



# Oregon State Infrastructure Protection Plan (OSIPP)



March 2017

**Table of Contents**

**EXECUTIVE SUMMARY ..... 3**

**INTRODUCTION ..... 5**

    Purpose..... 5

    Objective ..... 5

    Threats..... 5

    Oregon Jurisdictions & Regions ..... 7

**PLANNING FOR CIKR PROTECTION ..... 8**

    Oregon Strategies ..... 8

    Working With Security Partners ..... 9

    Roles and Responsibilities ..... 10

    Agencies with Critical Responsibilities..... 13

    US Homeland Security Grant Programs ..... 15

**CIKR PROTECTION STRATEGY ..... 16**

    NIPP Risk Management Framework ..... 16

    Threat and Vulnerability Assessments ..... 17

    Measuring Plan Effectiveness ..... 18

**CIKR PROTECTION RESILIENCY ..... 19**

    Protected Critical Infrastructure Information (PCII) Certification Program ..... 19

    Protective Programs, Initiatives, and Reports ..... 19

    Awareness & Training Programs ..... 20

**CONCLUSION ..... 21**

    Definitions ..... 22

    Glossary of Acronyms ..... 23

    References/Citations ..... 25

# EXECUTIVE SUMMARY

---

The State of Oregon has developed the Oregon State Infrastructure Protection Plan (OSIPP) to safeguard critical assets and resources that are vital to the operation of the daily lives of all Oregonians. Critical Infrastructure and Key Resources (CIKR) are defined by the US Department of Homeland Security (US DHS) as the backbone of our nation’s economy, security, and health. Simplified, CIKR are what makes our nation, our state, our local jurisdictions, and our tribal nations run. CIKR includes those assets, systems, and networks (physical or virtual) so vital that their incapacitation or destruction would have a debilitating impact. Key resources are publicly and privately controlled resources that are essential to the minimal operation of the nation’s economy, security, and health.

US DHS has identified 16 sectors to define critical infrastructure, these include:

<ul style="list-style-type: none"><li>• Chemical</li><li>• Commercial</li><li>• Communications</li><li>• Critical Manufacturing</li><li>• Dams</li><li>• Defense Industrial Base</li><li>• Emergency Services</li><li>• Energy</li></ul>	<ul style="list-style-type: none"><li>• Financial Services</li><li>• Food &amp; Agriculture</li><li>• Government Facilities</li><li>• Healthcare &amp; Public Health</li><li>• Information Technology</li><li>• Nuclear Reactors, Materials, &amp; Waste</li><li>• Transportation Systems</li><li>• Water &amp; Wastewater Systems</li></ul>
--	--

US DHS has developed the *National Infrastructure Protection Plan (NIPP)*. This plan outlines the national need for CIKR protection and is intended to guide local public and private stakeholders in the creation of infrastructure protection plans. The NIPP provides a framework from which state, regional, and local entities can develop infrastructure protection and resiliency plans and programs.

Oregon has developed a CIKR Program at the Oregon Terrorism Information Threat Assessment Network (TITAN) Fusion Center (OTFC), housed within the Criminal Justice Division of the Oregon Department of Justice. The OTFC is responsible for the daily dissemination of Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES), and For Official Use Only (FOUO) information related to Oregon’s homeland security efforts. The OTFC has been conducting threat assessments for locations and events throughout Oregon since 2007. Given the daily information exchange and uniquely qualified staff, infrastructure protection incorporates seamlessly into the OTFC’s mission “to protect Oregon citizens from terrorist and criminal activity”.

The risk environment surrounding CIKR is complex and uncertain. With evolving terror threats, unpredictable natural disasters and cyber-attacks, the term *threat* takes on a multitude of meanings. As such, the OSIPP utilizes the “all hazards” approach to risk assessment. Protection, security, and resiliency efforts will take into consideration all events that could destroy or incapacitate any human, physical, or virtual asset or resource in Oregon. In reviewing the consequences of all threats, we can foster mitigation and resiliency efforts regardless of the event or incident. This approach will guide all Oregon stakeholders in CIKR planning and resiliency. These stakeholders include but are not limited to: state, regional, local, and tribal governments, private security entities, and local community partners.

Community partner involvement in managing risks to CIKR is crucial to the success and implementation of the OSIPP. Composed of partnerships among asset owners and operators, non-profit organizations, regional entities and academia, community partners have a wide range of roles to support the statewide CIKR protection efforts. They will assist in identifying and detecting risks, reducing vulnerabilities and mitigating potential consequences from possible incidents or events that may occur.

Acquiring and maintaining accurate information and analysis about vulnerability and risk are essential to achieving resilience. Public and private outreach by the CIKR Program for education, coordination and information sharing efforts will be paramount in the success of the OSIPP. These efforts will also assist the CIKR Program in the continued update of the OSIPP as well as the achievement of all goals and objectives herein to ensure Oregon’s infrastructure is protected, secure, and resilient.

# INTRODUCTION

---

## **PURPOSE**

The purpose of the OSIPP is to facilitate a coordinated statewide effort to identify, assess, and protect CIKR assets within, and in support of, the State of Oregon. This plan is focused on those assets so vital that if destroyed or incapacitated, it would cause a debilitating impact within the state. The OSIPP is intended to be a springboard for future sector specific protection plans and coordination efforts.

The audience for this plan includes a wide-ranging infrastructure community comprised of public and private infrastructure asset owners and operators; federal departments and agencies, including Sector-Specific Agencies (SSAs); state, local, tribal, and territorial (SLTT) governments; regional entities; and other private and non-profit organizations charged with securing and strengthening the resilience of CIKR.

The strategy established by the OSIPP addresses specific concerns relating to CIKR to ensure that quality of life, economic prosperity, and cultural dimensions are preserved for the citizens and residents of Oregon.

## **OBJECTIVE**

Enhance protection of the State's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorist, other criminal elements or other catastrophic event to destroy, incapacitate, or exploit them; enable Oregon's preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency; and to protect the citizens of Oregon through proactive preparedness measures.

## **THREATS**

The following qualify as terrorist threats or state significant disasters:

- Events that would causes catastrophic health effects.
- Incidents that would impair State departments and agencies' abilities to perform essential missions, and ensure public safety and health.
- Actions that would undermine the State and local government capacities to maintain order.

- Events that would damage the private sector’s capability to ensure the orderly functioning of the economy and delivery of essential products and services.
- Actions that would have a negative effect on the economy through disruption of CIKR.
- Events that would undermine the public’s morale and confidence in the government and economic and political institutions.
- Events or actions that would cause substantial change in the quality in the way Oregon’s citizens live.

Critical infrastructure and key resources maintain a vital role in the Threat and Hazard Identification and Risk Assessment (THIRA) and the State Preparedness Report (SPR) process. Oregon, as well as all other states and territories receiving federal preparedness funds through the US DHS, complete a THIRA and SPR annually per the federal requirement in the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA). The THIRA and SPR process is focused on prominent state threats and hazards, and involves coordination from a broad range of community members and critical infrastructure sectors.

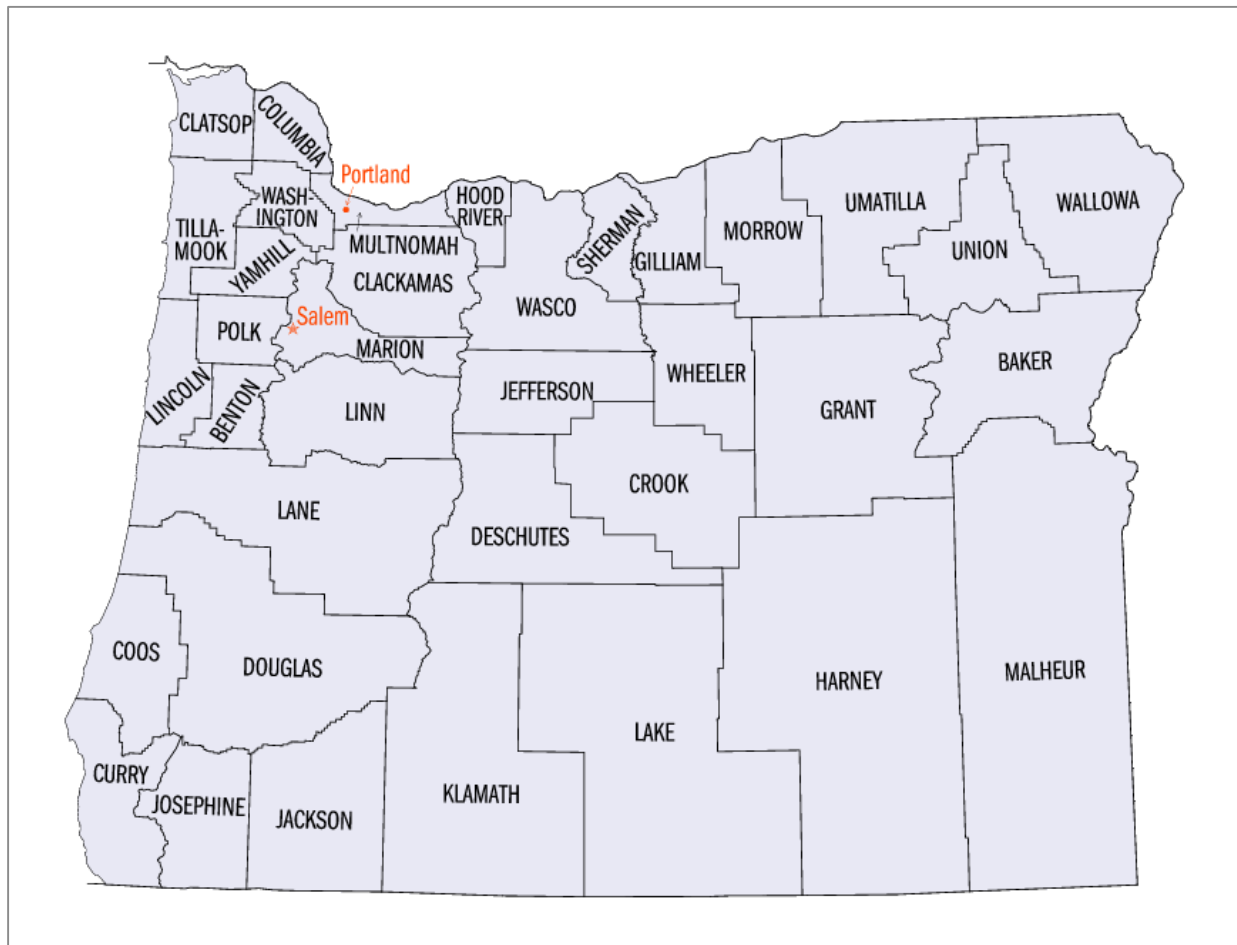
States and territories begin by setting capability targets identified in the THIRA process. They then assess their current preparedness levels for achieving their THIRA targets according to the 31 core capabilities defined in the *National Preparedness Goal (NPG)*. Core capabilities are distinct critical elements needed to achieve the NPG, and are referenced in many national preparedness efforts, including the National Planning Frameworks. With this in mind, CIKR are central to many core capabilities and therefore a necessary consideration in order to achieve optimal preparedness as defined in the NPG. Information pertaining to the CIKR, as well as engagement with CIKR partners, are important parts in assessing preparedness in Oregon.

## OREGON JURISDICTIONS AND REGIONS

Oregon is comprised of 36 counties and 1 Urban Area. Many of the jurisdictions within Oregon lack the ready resources necessary to respond to various emergencies, especially a Weapon of Mass Destruction (WMD) terrorism incident. They rely on larger jurisdictions to provide resources through mutual aid and inter-agency agreements. A key aspect of the Oregon strategy is assessing the current coverage of those agreements. This strategy will encourage municipalities that currently have capabilities, or that are developing those capabilities, to expand their existing area of mutual-aid/interagency agreement coverage. Jurisdictions are identified by county borders and the core urban area. Approving authority is maintained at the State Administrative Agency (SAA) level with coordination and program implementation facilitated by the Oregon Office of Emergency Management.

### Jurisdictions

The 37 jurisdictions are as follows: Baker, Benton, Clackamas, Clatsop, Columbia, Coos, Crook, Curry, Deschutes, Douglas, Grant, Gilliam, Harney, Hood River, Jackson, Jefferson, Josephine, Klamath, Lake, Lane, Lincoln, Linn, Malheur, Marion, Morrow, Multnomah, Polk, Sherman, Tillamook, Umatilla, Union, Wallows, Wasco, Washington, Wheeler, Yamhill, and the City of Portland.



# PLANNING FOR CIKR PROTECTION

---

Oregon's CIKR protection needs are similar to those of other states and of those outlined in national plans such as the *National Infrastructure Protection Plan* (NIPP) and the *National Response Framework* (NRF). The OSIPP utilizes the NIPP and the NRF's *CIKR Support Annex* to plan for the identification, protection, security, and resilience of Oregon's CIKR.

The *CIKR Support Annex* describes the policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting and restoring CIKR. The Annex details processes to ensure coordination and integration of CIKR-related activities among a wide array of public and private incident managers and CIKR security partners. Specifically:

- The Annex describes roles and responsibilities for CIKR preparedness, protection, response, recovery, restoration, and continuity of operations relative to the State of Oregon.
- The Annex establishes a concept of operations for incident related CIKR preparedness, protection, response, recovery and restoration.

Prevention, response, restoration, and recovery efforts are most efficient and effective when there is full participation of government and industry partners. The "value proposition" set forth in the NIPP articulates the mutual benefits to government and the private sector for engaging in preparedness and response activities.

Communities, tribes, states, the federal government, Nongovernmental Organization (NGOs), and the private sector should each understand their respective roles and responsibilities, and complement each other in achieving shared goals. Each governmental level plays a prominent role in developing capabilities needed to respond to incidents. These capabilities include developing plans, conducting assessments and exercises, providing and directing resources and capabilities, and gathering lessons learned. These activities require that involved organizations understand their roles and responsibilities and how they fit within and are supported by the framework.

## **OREGON STRATEGIES**

Oregon will implement many wide ranging efforts to support the national efforts of protecting, securing, and recovering from events that would threaten our state's CIKR. By pairing methodologies specific to the state with the national methodologies currently in place, we can contribute to the national framework while meeting the needs of the State of Oregon. The following strategies are essential for the success of a coordinated CIKR Program effort:



- Ensure owners and operators are engaged at senior executive and operational levels primarily through their respective Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs).
- Identify infrastructure assets and resources within Oregon and regionally (outside the state) that support Oregon.
- Articulate benefits of a risk-based, cross-sector approach to resilience and protection through outreach.
- Work with owners and operators to clearly establish priorities for prevention, protection, and recovery.
- Provide specialized technical expertise for CIKR-related protection, and recovery.
- Coordinate with federal partners, border states, and regional owners and operators on CIKR.
- Provide federal, state, and local governments, as well as asset owners and operators, timely, accurate, and actionable all-hazards information.
- Identify grant resources for CIKR protection and resiliency efforts.

These strategies will be accomplished by working with security partners, outlining partner roles and responsibilities, and identifying those partners with critical roles.

#### Working with Security Partners

Security Partners include private and public organizations that operate nationally, statewide, and locally to protect assets within Oregon. These partners are vital to the coordinated protection of infrastructure assets and key resources throughout the state.

- **Oregon State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC)**

US DHS enabled and facilitated the formation of the SLTTGCC which has organized to bring together CIKR protection experts from the private sector and all levels of government. The SLTTGCC functions as a forum for state, local, tribal, and territorial government representatives across functional disciplines to engage with the federal government and CIKR owners and operator within the Sector Partnership Model (SPM), to achieve the CIKR protection mission.

- **Oregon Homeland Security Council**

The Oregon Homeland Security Council is a formal group of homeland security professionals chosen per ORS 401.109(2). The group is comprised of law enforcement, military, emergency management, legislative representatives, and other key public department leaders. The Council receives briefings on security matters and related catastrophic disasters or states of emergency declared by the Governor. They advise other state agencies with responsibility for security matters as needed.

- **Oregon Emergency Response System (OERS) Council**

The purpose of OERS is to coordinate and manage state resources in response to natural and technological emergencies and civil unrest involving multi-jurisdictional cooperation between all levels of government and the private sector.

The OERS Council shall direct activities of OERS; all agencies participating in the OERS Council provide cooperative assistance within their resources and authority to other agencies, including but not limited to federal, state, county, city, special district and tribal entities in responding to and mitigating hazards that threaten the State of Oregon, pending further directives by the Governor.

## Roles and Responsibilities

### **State Government**

State department and agency responsibilities:

- Identify, prioritize, and coordinate protection of CIKR by working with the federal, tribal and local governments and the private sector.
- Ensure that homeland security programs do not diminish the overall economic security of Oregon.
- Provide information to the OTFC Threat and Vulnerability Assessment teams on CIKR sites deemed critical at the state level.
- Appropriately protect information associated with carrying out this directive.
- Enhance collaboration among state, local, and tribal entities through communication and coordination with one another, and to include private sector, non-governmental entities, and the general public to effectively prevent, protect, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

## **Local government**

Local government responsibilities:

- Provide information to the OTFC Threat and Vulnerability Assessment teams on CIKR sites deemed critical from the local level.
- Ensure that funding priorities are addressed and that resources are allocated efficiently and effectively.
- Address unique geographical issues, dependencies/interdependencies among agencies, and enterprises within each jurisdiction.
- Conduct or facilitate vulnerability assessments (with the assistance of the OTFC Assessment Teams).
- Encourage risk management strategies.
- Act as a focal point for coordination and promotion of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses and citizens.
- Document lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and apply the lessons to the CIKR protection context.
- Conduct CIKR protection public awareness activities.
- Facilitate the exchange of security information with the OTFC, including threat assessments, attack indications and warnings and advisories, in addition to information sharing among security partners within the jurisdiction.
- Share information with private sector and government security partners as appropriate, regarding CIKR sites deemed critical from the local perspective to enable prioritized protection and restoration of critical public services, facilities utilities, and processes within the jurisdiction.

## **Tribal government**

Tribal government responsibilities:

- Ensure that CIKR locations are identified, to include sacred sites, lands, burial sites, waters, and mountains.
- Work with and maintain open communications with local, state, federal agencies, and surrounding regions.

- Maintain an immediate information link between OTFC, state and federal law enforcement, and first responder agencies.
- Coordinate efforts with the OTFC Assessment Teams to concentrate the effort of acquiring site data and guiding the application of protective measures.

### **Private sector owners and operators**

Private Sector Owner and Operator responsibilities:

- Support risk management profile planning and hardening activities.
- Reassess and adjust continuity of operations and emergency management plans.
- Build in increased resiliency and redundancy into business processes and systems.
- Harden facilities against the physical and cyber-attacks and natural disasters.
- Coordinate and share threat information with OTFC and other external organizations.
- Collaborate with OTFC and other local, state, and federal partners to integrate efforts with Homeland Security programs to share threat information.

### **Sector-Specific Agencies**

Sector-Specific Agency responsibilities:

- Collaborate with USUS DHS to implement the NIPP sector partnership model and risk management framework.
- Develop protective programs and related requirements.
- Provide CIKR protection guidance consistent with overarching guidance established by USUS DHS pursuant to HSPD-7.
- Develop and submit Sector Specific Plan (SSP) and sector-level performance feedback to USUS DHS to enable national level gap assessments.

## Agencies with Critical Responsibilities

**Oregon TITAN Fusion Center (OTFC)** is responsible for Oregon's statewide CIKR program coordination. Through the use of SLTT and private sector partner workgroups, OTFC facilitates the statewide mission to enhance CIKR protection and resiliency. This coordinated effort brings together federal, state and local law enforcement, fire personnel, emergency managers, private security personnel, and other CIKR stakeholders to monitor threat activity, identify asset vulnerability, and provide mitigation guidance.

OTFC manages and encourages programs that promote interaction, training, and communication among the site managers and emergency response teams in order to achieve the most efficient reaction to incidents in Oregon. OTFC provides Fusion Liaison Officers (FLO) serving as the main communication link from an incident or disaster to the OTFC. The FLO program was created to relay information and intelligence efficiently between the OTFC and field resources.

OTFC's CIKR Program is responsible for the following:

- Develop and coordinate the OSIPP.
- Develop comprehensive multi-tiered risk-reduction programs and methodologies in coordination with OEM.
- Develop and coordinate cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols in coordination with the PSA.
- Establish threat/risk management and performance criteria and metrics within and across sectors using the US DHS IP Gateway and input from PSA as described below:
  - ✓ Identify, characterize and assess threats
  - ✓ Assess the vulnerabilities of critical assets to specific threats
  - ✓ Determine risk (likelihood and consequences of specific types of attacks on specific assets)
  - ✓ Identify ways to reduce those risks
  - ✓ Prioritize risk reduction measures based on a strategy

**Oregon Emergency Management (OEM)** is responsible for coordinating the consequences management component of CIKR planning and preparedness. This responsibility includes an analysis and integration of threat and vulnerability data to support local and tribal government, and state agency CIKR incident planning; application of CIKR risk management data to support emergency response actions statewide; and development of specific CIKR response and preparedness products that enhance operability during impacts to CIKR as well as enhancing statewide stability.

- Develops plans, processes, and relationships and facilitates coordinated consequences management planning with the private sector at the strategic, operational and tactical levels.
- Shares consequences management information, including threats and warnings, before, during and after an incident.
- Informs and orients the private sector on the contents of the State Emergency Management Plan, and encourages and facilitates the development and coordination of equivalent private-sector planning.
- Develops, implements and operates information sharing and communications strategies, processes and systems with homeland security stakeholders.

#### **Oregon Department of Justice (ODOJ)**

- Manages operations at the state fusion center (OTFC), and collects and maintains information relating to CIKR.
- Conducts criminal investigations across the State of Oregon.
- Can coordinate specialized HazMat, Explosive Ordnance Disposal (EOD), and Tactical Response Teams (TRT) to support agencies across the State of Oregon in support of OERS and OEM.
- Acquires, manages, and safeguards CIKR information in accordance with applicable laws

#### **Oregon Military Department (OMD)**

- Development and maintenance of a force protection program that manages risk; minimizes vulnerabilities through mission analysis, identification of key assets critical to mission success, threats determination, and vulnerabilities. Reduce risk through the implementation of appropriate protection controls to reduce the likelihood/impact of a stated threat.

- Exercises the force protection program by bringing together all security disciplines to mitigate hostile actions against Oregon Military Department personnel (to include family members) through training, situational awareness, and supporting unit family programs and events.
- Protects CIKR through concerted defensive measures to prevent and deter the vulnerability of property and facilities. These specific security measures are assessed by the facility commander/manager after considering a variety of factors including the threat level, current events that might increase the risk, and observed suspicious activity.

### **US Homeland Security Grant Programs**

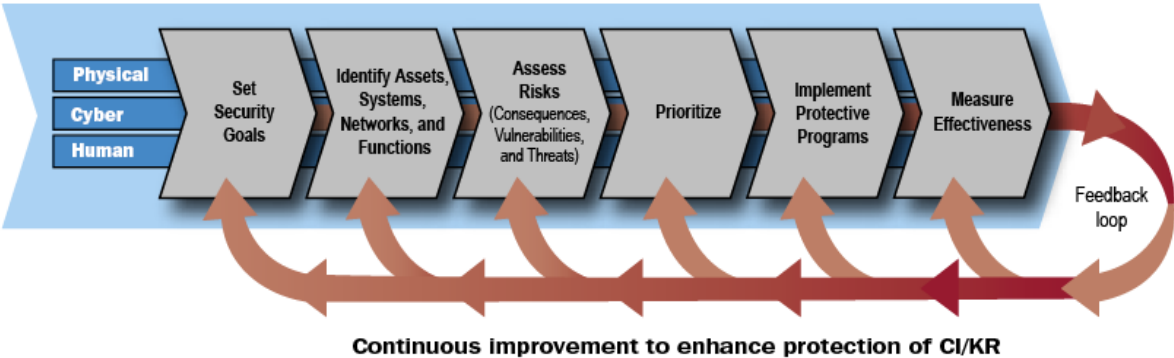
The goals and objectives outlined in the OSIPP would not be possible without financial resources from the US DHS. This funding supports the primary staff at the OTFC with the responsibility for the creation, update and implementation of the OSIPP and any applicable future plan annexes for each sector. The funding also provides the specialized training needed to OTFC personnel to conduct risk vulnerability assessments to assist asset CIKR owner/operators with risk identification and mitigation.

The US Homeland Security Grant Programs are administered by the Oregon Military Department's Office of Emergency Management (OEM) and are:

- State Homeland Security Grant Program (SHSGP)
- Urban Area Security Initiative (UASI)
  - There is one Urban Area Security Initiative (UASI) in Oregon, Portland UASI. The Portland UASI is comprised of Multnomah, Washington, Clackamas, Columbia and Clark (WA) Counties.
  - Portland UASI has working groups that provide input on State Strategy and define the priorities for the application of grant funding.
- Emergency Management Program Grant (EMPG)

# CIKR PROTECTION STRATEGY

## NIPP RISK MANAGEMENT FRAMEWORK



The Risk Management Framework illustrates the concept of a continuous improvement cycle of establishing goals; identifying assets; assessing risks, vulnerabilities and threats; prioritization; implementation; measurement of effectiveness, and reassessment.

### Setting Security Goals

- The OSIPP Goals include the consideration of the physical, cyber and human elements of CIKR protection.
- Goals are established collaboratively among stakeholders in the process with input from subject matter experts as key participants in the OSIPP.
- The state’s CIKR protection programs are managed through the OTFC; security goals will be recorded by OTFC staff into OSIPP revisions and updates.
- The OTFC teams collaborate with representatives from the Oregon CIKR sector representatives and the U.S. Department of Homeland Security’s Protective Security Advisor (PSA) to define program goals and establish parameters.



## Identify Assets

The OTFC is tasked with the maintenance of a comprehensive and up-to-date inventory that includes information about the assets, systems, and networks that comprise the state's CIKR. The OTFC staff will work directly with asset owner operators to gain accurate information on assets during this data collection effort. The OTFC may use several internal systems for asset identification information; additionally, the following federally administered systems will be utilized:

- The Homeland Security Information Network (HSIN) is a US DHS sponsored computer web-based counter terrorism communications system, distributed to all 50 states to strengthen the flow of threat information. HSIN provides information sharing amongst all federal, state and local partners. Each state and federal agency is responsible for their sector or geographic area of responsibility.

HSIN Oregon establishes a link to OTFC resources and statewide homeland security stakeholders and partners. This link provides enhanced integration of existing information sharing efforts within the state. The Oregon HSIN Portal is divided into three sub-portals:

- Oregon LE (LES) – For sworn law enforcement officers and law enforcement agency employed personnel with a valid need to know.
  - Oregon (FOUO) – For non-sworn and non-law enforcement agency employed personnel who have a professional responsibility for public safety and/or sector specific critical infrastructure security with a valid need to know.
  - Oregon IP (FOUO) – For specific IP users, often used in conjunction with the Oregon Community Of Interest (COI).
- The Infrastructure Protection (IP) Gateway is designed to identify, organize, and evaluate asset information and provides nationally standardized formatting of acquired data that may be readily accessed by FLOs in the field.

## Assessing Risks

- Risk assessment methodologies are accomplished through assessment teams and coordinated with the US DHS provided PSA and US DHS Intelligence Officer assigned to Oregon.
- The Risk Management Framework involves a continuous process of assessment, implementation, measurement and reassessment.

## Threat and Vulnerability Assessments

The OTFC will coordinate a process that uses current technologies and standardized best practices that will be implemented based on the statewide assessment of threat and vulnerability.

The US DHS IP Gateway provides the data collection framework that guides the assessment process. Information received by the OTFC will be utilized to identify risks, consequences, threats and vulnerabilities in order to determine the prudent application of the available resources. The OSIPP prevention efforts will include a way for protecting selected sites through design analysis, law enforcement proactive activities and the development of target hardening measures that are intended to mitigate the effects of man-made hazards.

## Prioritizing Risk – Tier Assignments

Results of risk assessments will be prioritized to help identify where vulnerability is greatest and risk reduction is most critical. The prioritization process defines the direction for the assignment of resources as identified by assessment teams. The prioritization data provides for an unbiased guide to support the prudent application of the available OSIPP resources.

## Measuring Plan Effectiveness

The OSIPP will use a metrics-based system to provide feedback on efforts to attain the program's goals and objectives. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the state effort.

Some possible data collection categories: Assets Identified, Risk Vulnerability Assessments Completed, Sector Specific Outreach, Sector Specific Annex Development, HSIN IP COI Users Gained and FLOs Gained.

Increased response capability and the application of resources to satisfy identified gaps recorded as a result of the Homeland Security Grant Program (HSGP) also provide for an effective measurement of program effectiveness. This process has gained improvement and greater refinement with each subsequent year of investment. Continued use of HSGP resources will be incorporated into the annual review.

# CIKR Protection Resiliency

---

OTFC's Fusion Liaison Officer (FLO) program provides the organization and structure for the statewide communication of information pertaining to CIKR assets. FLO personnel within each region are tasked to identify and acquire information on CIKR locations within their response area. This data is accumulated and evaluated at the OTFC using the structure allowed by state law and supported by the IP Gateway data collection system. These same FLOs serve as a conduit to immediately relay critical information to the CIKR site management entities during actual events or emergencies.

Protective Security Advisors (PSAs) are locally based US DHS CIKR and vulnerability assessment specialists assigned to local communities throughout the country. The PSA serves as the CIKR liaison between federal agencies; state, tribal, and local governments; and the private sector. The PSA contributes to the NIPP, NRF and OSIPP requirements by identifying, assessing, and monitoring CIKR and coordinating protective activities within their respective geographic areas during steady-state operations as well as during actual incidents.

## **Protective Programs, Initiatives, and Reports**

The protective programs are managed by OTFC, coordinated with guidance from the U.S. Department of Homeland Security's PSA.

The OTFC will collaborate with members of the Portland Urban Area Security Initiative's Law Enforcement Group or similar element to support the application of consistent and cohesive state protection strategies.

The OTFC will meet as required with stakeholders to facilitate the accomplishment of timely and relevant reporting of progress and areas of concern.

## **Protected Critical Infrastructure Information (PCII) and Other Security Regimes**

The Protected Critical Infrastructure Information (PCII) Program was established pursuant to the Critical Infrastructure Information (CII) Act of 2002. The Program provides a means for sharing private sector information with the government while providing assurances that the information will be exempt from unauthorized public disclosure and will be properly safeguarded. This assurance enables members of the private sector to voluntarily submit sensitive information regarding the CIKR to US DHS knowing that the information will be protected.

US DHS established the PCII Program Office to manage CII information, develop protocols for handling this information, and raise awareness of the need for protected information sharing between the public and private sectors. The PCII Program Office is responsible for receiving, validating, and safeguarding CII submitted to US DHS. The Program Office works with government programs and those entities in the private sector willing to share their information on a voluntary basis.

The PSA Program provides Protection Specialists that are assigned as liaisons between US DHS and the critical infrastructure protection community at the state, local, and private sector levels representing major concentrations of CIKR across the United States. The PSA is responsible for sharing risk information and providing technical assistance to local law enforcement and the owners and operators of assets within those areas. The PSA assists program participants in achieving compliance with PCII standards.

The Oregon Department of Justice (ODOJ) and other law enforcement agencies have an established structure for sensitive information that supports the creation of a statewide CIKR information system. ODOJ has identified the IP Gateway database as the system that will be utilized to acquire, manage and safeguard CIKR information at the OTFC. PCII and For Official Use Only (FOUO) data acquired and stored by ODOJ is offered legal protection by both State and Federal legislation.

### Awareness and Training Programs

The OTFC and OEM sponsor numerous ongoing programs featuring a number of training and awareness courses that are available to OSIPP participants and stakeholders. Oregon will provide CIKR stakeholders with training that supports CIKR programs within the state centered around manmade and natural disasters and focused on overall protection and sector specific challenges. Such training will be provided through coordinated outreach through existing events such as:

- OEM Conference
- Emergency Management Workshops
- Fusion Liaison Officer Trainings

In addition, there will be further efforts that will focus specifically on CIKR:

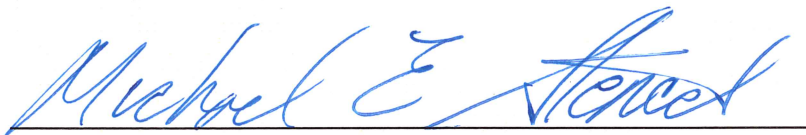
- Local Emergency Management Regional Meetings
- Sector Specific Statewide Meetings
- Regional collaborative outreach with bordering states

# CONCLUSION

---

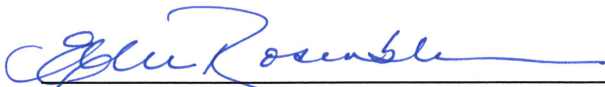
Oregon's Critical Infrastructure Program has developed the OSIPP to provide a first step in a coordinated effort to identify and protect critical infrastructure and key resources across the state. The combined strategies outlined herein will increase awareness and resiliency within the infrastructure community in Oregon. The outreach efforts will increase participation of local stakeholders and collaborators.

The Critical Infrastructure Program efforts enlist the expertise of federal, state, local, tribal and owner/operator partners to participate and enhance the OSIPP strategies, implementation processes, and overall goals. Together, the efforts put forth by the Critical Infrastructure Program and partners will create an environment that fosters information sharing and awareness. The information shared within the Oregon infrastructure community will be vital to extensive, efficient, and effective threat assessments and vulnerability awarenesses.



---

MICHAEL E. STENCEL  
Major General  
The Adjutant General  
Oregon Military Department



---

ELLEN ROSENBLUM  
Attorney General  
State of Oregon



---

KATE BROWN  
Governor  
State of Oregon

## Definitions

**Capability Targets** - the performance threshold(s) for each core capability.

**Critical infrastructure** - includes those assets, systems, networks, and functions—physical or virtual—so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.

**Core Capabilities** - distinct critical elements necessary to achieve the National Preparedness Goal.

**Defense Industrial Base** - the worldwide industrial complex sector that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

**Hazard** - a situation that poses a level of threat to life, health, property, or environment.

**Key resources** - publicly or privately controlled resources essential to minimal operation of the economy and the government.

**Resilience** - the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

**Threat** - an indication of possible violence, harm, or danger.

**Sector Partnership Model** - establishes the framework for the public-private cooperation necessary to secure CIKR assets.

**Steady-State operations** - preparedness or readiness activities conducted in the absence of a specific threat or hazard.

## **Glossary of Acronyms**

**BZPP**-Buffer Zone Protection Program  
**CIKR**- Critical Infrastructure and Key Resources  
**CII** – Critical Infrastructure Information  
**CLO**- Community Liaison Program  
**COI** – Community of Interest  
**EMPG** – Emergency Management Program Grant  
**EOD** – Explosive Ordnance Disposal  
**EOP**-Emergency Operations Plan  
**FLO**-Fusion Liaison Officer  
**FOUO** – For Official Use Only  
**GCC** – Governmental Coordinating Counsel  
**HSIN**- Homeland Security Information Network  
**HSPD**- Homeland Security Presidential Directive  
**IP** – Infrastructure Protection  
**IP Gateway** – Infrastructure Protection Gateway  
**IT**-Information Technology  
**LES** – Law Enforcement Sensitive  
**MOU**-Memorandum of Understanding  
**NIPP**-National Infrastructure Protection Plan  
**NGO** – Non Governmental Organization  
**NPG** – National Preparedness Goal  
**NRF** – National Response Framework  
**ODOJ**-Oregon Department of Justice  
**OEM**-Oregon Emergency Management  
**OERS** – Oregon Emergency Response System  
**OMD**-Oregon Military Department  
**OSIPP**-Oregon State Infrastructure Protection Plan  
**OTFC**-Oregon Terrorism Information Threat Assessment Network  
**PCII**- Protected Critical Infrastructure Information  
**PKEMRA** - Post-Katrina Emergency Management Reform Act  
**PSA**- Protective Security Advisor  
**SAVs**-Site Assistance Visits  
**SAA**- State Administrating Agency  
**SBU** – Sensitive But Unclassified  
**SCC** – State Coordinating Counsel  
**SHSGP** – State Homeland Security Grant Program  
**SHSS**-State Homeland Security Strategy

## **Glossary of Acronyms - continued**

**SLTTGCC** – State Local Tribal Territorial Governing Coordinating Counsel

**SPM** – Sector Partnership Model

**SPR**- State Preparedness Report

**SSA**- Sector-Specific Agencies

**SSP**- Sector-Specific Plan

**TCL**- Target Capabilities List

**THIRA** – Threat Hazard Identification and Risk Assessment

**TITAN** – Terrorism Information Threat Assessment Network

**TLO**-Terrorism Liaison Officers

**TRT** – Tactical Response Team

**UASI**-Urban Area Security Initiative

**US DHS**- United States Department of Homeland Security

**WMD** – Weapon of Mass Destruction



## References & Sources

- Critical Infrastructure and Key Resources Support Annexes (January 2008)  
<http://www.US DHS.gov/critical-infrastructure-and-key-resources-support-annex>
- Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level (September 2008)  
[https://www.US DHS.gov/xlibrary/assets/nipp\\_srtltt\\_guide.pdf](https://www.US DHS.gov/xlibrary/assets/nipp_srtltt_guide.pdf)
- Homeland Security Presidential Directive (HSPD) 7 (December 17, 2003)  
<http://www.US DHS.gov/homeland-security-presidential-directive-7>
- National Infrastructure Protection Plan (NIPP)(2013)  
<http://www.US DHS.gov/national-infrastructure-protection-plan>
- National Response Framework (May 2013)  
<https://www.fema.gov/media-library/assets/documents/32230>
- Presidential Policy Directive 21 (PPD-21): Infrastructure Security & Resilience (February 12, 2013)  
<https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- State of Oregon Homeland Security Strategy (SHSS)(2012)  
[http://www.oregon.gov/OMD/OEM/docs/plan\\_train/SHSP/FY2015/Oregon%20-%20SHSS%20-%202012.pdf](http://www.oregon.gov/OMD/OEM/docs/plan_train/SHSP/FY2015/Oregon%20-%20SHSS%20-%202012.pdf)
- State of Oregon Threat Hazard Identification and Risk Assessment (THIRA)(2014)  
[http://www.oregon.gov/OMD/OEM/docs/plan\\_train/SHSP/FY2015/2014%20OREGON%20THIRA.pdf](http://www.oregon.gov/OMD/OEM/docs/plan_train/SHSP/FY2015/2014%20OREGON%20THIRA.pdf)