Preparedness Report (SPR) by providing for the systematic acquisition of discipline specific and proven detection/response technologies, while allowing for the sustainment of specialized teams (bomb squads, SWAT, US&R, Hazmat, or an organized team with a defined mission in a WMD response, etc.).

#### **4) Community Resilience**

This investment will encourage whole community involvement in a community's preparedness efforts by allowing enhancement of and ensuring the sustainment of, CERT volunteer programs; public/private partnerships; public education and training, and activities encouraging whole community involvement in a community's preparedness efforts.

The investment addresses capability gaps in community preparedness, while continuing to support and enhance CERT generally. Specific gaps to be addressed include: enhancing the capacity of local CERT to manage volunteers and sustain their continued operation; sustaining and strengthening the CERT State Advisory Committee; increasing delivery of Train-the-Trainer courses; capitalizing on volunteer outreach using community preparedness events; creating a more resilient community through volunteer and community organizations; and supporting the creation of public/private partnerships.

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.

#### **5) Emergency Operation Centers**

This investment provides funding for capability improvements of state, local and tribal governments' primary and secondary EOC, as identified in a promulgated Emergency Operations Plan through equipment purchases as well as training and exercising.

All gaps addressed through this investment must have been identified in an EOC assessment, or through the After Action Report/Improvement Plan (AAR/IP).

This investment will require subrecipients to address the training and exercise components necessary for effective implementation of new equipment or training. Upon completion of any required equipment 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 with equipment implementation.

## **6) Mass Care and Mass Casualty**

This investment provides funding for the implementation of mass care and mass casualty plans written by communities for response to catastrophic and terrorism events in the community.

This investment is for the purchase of equipment and supplies, training and exercises directly related to the implementation of mass care and mass casualty plans. To be eligible for this investment justification, applicants must have a promulgated plan addressing mass care and/or sheltering and/or mass casualty events. The specific section of the promulgated plan which the proposed project is addressing must be referenced in the body of the application.

Jurisdictions must have a viable inventory management plan prior to applying to purchase shelf stable food and/or water. The inventory management plan must be referenced in the body of the application and the entire plan must be included with the electronic copies of application submission.

The State cannot, according to Federal guidance, spend more than \$100k in aggregate, for this grant program, on shelf stable food and water.

## **7) Cybersecurity**

This investment provides funding for the implementation of cybersecurity measures identified in a formal system assessment or cybersecurity plan.

This investment is for the purchase of software and hardware, training, and exercises directly related to the implementation of cybersecurity plans. The specific section of the promulgated plan or official assessment which the proposed project is addressing, must be referenced in the body of the application.

## **Federal Priority Funding Areas**

For 2021, DHS/FEMA has identified five priority areas that must be addressed by the State to receive the full grant award listed in the NOFO:

1. Enhancing cybersecurity (7.5 percent)
2. Enhancing the protection of soft targets/crowded places (5 percent)
3. Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies, including DHS (5 percent)
4. Combating domestic violent extremism (7.5 percent)
5. Addressing emergent threats (5 percent)

See the FY21 NOFO for more information about the federal priority areas:

[https://www.fema.gov/sites/default/files/documents/FEMA\\_FY2021-HSGP-NOFO\\_02-19-21.pdf](https://www.fema.gov/sites/default/files/documents/FEMA_FY2021-HSGP-NOFO_02-19-21.pdf).

Applicants are encouraged but not required to submit projects that address the priority areas. Competitive award applications that address the federal priority areas will be given priority.

### **Enhancing Cybersecurity**

Cybersecurity investments must support the security and functioning of critical infrastructure and core capabilities as they relate to preventing, preparing for, protecting against, or responding to acts of terrorism. Recipients and sub-recipients of FY21 HSGP grant awards will be required to complete the 2021 Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture.

### **Enhancing the Protection of Soft Targets/Crowded Places**

Soft targets and crowded places are increasingly appealing to terrorists and other 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 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, and similar facilities.

## **Enhancing Information and Intelligence Sharing and Analysis, and Cooperation with Federal Agencies**

Effective homeland security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism. This investment may include at least one dedicated fusion center project.

## **Combating Domestic Violent Extremism**

Domestic violent extremists, including ideologically motivated lone offenders and small groups, present the most persistent and lethal terrorist threat to the Homeland. These 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.

The COVID-19 pandemic has further created an environment that may lead to accelerated mobilization to targeted violence and/or radicalization to domestic terrorism, including driving lawful protests to incite violence, intimidate targets, and promote their violent extremist ideologies.

## **Addressing Emergent Threats**

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market.

Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

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



Kevin Jeffries, Grants Coordinator  
Operations and Preparedness Section  
Oregon Office of Emergency Management  
503-378-3661  
[kevin.jeffries@state.or.us](mailto:kevin.jeffries@state.or.us)

or

Traci Naile, Manager  
Operations and Preparedness Section  
Oregon Office of Emergency Management  
503-378-4025  
[traci.naile@state.or.us](mailto:traci.naile@state.or.us)