Washington Statewide Homeland Security Strategic Plan 2006 - 2011

Team Washington

Team Washington: A statewide collaborative partnership

Preface

As the Governor's Homeland Security Advisor, I am pleased to introduce our 2006-11 Washington Statewide Homeland Security Strategic Plan. This has been a year of tremendous change in our nation's approach to Homeland Security and these changes are reflected in this Plan.

I am proud to say that Washington is a recognized leader in homeland security with a statewide all-hazards partnership, known as TEAM WASHINGTON, focused on strengthening domestic security capabilities. Our collaborative efforts have fostered a system of systems capable of responding to major disasters and meeting the expectations of the newly articulated National Preparedness Goal and its associated Target Capabilities. Our work this past year in building Washington's Target Capabilities list has increased our response capabilities and overall level of preparedness.

The Statewide Homeland Security Strategic Plan also guides our progress in meeting the National Preparedness Goals through a mature and established strategic planning process. The strategic planning process provides a framework through which we will strengthen our ability to prevent, defend against, deter, respond to and recover from terrorist attacks as well as natural and technological disasters. It also sets the direction and priorities by which we will measure the results in protecting citizens from the many threats that confront us.

We face the complexity of evolving threats from natural disasters and from stateless groups of terrorists. This plan will provide security, safety and preparedness by effectively coordinating strategies, tactics, information, technology and other resources, including contingency planning, training and multi-disciplinary/multi-jurisdiction exercises.

By following this plan and working together, we can assure preparedness for any contingency and fulfill our commitment and responsibility to each other as citizens of this great State and Nation.

Together we will

"***Ensure a safe and secure State of Washington for the 21st Century.***"

Sincerely,

TIMOTHY J. LOWENBERG
Major General
The Adjutant General
Director, Washington Military Department
Washington Homeland Security Advisor

TABLE OF CONTENTS

SECTION ONE: VISION, MISSION & CORE VALUES

A. Vision

Ensure a safe and secure State of Washington for the 21st Century.

B. Mission

Protect the people, property, environment, culture, and economy of Washington State from acts of terrorism, enhance statewide all-hazards disaster resistance and minimize the effects of a terrorist attack, major disaster or other emergencies.

C. Core Values

- Freedom
- Community Health and Safety
- Economic Prosperity and Quality of Life
- Security – Protect People, Infrastructure and the Environment
- Teamwork – All-Citizen and All-State Focus
- Continuous Improvement
- Ethical Relationships and Management
- Financial Stewardship and Accountability

D. Guiding Principles

- Homeland security and all-hazards emergency preparedness are every citizen's responsibility.
- Prevention can be achieved through an empowered, educated and vigilant citizenry.
- Create response capability through planning, equipping, training and exercising.
- Build core statewide capabilities and augment resources based on assessed threats, vulnerabilities, and impacts - which when combined, reflect risk.
- Achieve safe and effective protections through standardization and interoperability.
- Capacity, once created, must be supported and sustained into the future.
- Washington State will be secure only when our communities are secure.

SECTION TWO: STRATEGIC PLANNING & IMPLEMENTATION OF PRIORITIES

A. Introduction to TEAM WASHINGTON

The vision and collective commitment of TEAM WASHINGTON is to reduce our vulnerabilities and defend against the disasters created by domestic attacks and natural or technological hazards. (For more information on TEAM WASHINGTON, please visit our webpage at: http://www.emd.wa.gov/5-prog/wahsas/wahsas-idx.htm).

Washington State has unique challenges in its more than 66,582-square miles of largely remote terrain, a 325-mile international border with Canada, numerous land and maritime border crossings, and 157-miles of open coastline. Our Team is comprised of a multi-jurisdictional Domestic Security Infrastructure (See Appendix A) consisting of the:

- *Domestic Security Executive Group (DSEG)* - the state government executive level policy and advisory group to advise the Governor on all matters pertaining to state domestic security.

- *Emergency Management Council (EMC)* - Revised Code of Washington (RCW) 38.52.040 established this council to advise the Governor and the Director of Washington Military Department on all matters pertaining to state and local emergency management.

- *Committee on Homeland Security (CHS)* - a subcommittee of the EMC, the CHS develops and recommends statewide homeland security strategies to the EMC.

- *State Interoperability Executive Committee (SIEC)* - a permanent sub-committee of the Information Services Board (ISB), was formed by legislation effective on July 1, 2003 (RCW 43.105.330) in the interests of public safety to pursue and promote statewide interoperability policies and standards.

- *Enhanced 9-1-1* (*E-911) Advisory Committee* – Chapter 38.52 RCW, Revised, established the State E911 Program to coordinate and facilitate the local planning, installation and operation of the E911 phone systems.

- *Regional Homeland Security Coordination Districts (RHSCD)* - The Washington State Homeland Security regional planning and coordination structure is divided into nine regions. The regions are made up of one or more counties that include cities, towns, and tribal nations within the regional geographical boundaries. This regional configuration was implemented to distribute federal grant funds, develop emergency responder equipment priority lists, plan and execute training and exercise programs, create regionally based mutual aid plans, and develop volunteer infrastructure to support citizens' involvement in homeland security initiatives. This regional structure has increased communication and collaboration, to include the sharing of best practices and resource coordination. Operations and physical resources are maintained at the local jurisdiction (county, city and tribal) level, and coordination and planning are facilitated at the regional level. (See Appendix B)

B. Enhancement Plan

In December 200, Washington conducted its first *Program and Capability Review*. Current state levels of capability were evaluated and initiatives developed for implementation over

the next three-five years to strengthen our capabilities. The resulting *Enhancement Plan* works in tandem with the State Homeland Security Strategy and will help the state direct its homeland security activities toward a holistic, interagency, interdisciplinary approach. The Enhancement Plan will assist the state in prioritizing the initiatives it wish to implement using preparedness program funding. The following cross-walk provides additional information on the Enhancement Plan.

2006 ENHANCEMENT PLAN CROSS-WALK
NATIONAL PRIORITIES TO WASHINGTON PRIORITIES, INITIATIVES & OBJECTIVES

NATIONAL PRIORITY	STATE PRIORITY	TARGET CAPABILITY	STATEWIDE INITIATIVE(S)	STATE HOMELAND SECURITY OBJECTIVES
Strengthen CBRNE Detection, Response, and Decontamination capabilities	Prevention	CBRNE Detection, Explosive Device Detection & Response Operations, WMD/Hazardous Materials Response & Decontamination	CBRNE Detection Surveillance and Monitoring, CBRNE HAZMAT Response and Decontamination, Explosive Device Response Operations	5.4.5-5.4.6
Implement the National Incident Management System & National Response Plan	Preparedness & Response, Recovery	Citizen Preparedness Risk Management Planning	NIMS/NRP: 1) NIMS Integration; 2) NRP Implementation; 3) NIMS Resource Management; Law Enforcement Investigation and Operations: 1) Mobilization Plan; 2) Forensic Labs; 3) Operations Plan; 4) Investigation Plan	5.1.1 - 5.6.2, 6.1.1-6.1.3
Expanded Regional Collaboration	Partnership & Planning	Citizen Preparedness Risk Management Planning	Regional Collaboration; Citizen Preparedness: 1) Resources; 2) Public Education; 3) Non-Government Emergency Responders	1.1.1-1.2.2
Implement the Interim National Infrastructure Protection Plan	Protection	Critical Infrastructure Protection, Food & Agriculture Safety and Defense	Critical Infrastructure: 1) Critical Infrastructure Protection Program; Agriculture: 1) Information Management; 2) Laboratory Enhancement; 3) Agricultural Products and Animal Disposal; 4) Surveillance and Inspection; 5) Response Coordination and Integration	4.1.1 - 4.2.5
Strengthen Information Sharing and Collaboration capabilities	Prevention	Intelligence/Information Sharing and Dissemination	Statewide Integrated Intelligence System	3.1.1-3.2.1
Strengthen Interoperable Communications capabilities	Communication	Interoperable Communications, Information Gathering and Recognition of Warnings and Indicators	Interoperable Communications: 1) Regional Committees; 2) Equipment Management; 3) Cyber Infrastructure	2.1.1 - 2.3.2
Strengthen Medical Surge and Mass Prophylaxis capabilities	Health Systems	Mass Prophylaxis, Medical Surge	Medical Surge: 1) Mass Fatality Management and Family Assistance; 2) Resource Sustainment; 3) Exercise Program; 4) Planning Integration; 5) Liability and Credentialing; Mass Prophylaxis: 1) Patient Tracking; 2) Staffing; 3) Resource Management	7.1.1 - 7.2.1

SECTION THREE: PRIORITIES, GOALS, OBJECTIVES AND IMPLEMENTATION STEPS

A. Partnership & Planning: Enhance Statewide, Regional, and Cross-Border Collaboration to Build Partnerships Across Multiple Jurisdictions.

Our goals under this priority include building strong regional partnerships through participation in statewide activities and investment in building capabilities and capacity. Through our annual action plan process, the state updates its strategy and prioritizes the resources required to strengthen the state's ability to prevent, protect, respond and recover from all-hazard events.

This priority incorporates all 36 Target Capabilities and primarily emphasizes the Common Target Capabilities: Planning & Risk Management.

Linked National Priorities:

Expanded Regional Collaboration: Strengthen regionally-based preparedness by focusing finite resources on expanded regional collaboration centered on urban areas with the greatest density of population, critical infrastructure, and other significant risk factors.

Strengthen Interoperable Communications Capabilities: Achieve interoperability not only in terms of communications, but also in the broad ability of systems and organizations to provide service and to accept service from one another across jurisdiction lines, enabling them to operate effectively together.

GOAL 1.1: Build Strong Regional Partnerships

Objective 1.1.1: Enhance statewide, regional, private sector and cross-border partnerships to strengthen prevention capabilities for emerging threats and our capacity to respond to all-hazards events by June 2007.

This objective supports the National Priority "Expand Regional Collaboration" and fosters interstate and intrastate collaboration through the Military Department's efforts to strengthen partnerships with international, federal, state, local, tribal and private sector organizations.

	The Washington Military Department will continue participation in the:	Target
1.1.1.1	Pacific Northwest Emergency Management Arrangement (PNEMA), provides a means to build international and intrastate mutual aid capability in the Pacific Northwest Region.	June 2007
1.1.1.2	Washington Joint Analytical Center (WAJAC), provides an avenue to strengthen statewide intelligence gathering capability for Homeland Security stakeholders.	June 2007
1.1.1.3	Northwest Warn Executive Committee (NWWARN), promotes collaboration on information sharing of significant intelligence information among Homeland Security stakeholders.	June 2007
1.1.1.4	2010 Olympics Task Force Committee, a forum for information and collaboration to prepare Washington State for its role in the 2010 Winter Olympics.	June 2007
1.1.1.5	Regional Technology Integration Initiative (RTII), presents opportunities for the use of technology and new organizational concepts to state and local jurisdictions.	June 2007

Objective 1.1.2: Establish a Washington State Emergency Operations Center – private sector partnership to build a disaster resistant economy and ensure a strong partnership for disaster response and recovery operations by June 2007.

This objective perpetuates and strengthens Emergency Operations Center (EOC) and private sector partnerships for information sharing and helps build a disaster resistant economy.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		**Target**
1.1.2.1	Develop an initiative to include the business community in forthcoming EOC activities via Community Trade and Economic Development (CTED) and Washington State Department of Agriculture (WSDA) participation until a formalized plan is adopted and implemented.	September 2006
1.1.2.2	Assess and analyze options to include the business community, and evaluate alternatives.	November 2006
1.1.2.3	Develop a private sector partnership—communications plan to enhance the ability to build a disaster resistant community and maximize the effectiveness of recovery and response operations.	January 2007
1.1.2.4	EOC and state agency partners implement a private sector—Washington State disaster information sharing plan.	March 2007
1.1.2.5	Educate the private sector and government partners on the information sharing plan and partnership.	June 2007
1.1.2.6	Assess the private sector—Washington State disaster information sharing plan.	September 2007

GOAL 1.2: Plan and Invest to Build Target Capabilities

Objective 1.2.1: Develop and maintain a Homeland Security Statewide Strategic Plan to track our progress toward building Capabilities to support the National Preparedness Goal by March 2007.

This objective links the Planning Target Capability, the foundation on which all other capabilities are developed and enhanced, to the state's Homeland Security efforts. Planning is a mechanism to develop, validate, maintain and track progress in building the 36 Target Capabilities required prevent, protect, respond to and recover from incidents such as those described in the National Planning Scenarios.

The Washington Military Department will lead statewide efforts to:		**Target**
1.2.1.1	Update Homeland Security State Strategic Plan to further align it with the 36 Target Capabilities (version 2.0 or later) and the National Preparedness Goal.	April 2006
1.2.1.2	Provide Balanced Scorecard Progress report for funded objectives.	April 2006
1.2.1.3	Implement action plans and distribute grant funding received (dependent upon receipt of federal funding).	June 2006
1.2.1.4	Publish Homeland Security State Strategic Plan as revised to demonstrate further alignment with the National Preparedness Goal	June 2006

	and the associated 36 Target Capabilities (version 2.0 or later).	
1.2.1.5	Revise Action Plans and prioritization process to further reflect the principles of the National Preparedness Goal, National Priorities and associated target capabilities.	June 2006
1.2.1.6	Revise Action Plan Templates to implement measurable objectives and implementation steps to build target capabilities.	September 2006
1.2.1.7	Revise the Homeland Security Strategic Plan based upon published guidance and submit to the Department of Homeland Security.	September 2006
1.2.1.8	Revise Strategic Plan Objectives and Supporting Action Plans.	September 2006
1.2.1.9	Conduct Strategy Working Group Meetings to revise State Strategic Plan.	September 2006
1.2.1.10	Prioritize Action Plans to maximize the investment of Homeland Security resources in building capabilities.	December 2006
1.2.1.11	Provide input to the Program and Capabilities Review and continuing development of the statewide Enhancement Plan and initiatives	December 2006
1.2.1.12	Partner with a statewide stakeholder group to review 2007 Grant Guidance, draft and publish state grant guidance (see Objective 1.2.2)	January 2007
1.2.1.13	Provide Briefings on Action Plan Prioritization and gain approval of Domestic Security Infrastructure stakeholders.	March 2007
1.2.1.14	Provide Briefings on Action Plan Prioritization for funding requests and gain approval of Domestic Security Infrastructure stakeholders.	March 2007

Objective 1.2.2: Implement an effective methodology to assure visibility/ tracking of Homeland Security funding, maximize investments and sustain capabilities by March 2007.

This objective addresses a need for statewide coordination to ensure effective and efficient investment in the state's homeland security resources, maximize the Homeland Security Funding to local jurisdictions and to sustain the capabilities built... In addition, the objective addresses the need for state grant guidance that describes the process for developing and linking: the state strategic plan, action plans, program and capabilities review, the state enhancement plan, investment justifications, contracts awarding grant funding and sub-receipt award expectations.

The Washington Military Department, Emergency Management Division will lead statewide efforts to:		**Target**
1.2.2.1	Review program and capabilities documents distributed by Department of Homeland Security.	January 2007
1.2.2.2	Conduct a review of statewide Homeland Security Program and Target Capability development.	January 2007
1.2.2.3	Create statewide grant guidance in and publish to stakeholders by using a timely and transparent peer review workgroup.	January 2007
1.2.2.4	Create an Enhancement Plan to illustrate implementation of the state strategy through statewide initiatives.	March 2007

B. Communication: Strengthen and Safeguard Our Public Safety Information Systems.

The three goals under this priority promote communications interoperability by establishing a governance structure, creating standard operating procedures (SOPs), implementing a statewide technology structure, and defining usage standards through a comprehensive training and exercise program; utilize technology to gather and share information to support regional partnerships and established alert and warning systems throughout the state; and protect information sharing and communications systems.

Linked National Priorities:

Strengthen Interoperable Communications Capabilities: Achieve interoperability not only in terms of communications, but also in the broad ability of systems and organizations to provide service and to accept service from one another across jurisdiction lines, enabling them to operate effectively together.

Expanded Regional Collaboration: Strengthen regionally-based preparedness by focusing our finite resources on expanded regional collaboration centered on urban areas with the greatest density of population, critical infrastructure, and other significant risk factors.

This priority incorporates all 36 Target Capabilities and primarily emphasizes the Common Target Capabilities: Interoperable Communications & Risk Management.

GOAL 2.1: Promote Communications Interoperability

Objective 2.1.1: Implement a governance structure for Interoperable Communications by June 2007.

This objective provides a method for establishing and sustaining a common governance structure to address interoperability issues. It also enhances communication coordination and cooperation, establishes guidelines and principles and reduces internal jurisdictional conflicts during incident response operations.

The State Interoperability Executive Committee will lead statewide efforts to:		**Target**
2.1.1.1	Identify and implement a governance structure that will coordinate and enable interoperable communications between state, regional, local, tribal and federal governments.	June 2007
2.1.1.2	Establish polices and guidelines to enable decision making and coordination for a phased migration to a standards based, opened architecture infrastructure that establishing a fully interoperable radio system.	June 2007
2.1.1.3	Enhance interoperable communications by identifying and designating a lead agency that will be responsible and accountable for: ▪ Developing and managing the system. ▪ Managing and controlling the shared infrastructure and processes associated with interoperable communications within state agencies ▪ Managing the fiduciary aspects of the proposed system, including funding, operational costs, and cost recovery mechanisms.	June 2007

Objective 2.1.2: Create a series of standard operating procedures (SOPs) for statewide interoperable communications by October 2007.

This objective creates a series of standard operating procedures (SOPs) that will act as formal written guidelines or instructions for statewide interoperable communications.

The State Interoperability Executive Committee will lead statewide efforts to:		Target
2.1.2.1	Review existing SOPs for updates and develop new SOPs as appropriate.	April 2007
2.1.2.2	Ensure that all SOPs follow Incident Command System (ICS)/National Incident Management System (NIMS) standards	July 2007
2.1.2.3	Coordinate with Technical Working Group as appropriate to include technical guidelines and checklists into written plans.	October 2007

Objective 2.1.3: Implement a technology structure for statewide interoperable communications by June 2011.

This objective builds a frequency and technology neutral statewide radio system.

The State Interoperability Executive Committee will lead statewide efforts to:		Target
2.1.3.1	Lead agency will meet with Regional Homeland Security Coordinators to determine the need and location of radio caches in their region.	May 2007
2.1.3.2	SIEC will determine state agency that will accept deed of the equipment. (Agency would also be responsible for continuing maintenance of equipment.).	July 2007
2.1.3.3	Selected state agency, responsible for owning and maintaining radio caches, will determine with Homeland Security Regional Coordinators the best location to house the equipment.	August 2007
2.1.3.4	Purchase radio caches to be deployed, at agreed to locations, in Homeland Security Regions.	September 2007
2.1.3.5	MOUs with agencies that may use equipment will be signed.	November 2007
2.1.3.6	Regions will be asked to conduct training program on the proper use and how to request equipment.	November 2007
2.1.3.7	SIEC will conduct an exercise using pre-positioned radio caches (please see Action Plan 13, Section 2.1.4 for additional information).	February 2008
2.1.3.8	Homeland Security Regions will be encouraged to use radio caches in their exercises.	June 2011

Objective 2.1.4: Develop and implement statewide interoperable communications training and exercises by November 2007.

This objective transforms the On Scene Command and Control Radio (OSCCR) Channel into the statewide interoperability channel.

The State Interoperability Executive Committee will lead statewide efforts to:		Target
2.1.4.1	Training material for the OSCCR deployment developed.	March 2008
2.1.4.2	State level OSCCR training begins.	April 2008
2.1.4.3	The Interoperable Communications Technical Assistance Program (ICTAP), working in concert with the SIEC, will design a tabletop exercise for the OSCCR Radio Network.	June 2008
2.1.4.4	Conduct OSCCR Tabletop exercise and complete an after action report.	August 2008
2.1.4.5	SIEC will work with partner agencies to determine next scenario for table top exercise based on lessons learned.	November 2008

Objective 2.1.5: Deploy interoperable equipment and sustain usage by state agencies and local governments by September 2011.

This objective supports the deployment of a fully interoperable radio system with rules of use that ensure NIMS Compliance. The first step is implementation of the On Scene Command and Control Radio (OSCCR).

The State Interoperability Executive Committee will lead statewide efforts to:		Target
2.1.5.1	Complete OSCCR Implementation Phase I.	March 2007
2.1.5.2	Complete Phase I of statewide network implementation.	September 2007
2.1.5.3	Complete OSCCR Implementation Phase II.	June 2008
2.1.5.4	Complete OSCCR Implementation Project.	August 2008

GOAL 2.2: Gather and Share Information in Support of Regional Partnerships

Objective 2.2.1: Maintain effective statewide emergency public safety communications networks to share threats advisories, information and emergency procedures by December 2007.

This objective strengthens a number of alert and warning systems in the State Emergency Operations Center, including: NAWAS, EAS, CEMNET, WebEOC, and PIER.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		Target
2.2.1.1	Review the statewide interoperable public safety emergency information sharing network for updates and system gaps.	June 2006
2.2.1.2	Review and procure funding for the Comprehensive Emergency Management Network (CEMNET) life cycle replacement costs.	June 2006

2.2.1.3	Acquire necessary resources to implement the statewide interoperable public safety emergency information sharing network.	June 2006
2.2.1.4	Procure necessary hardware and software to deploy an operational capability for the information sharing network.	October 2006
2.2.1.5	Identify and refine emergency information to be collected and shared and examine best practices on the distribution of information.	December 2006
2.2.1.6	Develop training and education materials for the information sharing network.	December 2007
2.2.1.7	Conduct training and education for fielding the information sharing network.	December 2007
2.2.1.8	Continue to assess information sharing network status and revise plans/capabilities.	December 2007

Objective 2.2.2: Develop information sharing templates and parameters for exchange of information by June 2009.

This objective provides information-sharing templates for exchange of public safety information which is accomplished by: 1) expanded use of WebEOC both in state agencies and local governments responsible for public safety; 2) refinement of the 172 existing templates to satisfy operational needs; 3) establishment of a WebEOC training program; and 4) the development of a communications exercise that focuses on the use of the templates provided in WebEOC.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		**Target**
2.2.2.1	Add an additional FTE staff to assist existing FTE in the statewide WebEOC information sharing development.	December 2006
2.2.2.2	Continue to refine and identify new WebEOC templates to share information.	December 2006
2.2.2.3	Develop generic WebEOC information sharing templates and standard operating procedures.	December 2006
2.2.2.4	Modify applicable emergency management operational plans to incorporate templates and procedures.	June 2007
2.2.2.6	Develop and conduct training for sharing information across state public safety networks.	June 2007
2.2.2.7	Develop and conduct WebEOC communications exercises to test the sharing of information across jurisdictions.	June 2007
2.2.2.8	Develop and conduct training for sharing information across state public safety networks.	June 2009
2.2.2.9	Develop and conduct WebEOC communication exercises to test the sharing of information across jurisdictions.	June 2009

Objective 2.2.3: Develop and formalize an information sharing architecture to facilitate statewide efforts to prevent, protect, respond to and recover from incidents such as those described in the National Planning Scenarios by June 2007.

This objective formalizes an information sharing architecture to prevent, protect, respond to and recover from incidents such as those described in the National Planning Scenarios.

The Washington Military Department will lead statewide efforts to:		**Target**
2.2.3.1	Identify mechanisms to provide crisis communication messages that would reach hearing impaired population and extend across language barriers and be incorporated into the key messages in the Agency Communications Plan.	June 2006
2.2.3.2	Review and update information sharing systems based on lessons learned.	January 2007
2.2.3.3	Review and update list of interdepartmental resources that can back each other up in a multi-incident information sharing events.	March 2007

Objective 2.2.4: Develop a best practice and lessons learned sharing information system to share information throughout the state by June 2008.

This objective develops a web-based collection network for the state to gather and share best practices to strengthen statewide ability to prevent, protect, respond to and recover from all-hazards events.

The Washington State Emergency Management Association (WSEMA) will lead statewide efforts to:		**Target**
2.2.4.1.	Develop a web based tool to launch a best practices and lessons learning information sharing system for TEAM WASHINGTON Homeland Security stakeholders.	June 2007
2.2.4.2.	Link the web based best practices and lessons learned information sharing system to the TEAM WASHINGTON and WSEMA web pages.	June 2007
2.2.4.3	Establish a process for reviewing information submitted by stakeholder (gatekeepers) to ensure appropriate content is posted to the web based tool.	June 2008
2.2.4.4	Develop information sharing protocols across all tiers of government and private sector, which specifies dissemination to the lowest organizational level possible to ensure that all stakeholders will receive appropriate information from the tool.	June 2008

GOAL 2.3: Protect Information Sharing and Communications Systems

Objective 2.3.1: Refine existing systems to improve the statewide cyber network and cyber preparedness capabilities by June 2011.

This objective provides a statewide Cyber Protection and Preparedness capability for state, county, and local government.

Cyber Exercises

The Washington Department of Information Services will lead statewide efforts to:		Target
2.3.1.1.1	Recruit participation from state, county, and local governments.	February 2006
2.3.1.1.2	Define acquisition criteria for scenario exercise modeling tool.	February 2006
2.3.1.1.3	Acquire exercise modeling tool.	March 2006
2.3.1.1.4	Design cyber exercises state, local, and regional organizations.	May 2006
2.3.1.1.5	Conduct and/or participate in statewide and regional cyber exercises	July 2006
2.3.1.1.6	Evaluate results and apply improvements	September 2006

Cyber Penetration Testing

The Washington Department of Information Services will lead statewide efforts to:		Target
2.3.1.2.1	Solicit penetration testing participants	January 2006
2.3.1.2.2	Identify penetration testing requirements.	February 2006
2.3.1.2.3	Design penetration testing environment.	April 2006
2.3.1.2.4	Acquire and install penetration testing equipment and systems	May 2006
2.3.1.2.5	Conduct penetration tests with participants	July 2006
2.3.1.2.6	Review results and apply improvements	September 2006

Cyber Security Technology

The Washington Department of Information Services will lead statewide efforts to:		Target
2.3.1.3.1	Identify Network Admission Control system, Log Storage and Search system, and Intrusion Prevention System requirements.	May 2006
2.3.1.3.2	Acquire Network Admission Control system, Log Storage and Search system, and Intrusion Prevention Systems.	July 2006
2.3.1.3.3	Install Network Admission Control system, Log Storage and Search system, and Intrusion Prevention Systems.	September 2006
2.3.1.3.4	Utilize Network Admission Control system, Log Storage and Search system, and Intrusion Prevention Systems in cyber exercise.	November 2006
2.3.1.3.5	Evaluate level of increased security.	December 2006

Cyber Communication Processes & Systems

The Washington Department of Information Services will lead statewide efforts to:		Target
2.3.1.4.1	Review physical & cyber incident response plans.	April 2006
2.3.1.4.2	Develop cyber/physical crosswalk for incident response plans	May 2006
2.3.1.4.3	Identify incident communication system requirements.	July 2006

2.3.1.4.4	Acquire incident communication system requirements.	September 2006
2.3.1.4.5	Implement incident communication system requirements.	October 2006
2.3.1.4.6	Use NIMS to test and evaluate processes and procedures.	November 2006

Cyber Security Education

The Washington Department of Information Services will lead statewide efforts to:		**Target**
2.3.1.5.1	Identify cyber security education and awareness training requirements	October 2006
2.3.1.5.2	Acquire cyber security education and awareness training system	December 2006
2.3.1.5.3	Install cyber security education and awareness training system	January 2007
2.3.1.5.4	Test and evaluate cyber security education and awareness training system	February 2007

Objective 2.3.2: Refine existing cyber infrastructure to improve continuity of statewide information sharing and communications systems and mitigate the effects of disruption from terrorist or natural disasters by January 2010.

This objective enhances the statewide telecommunications infrastructure that provides continuous operation of the State Government Network (SGN).

The Washington Department of Information Services will lead statewide efforts to:		**Target**
2.3.2.1	Implement hierarchical model for core network.	December 2005
2.3.2.2	Implement Virtual Firewall technology	June 2006
2.3.2.3	Extend Virtual Firewall technology to Eastern Washington	September 2006
2.3.2.4	Establish Eastern Washington ISP connection	September 2006
2.3.2.5	Establish Eastern Washington Internet gateway images	December 2006
2.3.2.6	Assess additional technology and security requirements to build the plan for next phase of telecommunications, security and computing capacity.	January 2008
2.3.2.7	Deploy technology and security solutions resulting from year three assessment.	June 2009
2.3.2.8	Reassess enterprise information technology and cyber needs and update plans	January 2010

CH-47 Helicopters from the 66th Aviation Brigade conducting relief operations in Pakistan

Photo courtesy of the Washington National Guard

C. Prevention: Strengthen Intelligence, Information Sharing Among Public and Private Sector Entities

This priority has two objectives to support the goal of a statewide integrated intelligence system: First, implement a statewide integrated intelligence plan and sustain the Washington Joint Analytical Center (WAJAC). Second, establish an intelligence sub-committee within the state domestic security infrastructure to coordinate and facilitate statewide prevention efforts.

This priority focuses on the Prevent Mission Area Target Capabilities: Information Gathering and Recognition of Indicators and Warnings, Intelligence Analysis and Production, Intelligence/Information Sharing and Dissemination, Law Enforcement Investigation and Operations and CBRNE Detection.

Linked National Priorities:

Strengthen Information Sharing and Collaboration Capabilities: Establishing prevention frameworks based on expanded regional collaboration that are linked in a national network will facilitate efforts to achieve information sharing and collaboration capabilities.

Expanded Regional Collaboration: Strengthen regionally-based preparedness by focusing our finite resources on expanded regional collaboration centered on urban areas with the greatest density of population, critical infrastructure, and other significant risk factors.

GOAL 3.1: Establish a Statewide Integrated Intelligence System

Objective 3.1.1: Establish a statewide integrated intelligence system for all local, state and federal law enforcement agencies operating within the State of Washington by June 2011.

This objective implements a statewide integrated intelligence plan and supports sustainment of the Washington Joint Analytical Center (WAJAC).

The Washington State Patrol will lead statewide efforts to:		Target
3.1.1.1	Research and identify operational procedures and policies for WAJAC and regional intelligence groups.	June 2007
3.1.1.2	Research and identify current and future technological and equipment needs for WAJAC and regional intelligence groups.	June 2007
3.1.1.3	Develop training curriculum for intelligence analysts, intelligence detectives, and intelligence managers and commanders.	June 2007
3.1.1.4	Establish performance measures and reporting procedures for WAJAC and regional intelligence groups.	June 2007
3.1.1.5	Continue to develop support for the WAJAC Advisory Board.	June 2007
3.1.1.6	Solicit support from WASPC members for participation in WAJAC and regional intelligence groups.	June 2007
3.1.1.7	Coordinate intelligence collection processes and disseminate threat assessments, advisory bulletins, and intelligence trends from WAJAC to stakeholders.	June 2007
3.1.1.8	Provide NWWARN training to public and private sector.	June 2007
3.1.1.9	Provide training to stakeholders regarding the Western State Information Network (WSIN) all crimes pilot project database.	June 2007
3.1.1.10	Establish a sustainable funding source for the positions assigned to WAJAC and the regional intelligence groups.	June 2007
3.1.1.11	Seek funding sources for overtime costs for personnel to participate in investigative and intelligence sharing activities specifically related to homeland security.	June 2007
3.1.1.12	Solicit user feedback regarding future requirements for WAJAC and regional intelligence groups.	June 2009
3.1.1.13	Continue to evaluate WSIN all crimes database for continued intelligence use.	June 2009
3.1.1.14	Develop a secure computerized storage system to support intelligence collection, collation, mapping, analysis, and dissemination.	June 2009
3.1.1.15	Update and refine intelligence's role in the identification and threat assessment rating of critical infrastructures.	June 2009
3.1.1.16	Evaluate effectiveness of established performance measures for WAJAC and regional intelligence groups.	June 2009
3.1.1.17	Identify resources to maintain one lieutenant, one sergeant and six intelligence detectives in the WAJAC. Identify the resources to support regional intelligence groups.	June 2009

3.1.1.18	Evaluate support for WAJAC, regional intelligence groups, and JTTFs. Adjust resources as necessary to meet current and future needs.	June 2011

Objective 3.1.2: Establish an intelligence sub-committee within the state domestic security infrastructure to coordinate and facilitate statewide prevention efforts by June 2011.

This objective establishes a prevention sub-committee within the state domestic security infrastructure to assist in the coordination and facilitation of statewide prevention efforts.

The Washington State Patrol will lead statewide efforts to:		**Target**
3.1.2.1	Identify and analyze current activities occurring within the state to determine coordinated, successful priorities. Examples include the usage of WSIN for an intelligence pointer system; LinX for incident based law enforcement and NWWARN for dissemination of intelligence/threat information.	June 2007
3.1.2.2	Identify and select additional subject matter experts (SMEs) for the intelligence committee that integrates a wider more diversified group of experts in prevention.	June 2006
3.1.2.3	Select a sub-committee co-chair from law enforcement.	June 2006
3.1.2.4	Select a sub-committee co-chair from the private sector.	June 2006
3.1.2.5	Organize and build effective collaborations among all private and public sector entities operating within the state's homeland security structure.	June 2007
3.1.2.6	Recommend strategic priorities and operational initiatives to improve statewide efforts.	June 2009
3.1.2.7	Continue to evaluate current terrorism prevention initiatives for continued improvement.	June 2009
3.1.2.8	Continue to evaluate current terrorism prevention initiatives for continued improvement.	June 2011

Objective 3.1.3: Establish intelligence system partnerships and define state roles, responsibilities and actions to improve the northern border area security by June 2010.

This objective focuses on security planning for events that affect the security of the state's northern border, such as the 2010 Winter Olympics in British Columbia, Canada.

The Washington State Patrol will lead statewide efforts to:		**Target**
3.1.3.1	Participate in event planning for the 2010 Olympics Task Force to improve northern border area security.	June 2010
3.1.3.2	Seek opportunities for cross-border information sharing to establish prevention strategies	June 2010
3.1.3.3	Enhance cross-border partnerships to strengthen prevention measures	June 2010

Border patrol agents co-located with Coast Guard Station Bellingham patrol together near the city of Bellingham.

Photo Courtesy of the United States Coast Guard, 13th District, Seattle, Washington

D. Protection: Implement the Interim National Infrastructure Protection Plan.

The two goals under this priority are to develop and sustain an infrastructure protection program and an agricultural specific protection program. Most of the state's critical infrastructure is owned by private entities. Private sector participation in these programs is voluntary but vital to protecting the state's economy and business interests.

This priority focuses on the Protect Mission Area Target Capabilities: Critical Infrastructure Protection (CIP) and Food and Agricultural Safety and Defense.

Linked National Priority:

Implement the National Infrastructure Protection Plan: Strengthen capabilities to protect high traffic borders, ports, public transit systems, and other high priority critical infrastructure both interstate and intrastate.

Expanded Regional Collaboration: Strengthen regionally-based preparedness by focusing our finite resources on expanded regional collaboration centered on urban areas with the greatest density of population, critical infrastructure, and other significant risk factors.

GOAL 4.1: Develop and Sustain an Infrastructure Protection Program

Objective 4.1.1: Develop a statewide infrastructure protection program by June 2008.

This objective details the steps for implementation of the Washington State Infrastructure Protection Program.

The Washington Military Department, Emergency Management Division will lead statewide efforts to:		**Target**
4.1.1.1	Identify Critical Infrastructure within Washington State through public and private sector partnerships.	March 2006
4.1.1.2	Provide the Department of Homeland Security an initial data list of identified critical infrastructure within Washington for the National Assets Database.	March 2006
4.1.1.3	Complete design and population of the statewide Critical Infrastructure Database.	March 2006
4.1.1.4	Identify statewide stakeholders and partnerships that would help facilitate critical infrastructure identification and protection planning.	June 2006
4.1.1.5	Develop an information archiving capacity for Critical Infrastructure (CI)/Key Resources (KR) and Buffer Zone Protection Plan (BZPP) data.	June 2006
4.1.1.6	Develop the capacity and acquire the resources to store and manipulate the CI/KR data in written and geospatial terms.	June 2006
4.1.1.7	Conduct/gather vulnerability analysis.	December 2006
4.1.1.8	Develop a clearing house for CI/KR and BZPP "best practices".	December 2006
4.1.1.9	Locate, map, score, validate, prioritize and vet critical infrastructure data.	June 2007
4.1.1.10	Provide the Department of Homeland Security further refined data list of identified critical infrastructure within Washington State for the NADB correcting current national database contents.	June 2007
4.1.1.11	Collect vulnerability assessment data and information.	June 2007

4.1.1.12	Identify potential critical infrastructure protection strategies with the assessed infrastructure.	June 2007
4.1.1.13	Locate, map, score, validate, and prioritize additional critical infrastructure data.	December 2007
4.1.1.14	Provide the Department of Homeland Security further refined data list of identified critical infrastructure within Washington State for the NADB correcting current national database contents.	December 2007
4.1.1.15	Develop the capacity and acquire the resources to store and manipulate the CI/KR data in written and geospatial terms.	December 2007
4.1.1.16	Work to develop a statewide protected information sharing methodology for critical infrastructure.	December 2007
4.1.1.17	Following vulnerability analysis identify risk associated with critical infrastructure.	December 2007
4.1.1.18	Collect additional vulnerability assessment data and information.	December 2007
4.1.1.19	Identify potential critical infrastructure protection strategies with the assessed infrastructure.	December 2007
4.1.1.20	Find funding mechanism for protection strategies.	December 2007
4.1.1.21	Prioritize infrastructure and create (coordinate and write the state infrastructure) protection plan.	June 2008
4.1.1.22	Reassess and adjust plans (ongoing).	June 2008

Objective 4.1.2: Identify and collect statewide Chemical/Hazardous Material (HAZMAT) site information by August 2007.

This project enables Ecology, on behalf of the State Emergency Response Commission (SERC), to collect and provide more meaningful and valuable chemical storage data for facilities throughout the state.

The Washington Department of Ecology will lead statewide efforts to:		**Target**
4.1.2.1	Redesign and test EPCRA Tracking System and auxiliary applications by March 2006.	March 2006
4.1.2.2	Implement change to chemical inventory reporting requirements (update publications, web sites, forms and instructions).	March 2006
4.1.2.3	Provide Emergency Planning and Community Right to Know Act (EPCRA) workshops in partnership with the Environmental Protection Agency (EPA) and Local Emergency Planning Committees (LEPC) statewide.	February 2007
4.1.2.4	Provide ongoing technical support and education.	June 2007
4.1.2.5	Perform analysis, determine system requirements, develop specifications, and create a project management plan for on-line reporting system development.	June 2007
4.1.2.6	Budget / fund system development.	July 2007
4.1.2.7	Procure contractor to perform services.	July 2007
4.1.2.8	Implement project management plan.	August 2007

The beautiful Columbia River in Eastern Washington

Photo courtesy of Access Washington

Objective 4.1.3: Develop a statewide first responder/critical incident mapping information system which will lead to the creation of Buffer Zone Protection Plans by June 2011.

This objective creates a statewide first responder/critical incident mapping information system that will provide first responders with the information they need to be successful when disasters occur. All privately, federally, and tribally owned buildings/infrastructures may voluntarily participate in this program.

The Washington Association of Sheriffs and Police Chiefs (WASPC) will lead statewide efforts to:		**Target**
4.1.3.1	Complete mapping of all middle and elementary schools.	June 2007
4.1.3.2	Determine the order in which schools, other local and state governmental facilities, and private sector facilities should be mapped.	June 2007
4.1.3.3	Expand current standards committee to assist in the development of guidelines for a mapping system for federal, tribal, and private sector critical infrastructures.	June 2009
4.1.3.4	Determine order in which public and private sector critical infrastructures should be mapped and/or resources provided for creation of Buffer Zone Protection Plans.	June 2009
4.1.3.5	Creation of incident response plans for critical infrastructures.	June 2009
4.1.3.6	Creation of Buffer Zone Protection Plans for critical infrastructures.	June 2009
4.1.3.7	Develop guidelines on how mapping information shall be made available to partner agencies.	June 2009
4.1.3.8	Develop training guidelines for use of the mapping information system.	June 2009
4.1.3.9	Budget / finance continued mapping and development of protection plans.	June 2011
4.1.3.10	Continue mapping and development of Buffer Zone Protection Plans for critical infrastructures.	June 2011
4.1.3.11	Evaluate support for public and private sector organizations in the continued mapping and development of Buffer Zone Protection Plans.	June 2011

Objective 4.1.4: Develop statewide geospatial mapping and database capabilities, based on the Washington Geographic Information Council (WAGIC) Framework by June 2010.

This objective develops a geospatial infrastructure database and applications to map critical infrastructure.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		**Target**
4.1.4.1	Manage development of initial Homeland Security Infrastructure geospatial database applications.	June 2006
4.1.4.2	Establish a Interagency Agreement with Thurston County to provide ArcIMS support.	June 2006
4.1.4.3	Annually review the collected and updated infrastructure data from data stewards.	December 2006
4.1.4.4	Provide support to WAGIC in efforts to establish enterprise GIT architecture for orthoimagery, hydrology & transportation frameworks	June 2007
4.1.4.5	Identify additional users and their needs.	June 2007
4.1.4.6	Manage continued application enhancements to meet user needs.	June 2007
4.1.4.7	Annually report resource requirements during each budget cycle	March 2007
4.1.4.8	Annually review the collected and updated infrastructure data from data stewards.	December 2007
4.1.4.9	Provide for secure access of geospatial data by authorized users through the Internet, when budget support is obtained.	December 2007
4.1.4.10	Annually report resource requirements during each budget cycle	March 2008
4.1.4.11	Convert geospatial data from shapefile to ArcSDE to support faster access from Internet, when budget support is obtained	July 2008
4.1.4.12	Annually review the collected and updated infrastructure data from data stewards.	December 2008
4.1.4.13	Reevaluate program requirements	July 2010

Objective 4.1.5: Increase the security of Washington's statewide transportation systems and support federal transportation system initiatives through vigilant and effective screening of our ferry, highway, and railway and aviation networks by July 2007.

This objective seeks to increase the security of the Washington State Ferry (WSF) system, largest marine mass transportation system in United States and second largest worldwide.

The Washington State Patrol will lead statewide efforts to:		**Target**
4.1.5.1	Review existing law enforcement mutual aid contracts (annual)	Ongoing
4.1.5.2	Operational capability in support of MARSEC 2.	July 2006
4.1.5.3	Educate and train local law enforcement agencies on ferry incident response.	July 2007

4.1.5.4	Support equipment requests for Washington State Patrol Divisions and local law enforcement that support ferry security.	July 2007
4.1.5.5	Ensure that all tactical responses to ferry incidents are coordinated with Washington State Patrol VATS and SWAT.	July 2007
4.1.5.6	Ensure that all bomb threat responses to ferry incidents are coordinated with Washington State Patrol VATS and SWAT.	July 2007

GOAL 4.2: Develop an Agricultural Protection Program

Objective 4.2.1: Develop and implement effective agricultural protection and agri-terrorism prevention plans by June 2009.

This objective assists agricultural organizations in conducting risk and vulnerability assessments and developing comprehensive prevention and response plans for key agricultural infrastructure.

The Washington State Department of Agriculture (WSDA) will lead statewide efforts to:		**Target**
4.2.1.1	Assess Washington State agriculture preparedness and protection plans, strengths, effectiveness and efficiency.	December 2006
4.2.1.2	Review existing plans, perform gap analysis, and develop or modify when necessary to align the WSDA response capability with the Target Capability List.	December 2006
4.2.1.3	Partner with the agricultural industry, all levels of government, and educational institutions to address issues/actions.	January 2007
4.2.1.4	Ensure appropriate state laws, policies and procedures support preparedness, prevention, response, and recovery requirements for legislative initiatives for the Legislative Session 2007.	January 2007
4.2.1.5	Conduct risk assessment activities to support the prevention of, response to, and recovery from an agricultural incident or event to ensure the critical infrastructure is identified as part of the National Asset Database.	March 2007
4.2.1.6	In partnership with state and federal agencies, the agricultural industry, and stakeholders, develop and implement a homeland security public prevention education and information outreach program to educate Washington State agriculture to support prevention, response, and recovery from an agricultural incident, either natural, technological, or terrorism.	June 2009

Objective 4.2.2: Strengthen agricultural laboratory capabilities by June 2011.

This objective upgrades equipment in Washington State Department of Agriculture (WSDA) laboratories to increase state laboratory capability and capacity to identify potential agricultural threats and/or outbreaks.

The Washington Department of Agriculture will lead statewide efforts to:		Target
4.2.2.1	Modernize, add safe/secure facilities, and update equipment/ processes of the agricultural labs in the state of Washington.	June 2009
4.2.2.2	Integrate state and university diagnosis laboratory capabilities to address capacity, turnaround times and quality control to ensure standardized results; equipment or upgrade as needed.	June 2009
4.2.2.3	Provide increased capability for human and animal disease in case of loss of other lab facilities (e.g. diversification and replication of facilities insures capacity and capability across state).	June 2009
4.2.2.4	Decrease turnaround time with dependable results in case of contagious disease.	June 2009

Objective 4.2.3: Strengthen WSDA staff ability to assess terrorism prevention, provide incident response, and perform incident recovery in partnership with the private sector, volunteer organizations, and federal, state, and local agencies by December 2009.

This objective outlines the plan for equipping, training and exercising Washington State Department of Agriculture (WSDA) responders and procedures to ensure a timely respond to an agricultural incident anywhere in the state and effective coordination with neighboring states and provinces utilizing the National Incident Management System.

The Washington Department of Agriculture will lead statewide efforts to:		Target
4.2.3.1	Develop training package for WSDA communications equipment.	June 2006
4.2.3.2	Plan and conduct a Food Safety workshop and tabletop exercise to include WSDA staff, volunteers, and industry.	November 2006
4.2.3.3	Review and update equipment requirements as the technology and mission evolve.	December 2006
4.2.3.4	Continue the implementation of the training plan to bring WSDA responders to the operations level.	December 2006
4.2.3.5	Continue implementation of the National Incident Management System.	December 2006
4.2.3.6	Plan and conduct at least three information and/or education events for volunteer organizations and the agricultural industry.	December 2006
4.2.3.7	Plan, train, and conduct a communications exercise	December 2006
4.2.3.8	Continue the implementation of the training plan to bring WSDA responders to the intermediate level for agricultural incidents.	July 2007
4.2.3.9	Provide refresher training on WSDA response equipment.	December 2007
4.2.3.10	Review and update equipment requirements as the technology and mission evolve.	December 2007
4.2.3.11	Plan and conduct a workshop and a tabletop exercise	June 2008
4.2.3.12	Continue the implementation of the training plan to bring WSDA responders to the advanced level for agricultural incidents.	October 2008

4.2.3.13	Review and assess adequacy of individual training programs	December 2008
4.2.3.14	Review and update equipment requirements as the technology and mission evolve.	December 2008
4.2.3.15	Plan and conduct a tabletop and a full-scale exercise to include volunteer organizations and the agricultural industry.	December 2008
4.2.3.16	Complete investigator training program for WSDA response staff.	December 2008
4.2.3.17	Develop a training sustainment plan that ensures WSDA responders are trained for agricultural incidents.	July 2009
4.2.3.18	Plan and conduct a seminar and a tabletop exercise	July 2009
4.2.3.19	Review and update equipment requirements as the technology and mission evolve.	December 2009
4.2.3.20	Conduct full-scale exercise	December 2009

Objective 4.2.4: Develop, enhance and implement USDA- and FDA-compatible animal, food, and commodity tracking systems to support Washington State Health Officials by July 2009.

This objective develops a prevention tool; establishes a state-wide inventory of food, animal feed and animal premises; and enables targeted education in prevention techniques and programs.

The Washington Department of Agriculture will lead statewide efforts to:		**Target**
4.2.4.1	Complete 1st year education and registration effort for premises not in existing state databases.	January 2006
4.2.4.2	Begin individual and group animal identification using national system.	January 2006
4.2.4.3	Purchase and deploy hand-held computers/laptops to field inspectors.	May 2006
4.2.4.4	Pilot Program in place – track inspection progress against applicable grading standards (ongoing).	July 2006
4.2.4.5	Continue premise education and registration effort for 2nd year.	August 2006
4.2.4.6	Complete Pilot Program.	June 2007
4.2.4.7	Develop education material for all dealers to prevent any distribution to wrong parties (ongoing).	June 2007
4.2.4.8	Inspect fertilizer storage facilities for proper security measures and appropriate containment (ongoing).	September 2007
4.2.4.9	Inspect feed establishments to ensure there are adequate safeguard against receiving contaminated products and protection to minimize chance of contamination in the facilities and adequate information for recall, if needed.	September 2007
4.2.4.10	Expand Pilot Program to all commodity field inspections.	December 2007
4.2.4.11	Develop Animal Tracking System.	January 2008
4.2.4.12	Analyze the vulnerability assessment of the agricultural community (feed and fertilizer establishments) to terrorist activities.	July 2008
4.2.4.13	Maintain & upgrade system to enhance traceability.	December 2008

4.2.4.14	Continue premise education, registration effort, and movement reporting (ongoing).	July 2009
4.2.4.15	Maintain & upgrade system to enhance traceability (ongoing).	July 2009
4.2.4.16	Inspect fertilizer storage facilities for proper security measures and appropriate containment (ongoing).	July 2009
4.2.4.17	Inspect feed establishments to ensure there are adequate safeguard against receiving contaminated products and protection to minimize chance of contamination in the facilities and adequate information for recall, if needed (ongoing).	July 2009
4.2.4.18	Distribute education material for all dealers to prevent any distribution to any wrong parties (ongoing).	July 2009

Objective 4.2.5: Revise agency program vector control policies, procedures and operations to ensure WSDA has the capabilities to identify, control, contain and/or eradicate pest- and disease-spreading organisms by June 2007.

This objective facilitates an assessment and revision of plant protection, animal health, commodity/grain inspection, pesticide and food safety vector control policies, procedures and operations to align with the National Response Plan and the associated capabilities elements of that Plan.

The Washington Department of Agriculture will lead statewide efforts to:		**Target**
4.2.5.1	Identify and assign staff to review policies, procedures and operations.	January 2006
4.2.5.2	Final revisions completed and gaps identified.	August 2006
4.2.5.3	Strategies developed to address needs/gaps.	September 2006
4.2.5.4	Review criteria identified and initial analysis and drafts produced and reviewed (ongoing).	June 2007
4.2.5.5	Evaluate capabilities related to resource/budget requests.	June 2007
4.2.5.6	Pursue funding/resources to fill needs and gaps (ongoing).	June 2007

E. Preparedness and Response: Strengthen Response Capabilities to Prepare First Responders and Citizens for All-Hazards Events.

This priority has six goals beginning with institutionalizing both the National Incident Management System (NIMS) and the National Response Plan (NRP). The goals also focus on enhancing incident management, regional response and resource management capabilities, as well as increasing citizen preparedness and participation.

This priority focuses on the Respond

Linked National Priorities:

Implement the National Incident Management System and the National Response Plan: Implement the National Incident Management System and National Response Plan nation-wide.

Strengthen Chemical, Biological, Radiological, Nuclear and Explosive Detection, Response and Decontamination Capabilities: Strengthen statewide CBRNE Detection Capabilities.

Mission Area Target Capabilities: Onsite Incident Management, Emergency Operations Center Management, Critical Resource Logistics and Distribution, Volunteer Management and Donations, Responder Safety and Health, Public Safety and Security Response, Animal Health Emergency Response Environmental Health and Vector Control, Explosive Device Response Operations, Firefighting Operations and Support, WMD/Hazardous Materials Response and Decontamination, Citizen Protection: Evacuation and/or-In Place Protection, Urban Search Rescue (local capability, not FEMA teams) and Emergency Public Information and Warning.

GOAL 5.1: Institutionalize the National Incident Management System (NIMS)

Objective 5.1.1: Coordinate statewide to ensure National Incident Management System (NIMS) adoption and provide technical assistance for state agencies, tribal governments and local governments to fully implement, and formally recognize NIMS principles and polices statewide by September 2006.

The Washington State Patrol (WSP) and the Washington Military Department Emergency Management Division (EMD) will coordinate statewide efforts to achieve the FFY 2006 NIMS requirements.

The Washington Military Department Emergency Management Division and Washington State Patrol will lead statewide efforts to:		Target
5.1.1.1	Coordinate statewide to ensure NIMS adoption and provide technical assistance for state agencies, tribal governments and local governments to fully implement and formally recognize NIMS principles and polices statewide in FFY 2006.	September 2006
5.1.1.2	Incorporate the NIMS into existing statewide education, training and exercise programs.	September 2006
5.1.1.3	Incorporate NIMS into Emergency Operations Plans (EOP's) statewide at all levels of government.	September 2006

GOAL 5.2: Institutionalize the National Response Plan (NRP)

Objective 5.2.1: Coordinate statewide to implement and institutionalize the National Response Plan by June 2010.

This objective details statewide coordination to implement and institutionalize the National Response Plan (NRP).

The Washington Military Department Emergency Management Division will lead statewide efforts to:		Target
5.2.1.1	Rewrite State Local Jurisdiction Planning Guidance and distribute.	April 2006
5.2.1.2	Rewrite State CEMP to incorporate NRP changes.	June 2006
5.2.1.3	Distribute revised CEMP.	August 2006

5.2.1.4	Conduct Planning Seminars for Local Jurisdictions.	June 2007
5.2.1.5	Review Local Planning Guidance.	March 2008
5.2.1.6	Review CEMP.	June 2008
5.2.1.7	Review and Update Local Planning Guidance.	March 2010
5.2.1.8	Review and Update CEMP.	June 2010

GOAL 5.3: Enhance Incident Management Capability

Objective 5.3.1: Develop a multi-discipline training capability to provide statewide emergency responders training, certification, and credentialing in support of NIMS implementation by June 2007.

This objective develops a multi-discipline training capability to provide statewide emergency responders training, certification, and credentialing.

The Washington Homeland Security Institute and Washington Military Department, Emergency Management Division will lead statewide efforts to:		**Target**
5.3.1.1	Provide a system for cross-discipline, awareness-level, ODP & FEMA-approved online training courses (including NIMS, WMD-related course, HAZMAT, etc.).	June 2007
5.3.1.2	Implement a training registration program.	June 2007
5.3.1.3	Market program to state and local partners. Conduct exchanges with other states and federal providers.	June 2007
5.3.1.4	Seek additional national (like the Competitive Training Grant secured for ferry training in 2006), state, and local funding opportunities.	June 2007
5.3.1.5	In partnership with EMD, coordinate and facilitate communication regarding traditional classroom training program availability.	June 2007
5.3.1.6	Expand and refine the database of certified trainers (to include qualified NIMS trainers) and make available to state, region, county, and local jurisdictions.	June 2007
5.3.1.7	Develop processes to support train-the-trainer needs.	June 2007
5.3.1.8	Build on the Emergency Response Training Assessment and Recommendations report delivered in 2006, and analyze output from Skills Panels in partnership with the Homeland Security Institute.	June 2007
5.3.1.9	Continue development of statewide credentialing system which interfaces nationally.	June 2007
5.3.1.10	Integrate online course development with the for-credit certificate programs and degrees being offered by the state community and technical college system and universities.	June 2007

Objective 5.3.2: Explore best practices and work to enhance transportation system security by June 2011.

This objective develops a public education program to build secure maritime transportation systems within the state of Washington, specifically focused on the Washington State Ferries (WSF).

The Washington State Patrol will lead statewide efforts to:		Target
5.3.2.1	Evaluate current training and education tools and technologies that can enhance program delivery and information sharing.	June 2007
5.3.2.2	Partner with the Homeland Security Institute for the implementation of a $1 million Ferry Passenger Partner Program.	June 2007
5.3.2.3	Develop and conduct public education plan.	June 2007
5.3.2.4	Evaluate current training and education tools and technologies that can enhance program delivery and information sharing.	June 2009
5.3.2.5	Develop and conduct public education plan.	June 2009
5.3.2.6	Continued evaluation of training and education tools and technologies as well as the need for the program.	June 2009
5.3.2.7	Continued evaluation of training and education program for effectiveness and improvements.	June 2009
5.3.2.8	Continued evaluation of training and education tools and technologies as well as the need for the program.	June 2011
5.3.2.9	Continued evaluation of training and education program for effectiveness and improvements.	June 2011

Objective 5.3.3: Increase Washington State Patrol involvement in the Marine Training Response exercises and implement lessons learned by June 2007.

This objective strengthens our ability to response to all-hazard events involving the Washington State Ferry (WSF) system.

The Washington State Patrol will lead statewide efforts to:		Target
5.3.3.1	Annual renewal of existing mutual aid contracts.	June 2007
5.3.3.2	Establish internal WSP VATS committee for regular review and needs assessment.	June 2007
5.3.3.3	Conduct training on ferry incident response.	June 2007
5.3.3.4	Train all Washington State Civil Disturbance Action Teams (CDAT) on ferry response, protection and recovery.	June 2007

Objective 5.3.4: Strengthen the ability for Washington State Department of Transportation (WSDOT) personnel to plan for, respond to and recover from all hazard events involving statewide transportation infrastructure by June 2008.

This objective outlines a preparedness program that will equip and train WSDOT staff for planning, response, and recovery for all-hazard events affecting the transportation infrastructure.

The Washington Department of Transportation (WSDOT) will lead statewide efforts to:		**Target**
5.3.4.1	Hire consultant to develop the I-90 bridges emergency plan and coordinate a WSDOT/Local Agency/First responder drill.	May 2006
5.3.4.2	Research equipment gaps for maintenance personnel.	July 2006
5.3.4.3	Provide security training for WSDOT personnel.	November 2006
5.3.4.4	Develop terrorist/all hazard procedures for maintenance personnel.	December 2006
5.3.4.5	Develop emergency plan for I-90 bridges.	June 2007
5.3.4.6	I –90 bridge drill with WSDOT and emergency responders.	April 2008
5.3.4.7	Evaluation and Lessons Learned/ National Incident Management System (NIMS) Consideration.	June 2008

Objective 5.3.5: Identify those areas that have the ability to cultivate personnel and have the desire to have a functioning Type 3 Incident Management Team (IMT) available for local, regional and statewide response by June 2011.

Three Type 3 IMTs, in addition to the existing three Type 3 IMTs, are established through this objective to provide rapid response to an incident, better prepare local communities, provide better trained first response personnel and promote the use of NIMS ICS. A Type 3 IMT is a standing team of trained personnel from different departments, organizations, agencies, and jurisdictions within a state or DHS Urban Area Security Initiative region, activated to support incident management at major or complex emergency incidents or special events that extend beyond one operational period.

The Washington State Patrol will lead statewide efforts to:		**Target**
5.3.5.1	Secure approximately $100,000 of funding to complete a gap analysis.	June 2007
5.3.5.2	Identify participants and implement training plans.	June 2007
5.3.5.3	Secure funding for personnel and training.	September 2007
5.3.5.4	Secure funding to train administrators, and assist new teams' planning section in developing Incident Action Plans.	December 2007
5.3.5.5	Secure funding to purchase equipment, and oversee the teams' equipment operation training.	March 2008
5.3.5.6	Secure funding for the development and completion of a tabletop exercise and a regional/statewide exercise.	June 2008
5.3.5.7	Continue building teams encouraging each team to have personnel three deep for each position.	June 2010
5.3.5.8	Continue developing and implementing exercises to test teams and evaluate their performance.	June 2010
5.3.5.9	Identify additional areas to develop an additional three Type 3 Teams, continue with training, planning and exercises to prevent teams from folding due to attrition.	June 2011

GOAL 5.4: Strengthen Regional Response Capabilities

Objective 5.4.1: Identify gaps in firefighting operational capability and state firefighting operations with the statewide National Incident Management System (NIMS) implementation by June 2008.

This objective seeks resources and support for fire mobilization activities conducted in support of state fire mobilization and to fully integrate firefighting operations with the statewide NIMS implementation.

The Washington State Patrol will lead statewide efforts to:		Target
5.4.1.1	Identify state fire mobilization gaps in Personnel, Planning, Training, Exercising, and Equipment capabilities.	June 2007
5.4.1.2	Determine CBRNE/HAZMAT training needs for fire fighting operations.	December 2007
5.4.1.3	Review and update existing fire mobilization mutual aid agreements.	June 2008

Objective 5.4.2: Establish and sustain regional Search and Rescue (SAR) response capability by TBD.

This objective identifies the gaps in the Search and Rescue (SAR) response capability in Washington and develops a state program structure and sustainable funding mechanism for statewide SAR operations.

The Washington Military Department, Emergency Management Division, in collaboration with the Pierce County Puget Sound Urban Search and Rescue Task Force (FEMA), will lead statewide efforts to:		Target (NEW OBJECTIVE)
5.4.2.1	Complete an inventory of existing SAR response capability, by FEMA Type Code, within Washington state.	TBD
5.4.2.2	Recommend a state program structure that provides SAR regional response capability.	TBD
5.4.2.3	Request Governor's Office and stakeholder assistance through the EMC and DSEG in obtaining legislative funding to support statewide SAR capability/structure for regional response.	TBD
5.4.2.4	Create a sustainable funding mechanism to support regional response team capability.	TBD
5.4.2.5	Implement statewide structure/system supporting regional SAR response capability.	TBD
5.4.2.6	Maintain statewide SAR regional response capability by establishing an annual review process.	TBD

Objective 5.4.3: Develop a five-year exercise and evaluation program to strengthen the regional response capabilities by June 2009.

This objective develops an integrated systemic approach to statewide exercise development, implementation and evaluation to strengthen the statewide public safety and security response.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		Target
5.4.3.1	Conduct the annual integrated exercise/training planning workshop.	August 2006
5.4.3.2	Partner with Office of Grants and Training to conduct exercise design/evaluation course.	May 2006
5.4.3.3	Develop a five-year State Homeland Security Exercise & Evaluation Program.	May 2006
5.4.3.4	Develop a new exercise evaluation course.	January 2007
5.4.3.5	Coordinate state participation in a national-level full-scale exercise (Top Officials - 4).	October 2007
5.4.3.6	Continue to exercise on a consistent basis (ongoing annually).	June 2007
5.4.3.7	Develop an exercise evaluator program and database.	June 2009

Objective 5.4.4: Develop and exercise inter-state and intra-state mutual assistance compacts by January 2008.

This objective involves all levels of government in Washington State in developing and exercising intra-state and inter-state mutual assistance compacts.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		Target
5.4.4.1	Conduct a mutual aid summit to involve all interested stakeholders in the development of a mutual aid system.	June 2006
5.4.4.2	Develop and submit draft mutual aid legislation.	September 2006
5.4.4.3	Develop a talking paper on Intra-state Mutual Aid for the Legislature.	September 2006
5.4.4.4	Testify to appropriate legislative committees as required.	January 2007
5.4.4.5	Appoint a governance body for Intra-state Mutual Aid.	August 2007
5.4.4.6	Develop a governance body meeting schedule and task list for implementation.	January 2008

Objective 5.4.5: Establish and sustain a regional Hazardous Materials (HAZMAT) and Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) response capability by January 2008.

This objective identifies the gaps in capability to respond to Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE)/Hazardous Materials events and aids the development of a statewide CBRNE/HAZMAT capability.

The Washington State Emergency Response Commission (SERC) will	Target

lead statewide efforts to:		
5.4.5.1	Complete a study on the current status of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE)/Hazardous Materials response in Washington State.	November 2005
5.4.5.2	Recommend a state program structure.	December 2005
5.4.5.3	Request Emergency Management Council support for legislation to establish a sustainable statewide CBRNE/HAZMAT response capability.	April 2006
5.4.5.4	Achieve a sustainable funding mechanism to support regional CBRNE/HAZMAT response teams.	May 2007
5.4.5.5	Implement regional CBRNE/HAZMAT response teams.	January 2008
5.4.5.6	Maintain statewide CBRNE/Hazmat statewide response capability by establishing an annual review process.	January 2009

Objective 5.4.6 Establish and sustain statewide chemical, radiological, nuclear, and explosive (CBRNE) evidence screening and recognition capability by January 2007.

This objective provides equipment and training that will bring the seven crime laboratories of the Washington State Patrol (WSP) Crime Laboratory Division (CLD) to an appropriate level of readiness so that evidence submitted to any of the laboratories can be screened for the presence of a chemical, biological, or radiological agents.

The Washington State Patrol will lead statewide efforts to:		Target
5.4.6.1	Identify existing laboratory personnel to participate in suspected chemical, biological, and radiological agent screening.	January 2006
5.4.6.2	Meet with stakeholder laboratories to develop a coordinated analysis and evidence transfer plan.	March 2006
5.4.6.3	Begin training of selected personnel.	June 2006
5.4.6.4	Develop specifications and order necessary equipment.	July 2006
5.4.6.5	Validate analytical protocols for analysis.	September 2006
5.4.6.6	Develop annual proficiency testing requirements.	December 2006
5.4.6.7	Develop a plan to participate in annual CBRNE exercises.	December 2006
5.4.6.8	Certify analytical readiness.	January 2007

Objective 5.4.7: Enhance Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) capabilities by developing integrated response teams for statewide CBRNE coverage by December 2007.

This objective integrates the WSP SWAT team and the Washington State National Guard 10th Civil Support Team into a cohesive WMD response team.

The Washington State Patrol will lead statewide efforts to:		Target
5.4.7.1	Identify equipment standards and priorities.	June 2007

5.4.7.2	Obtain cost estimates for CBRNE vehicle.	June 2007
5.4.7.3	Order vehicle.	June 2007
5.4.7.4	Develop training plan to integrate vehicle into response operations.	September 2007
5.4.7.5	Integrate CBRNE vehicle into response operations.	December 2007

Objective 5.4.8: Develop capability to perform Mass Depopulation and Animal Disposal Operations in an efficient, humane, and timely manner to prevent the spread of disease and dispose of dead animals by December 2008.

This objective describes the plan for developing the capability to conduct Mass Depopulation and Animal Disposal Operations.

The Washington Department of Agriculture will lead statewide efforts to:		**Target**
5.4.8.1	Hire an Animal Health/Homeland Security Planner.	June 2006
5.4.8.2	Review existing plans and procedures for mass depopulation and animal disposal.	September 2006
5.4.8.3	Coordinate mass depopulation and animal or food disposal issues with local jurisdictions, regions, and our federal partners.	September 2006
5.4.8.4	Plan a WSDA tabletop exercise to evaluate the Mass Depopulation and Animal or Food Disposal Plan.	November 2006
5.4.8.5	Develop a Mass Depopulation and Animal or Food Disposal Plan.	December 2006
5.4.8.6	Continue to update ESF 25 of the Washington State Comprehensive Emergency Management Plan (CEMP) and convert it to ESF 11 and work on existing animal disposal procedures.	June 2007
5.4.8.7	Determine equipment requirements to conduct a Mass Depopulation and Animal or Food Disposal Operation.	December 2007
5.4.8.8	Enhance GIS information to support decision making for Mass Depopulation and Animal Disposal Operations.	December 2007
5.4.8.9	Revise Mass Depopulation and Animal or Food Disposal Operations Plan using input from the tabletop exercises.	December 2007
5.4.8.10	Plan and conduct a functional Mass Depopulation and Animal or Food Disposal Operations Exercise.	April 2008
5.4.8.11	Revise Mass Depopulation and Animal Disposal Operations Plan using input from the functional exercises.	December 2008
5.4.8.12	Update data on the resources required to conduct Mass Depopulation and Animal or Food Disposal Operations.	December 2008
5.4.8.13	Continue to enhance GIS information to support decision making for Mass Depopulation and Animal or Food Disposal Operations.	December 2008
5.4.8.14	Revise Mass Depopulation and Animal or Food Disposal Operations Plan using input from the functional exercise.	December 2009
5.4.8.15	Plan and conduct a full scale Mass Depopulation and Animal or Food Disposal Operations Exercise.	December 2010
5.4.8.16	Revise Mass Depopulation and Animal or Food Disposal Operations Plan using input from the full scale exercise.	June 2011

5.4.8.17	Update data on the resources required to conduct Mass Depopulation and Animal Disposal Operations.	June 2011
5.4.8.18	Continue to enhance GIS information to support decision making for Mass Depopulation and Animal or Food Disposal Operations.	July 2011

GOAL 5.5: Build Resource Management Capabilities

Objective 5.5.1: Enhance the capability to coordinate, acquire, receive, store and distribute emergency response resources to affected areas of the state including the use of local, state and federal points of distribution, staging areas, stockpiles, pre-positioned equipment and mutual aid assistance resources by July 2009.

This objective identifies gaps in resource management capability for emergency and disaster response and recovery in Washington State.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		**Target**
5.5.1.1	Complete Standard Operating Guidance (SOG)/Procedures (SOP) for Logistics and Mutual Aid.	March 2007
5.5.1.2	Establish semi-annual statewide logistics meetings.	January 2006
5.5.1.3	Collaborate in the development of a regional logistics support concept.	July 2007
5.5.1.4	Develop a statewide resource distribution plan.	January 2007
5.5.1.5	Develop and contribute to a statewide logistics information sharing strategy.	January 2007
5.5.1.6	Establish a resource tracking capability.	May 2007
5.5.1.7	Maintain state-wide logistics capability by establishing an annual review process.	July 2009

Objective 5.5.2: Develop and maintain a statewide disaster emergency logistics plan by June 2011.

This objective supports development of a statewide disaster/emergency logistics plan and implements a program structure to support emergency resource management within the state and local jurisdictions to include the capability to coordinate, acquire, receive, store, and distribute emergency response resources to affected areas.

The Washington Department of General Administration will lead statewide efforts to:		**Target**
5.5.2.1	Identify sites for pre-positioned emergency equipment and supply containers.	June 2006
5.5.2.2	Identify stakeholders to develop statewide disaster/emergency logistics plan.	June 2006

5.5.2.3	Procure mobile threat assessment equipment.	January 2007
5.5.2.4	Procure emergency equipment and supplies containers.	June 2007
5.5.2.5	Establish emergency container sites and stock them.	December 2007
5.5.2.6	Develop and implement the statewide disaster/emergency logistics plan.	June 2009
5.5.2.7	Evaluate and test the logistics plan.	June 2009
5.5.2.8	Conduct a table top exercise and incorporate lessons learned into the logistics plan.	June 2011

GOAL 5.6: Increase Citizen Preparedness and Participation

Objective 5.6.1: Enhance the all-hazards public education program to provide citizens information on how to prepare for, recognize, report, and respond to all-hazards events by June 2011.

This objective enhances Washington's all-hazard public education program to include tribal representatives, local, and state populations.

The Washington Military Department Emergency Management Division will lead statewide efforts to:		**Target**
5.6.1.1	Form steering committee to develop coordinated message, create a strategic plan for all-hazard preparedness, and develop an EMD public education library.	April 2006
5.6.1.2	Develop and fill a public education coordinator position.	July 2006
5.6.1.3	Develop material distribution tracking database and valid, reliable performance testing instruments.	October 2006
5.6.1.4	Develop and produce CBRNE card and DVD. Contract with public education expert for training.	October 2006
5.6.1.5	Include non-governmental agencies.	June 2009
5.6.1.6	Review effectiveness of current campaign (ongoing).	June 2011
5.6.1.7	Revise and update materials for distribution (ongoing).	June 2011
5.6.1.8	Prepare CBRNE card for specific needs populations (ongoing).	June 2011

Objective 5.6.2: Build a strong statewide volunteer capability to assist emergency responders for all-hazards by June 2011.

This objective supports further development of Citizen Corps to harness the power of every individual through ***education, training, and volunteer service*** to make communities safer, stronger, and better prepared to respond to the threats of terrorism, crime, public health issues, and disasters of all kinds.

The Washington Citizen Corps Council will lead statewide efforts to:		Target
5.6.2.1	Develop, conduct and evaluate public education programs.	June 2007
5.6.2.2	Develop and conduct training courses for citizen participation in incident management.	June 2007
5.6.2.3	Maintain and expand training and exercise programs to prepare volunteers for all-hazard incident support.	June 2007
5.6.2.4	Work with the Committee on Homeland Security to develop a statewide identification system for trainers related to local preparedness and programmatic subject matter experts.	June 2007
5.6.2.5	Develop support for Citizen Corps Councils and programs.	June 2007
5.6.2.6	Address liability issues, integration of Citizen Corps volunteers into the Emergency Worker Program.	June 2007
5.6.2.7	Address licensure issues for all professionals.	June 2007
5.6.2.8	Write plans for each CCP in the state to include how they will provide opportunities for the community to volunteer.	June 2007
5.6.2.9	Increase volunteer participation in the emergency responder communities.	June 2007
5.6.2.10	Address capability of state and local communities to develop a Citizen Corps and participate in community preparedness.	June 2009
5.6.2.11	Develop projects and collaboration with academic community to institutionalize training and preparedness in all grade levels, including college level programs.	June 2011
5.6.2.12	Engage the business community to participate in Citizen Corps programs and prepare within their community.	June 2011

The 10th Civil Support Team participating in a local exercise.

Photo Courtesy of the Washington National Guard

Region 2 First Responders from Clallam and Kitsap Counties attending a technical rescue training class.

Photo Courtesy of Homeland Security Region 2

F. Recovery: Promote Economic and Community Recovery from All-Hazard Events.

The one goal under this priority focuses on building our capability to recover from all-hazard events.

This priority addresses on the Recover Mission Area Target Capabilities: Structural Damage and Mitigation Assessment, Restoration of Lifelines, and Economic and Community Recovery.

Linked National Priorities:

Implement the National Incident Management System and the National Response Plan: Implement the National Incident Management System and National Response Plan nation-wide.

GOAL 6.1: Increase Capability to Recover From All-Hazard Events

Objective 6.1.1: Develop comprehensive statewide recovery planning and strengthen our ability to mitigate the consequences of an all-hazards event by June 2011.

This objective outlines efforts to review and strengthen existing statewide recovery capabilities as outlined in the Comprehensive Emergency Management Plan (CEMP).

The Washington Military Department Emergency Management Division will lead statewide efforts to:		**Target**
6.1.1.1	Identify resources for coordinating the development of statewide recovery planning.	June 2007
6.1.1.2	Develop a strategy for comprehensive statewide recovery planning within the context of the CEMP.	June 2007
6.1.1.3	Develop a strategy for training and staffing key recovery functions with multiple staff.	June 2007
6.1.1.4	Identify all existing recovery training and exercise plans statewide.	June 2007
6.1.1.5	Add a full-time Recovery Strategist as well as 3 full-time FTEs for Public Assistance, Human Services, and Hazard Mitigation programs to EMD staff.	June 2007
6.1.1.6	Begin a series of table-top recovery exercises to determine critical shortfalls.	June 2008
6.1.1.7	Ensure adequate resources exist for continued coordination and development of statewide recovery planning, training, and exercises.	June 2008
6.1.1.8	Identify all existing recovery plans as a foundation for creating a basis for comprehensive statewide recovery planning.	June 2008
6.1.1.9	Incorporate comprehensive statewide recovery planning within the CEMP as it is brought into alignment with the National Response Plan.	June 2008
6.1.1.10	Develop a five-year training and exercise plan to test the recovery elements of the CEMP.	June 2009
6.1.1.11	Continuation of staffing, planning, training, and exercising done in 2005-2007.	June 2009
6.1.1.12	Conduct annual recovery training for all crossed-trained EMD recovery staff.	June 2009
6.1.1.13	Conduct training and exercise the recovery elements of the CEMP.	June 2009

6.1.1.14	Revise the recovery elements of the CEMP based on lessons learned through the exercises.	June 2009
6.1.1.15	Update the recovery elements of the CEMP and maintain the supporting training and exercise plans to validate the recovery elements of the CEMP.	June 2009
6.1.1.16	Conduct coordination meetings among affected entities to sustain comprehensive recovery planning.	June 2009
6.1.1.17	Continuation of staffing, planning, training, and exercising done in 2005-2007.	June 2011
6.1.1.18	Conduct annual recovery training for all crossed-trained EMD recovery staff.	June 2011
6.1.1.19	Conduct training and exercise the recovery elements of the CEMP.	June 2011
6.1.1.20	Revise the recovery elements of the CEMP based on lessons learned through the exercises.	June 2011
6.1.1.21	Update the recovery elements of the CEMP and maintain the supporting training and exercise plans to validate the recovery elements of the CEMP.	June 2011
6.1.1.22	Conduct coordination meetings among affected entities to sustain comprehensive recovery planning.	June 2011

Objective 6.1.2: Develop and/or refine existing mass care plans for all-hazard disasters events by June 2009.

This objective develops plans to provide immediate shelter, feeding centers, basic first aid, bulk distribution of needed items, and related services to persons affected by a large-scale incident, including special needs populations.

The Washington Department of Social and Health Services will lead efforts to:		**Target**
6.1.2.1	Determine gaps in existing support system functions and additional capabilities required.	June 2007
6.1.2.2	Clarify the strategic and operational roles for team members regarding function and responsibilities.	June 2007
6.1.2.3	Establish and clearly define and develop reporting and communication mechanisms.	June 2007
6.1.2.4	Seek resources for the developing a statewide mass care plan.	June 2007
6.1.2.5	Develop a statewide mass care plan.	June 2007
6.1.2.6	Develop and implement a statewide training program for the mass care plan.	June 2007
6.1.2.7	Integrate services and develop methods to ensure all team members understand relationships.	June 2007
6.1.2.8	Test mass care plan on local level, regional level and state level.	June 2009
6.1.2.9	Apply lessons learned from plan testing to update the mass care plan.	June 2009

Objective 6.1.3: Strengthen Washington State's infrastructure by testing structure vulnerabilities, developing mitigation measures and improving survivability of transportation systems by June 2007.

This objective addresses critical infrastructure protection, terrorism investigation and intervention, and structural damage assessment and mitigation statewide.

The Washington State Department of Transportation (WSDOT) will lead statewide efforts to:		**Target**
6.1.3.1	Evaluate and update current training.	February 2006
6.1.3.2	Develop training curriculum for forensic investigation, with involvement from ERDC (Consultant) that addresses Washington State Patrol (WSP) and First Responder needs.	February 2006
6.1.3.3	Identify training needs for forensic investigation of remnants of a bridge blast.	April 2006
6.1.3.4	Advertise the training opportunity through EMD.	April 2006
6.1.3.5	Establish process for sharing information with all stakeholders and across critical infrastructure sectors.	July 2006
6.1.3.6	Develop an information sharing technology for this project.	July 2006
6.1.3.7	Sharing information – location, structure, and ease of use to be determined by Consultants and WSDOT.	November 2006
6.1.3.8	Identify key stakeholders, contributors, and consumers of information.	November 2006
6.1.3.9	Develop train the trainer program and offer future training program through WSP.	December 2006
6.1.3.10	Include stakeholders in planning process (continuous).	December 2006
6.1.3.11	Identify relevant data categories with stakeholders.	January 2007
6.1.3.12	Hire a consultant to conduct a blast test: (1) pre-test analysis, (2) design, install, and activate blast loadings, (3) instrumentation, and (4) post-analysis.	June 2007
6.1.3.13	Following blast test, develop lessons learned to improve training plans and internal procedures.	June 2007

Homeland Security Regions 3 and 4 participate in Citizen Emergency Response Training (CERT)

Photo courtesy of Region 3

G. Health Systems: Enhance Healthcare and Public Health Systems to Provide Medical Surge and Mass Prophylaxis Capacity for Emergencies and Large-Scale Disasters.

The two goals under this priority are to increase statewide medical surge capability and to strengthen mass prophylaxis operations.

This priority focuses on the Prevent, Protect and Respond Mission Area Target Capabilities: CBRNE Detection, Public Health and Epidemiological Investigation and Laboratory Testing, Triage and Pre-Hospital Treatment, Medical Surge, Medical Supplies Management and Distribution, Mass Prophylaxis and Fatality Management.

Linked National Priorities:

Strengthen Medical Surge and Mass Prophylaxis Capabilities: Establish emergency-ready public health and health care agencies across the Nation.

GOAL 7.1: Increase Medical Surge Capability

Objective 7.1.1: Train and educate health care professionals to recognize and treat victims of all-hazard events by June 2007.

This objective details the steps required to prepare the healthcare community and public health agencies to respond acts of terrorism or other emergencies that impact the health of the people of Washington State by providing resources and guidance for the acquisition of education and training in proper recognition, triage, and treatment of victims of a chemical, biological, radiological, nuclear, explosive (CBRNE) or naturally occurring incident.

The Washington Department of Health will lead statewide efforts to:		Target
7.1.1.1	Ongoing development and implementation of regional and statewide public health preparedness and response training plans.	June 2007
7.1.1.2	Initial development of a statewide healthcare preparedness and response training plan.	June 2007

Objective 7.1.2: Optimize medical surge capacity for victims of all-hazard events by June 2007.

This objective prepares the healthcare community and public health agencies to respond acts of terrorism or other emergencies that impact the health of the people of Washington State by enabling medical and public health surge capacity and capability.

The Washington Department of Health will lead statewide efforts to:		Target
7.1.2.1	Ongoing assessment and addressing of identified needs.	June 2007

Objective 7.1.3: Enhance statewide medical laboratory capacity to respond to all-hazards events by June 2011.

This objective enhances medical laboratory capability by acquiring laboratory equipment for testing and identification of biological and environmental (chemical and radiological) samples that arise either through suspected terrorism activities or through natural or man-made contamination incidents.

The Washington Department of Health will lead statewide efforts to:		Target
7.1.3.1	Specify and receive formal quotations for specific equipment.	March 2006
7.1.3.2	Purchase and install equipment.	July 2006
7.1.3.3	Train staff, develop internal protocols and participate in CDC's Laboratory Response Network proficiency testing to become certified as part of the state-wide and national response system for the agents.	January 2007
7.1.3.4	Test proficiency of laboratory staff and reliability of equipment through actual events and response exercises.	June 2009
7.1.3.5	Continue to test proficiency of laboratory staff and reliability of equipment through actual events and response exercises.	June 2011

Objective 7.1.4: Develop statewide capacity to isolate and/or quarantine (as appropriate) victims of all-hazard events by June 2011.

The purpose of this objective is to develop a statewide disease containment strategy based on quarantine and isolation capacity to be used in communicable disease and biological terrorism events as applicable.

The Washington Department of Health (DOH) will lead statewide efforts to:		Target
7.1.4.1	Continue planning effort to define the role of the state in isolation and quarantine capacity.	June 2007
7.1.4.2	Conduct assessment of local/regional capacity and readiness.	June 2007
7.1.4.3	Review and finalize isolation and quarantine portion of the DOH Communicable Disease Emergency Response Plan (CDERP).	June 2007
7.1.4.4	Develop protocols and procedures for implementation of isolation and quarantine portion of CDERP.	June 2007
7.1.4.5	Identify and address training needs.	June 2007
7.1.4.6	Identify and address staffing needs.	June 2007
7.1.4.7	Review, exercise and test state and regional plans.	June 2007
7.1.4.8	Develop mutual aid and resource typing systems for public health.	June 2007
7.1.4.9	Develop public health emergency public education campaigns.	June 2007
7.1.4.10	Review, exercise and test state and regional plans.	June 2009
7.1.4.11	Review, exercise and test state and regional plans.	June 2011

Objective 7.1.5: Build our statewide healthcare systems' capability to provide personal protection for providers and decontamination capabilities by June 2011.

This objective prepares the healthcare community to respond to events that require providers to be protected from biological agent exposure and to decontaminate patients to be able to provide care and protect the integrity of the healthcare facility.

The Washington Department of Health will lead statewide efforts to:		Target
7.1.5.1	Ensure all hospitals receive appropriate amounts of PPE, decontaminations systems and associated training.	September 2006
7.1.5.2	Ensure all ancillary healthcare entities, appropriately identified, receive PPE, decontamination systems and associated training.	June 2009
7.1.5.3	Conduct continuous training and exercises.	June 2011

Objective 7.1.6: Develop a statewide mass fatality plan by June 2011.

This objective outlines efforts to prepare the state of Washington to support local jurisdictions in incidents that result in the deaths of large numbers of persons.

The Washington Department of Health will lead statewide efforts to:		Target
7.1.6.1	Finalize a state-level mass fatality management plan.	September 2006
7.1.6.2	Validate the state mass fatality management plan through statewide/ regional exercises.	September 2008
7.1.6.3	Update the plan to reflect lessons learned.	June 2009
7.1.6.4	Re-validate the mass fatality plan through a rigorous exercise program.	September 2010

7.1.6.5	Update each local plan to reflect lessons learned.	June 2011

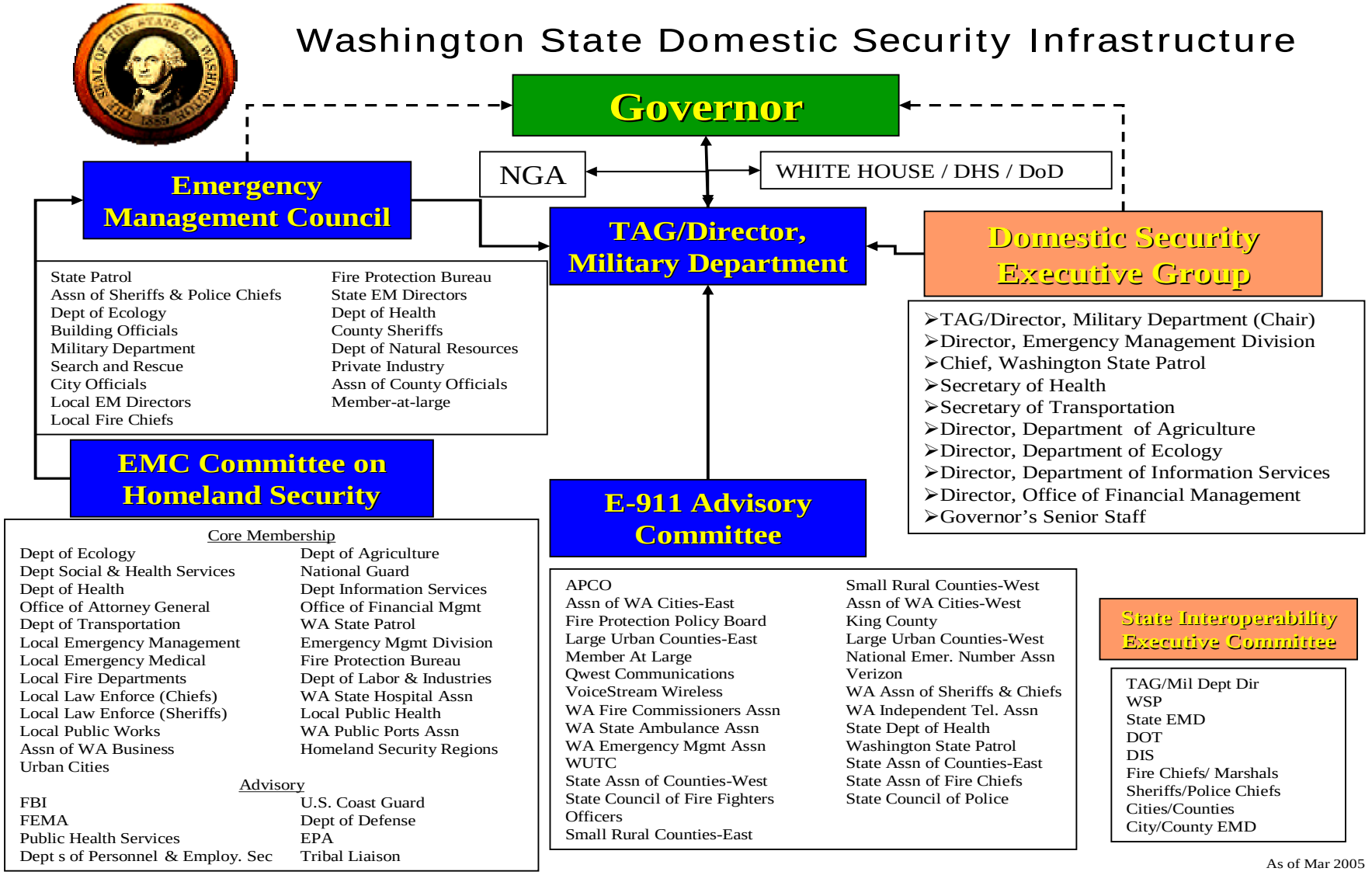
GOAL 7.2: Strengthen Mass Prophylaxis Operations

Objective 7.2.1: Strengthen our capability to receive and distribute medical supplies by June 2011.

This objective prepares Washington to dispense lifesaving medications and other medical supplies in the wake of a bioterrorism attack, other widespread dangerous infectious disease outbreak, or other emergency requiring large quantities of medical supplies.

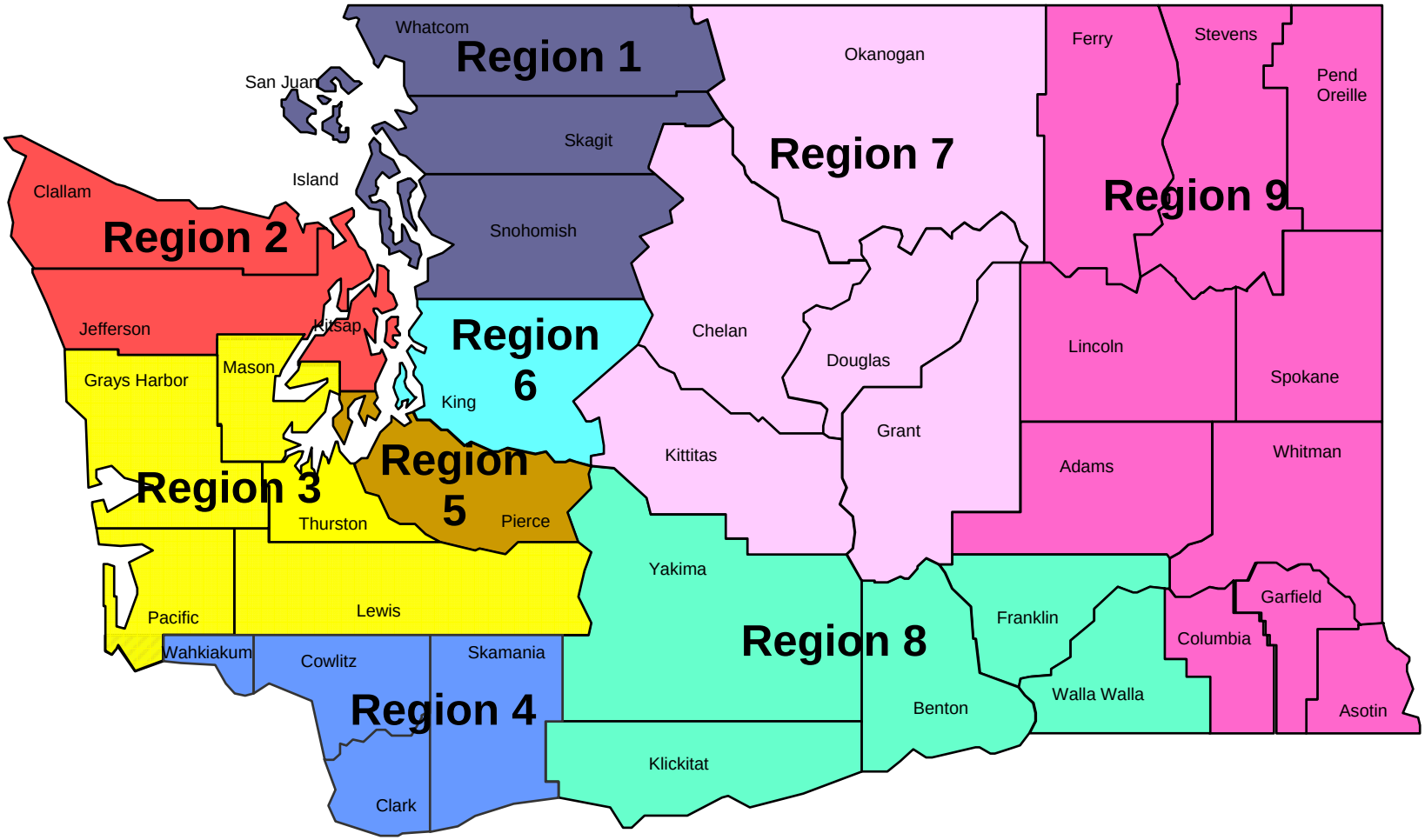
The Washington Department of Health will lead statewide efforts to:		Target
7.2.1.1	Test local mass prophylaxis plans through rigorous exercises.	September 2006
7.2.1.2	Update each local plan to reflect lessons learned.	June 2007
7.2.1.3	Validate each local mass prophylaxis plan through statewide/regional exercises.	September 2008
7.2.1.4	Update each local plan to reflect lessons learned.	June 2009
7.2.1.5	Re-validate each local mass prophylaxis plan through statewide/regional exercises.	September 2010
7.2.1.6	Update each local plan to reflect lessons learned.	June 2011

APPENDIX A


Washington State Domestic Security Infrastructure
Governor
NGA
WHITE HOUSE / DHS / DoD
Emergency Management Council
TAG/Director, Military Department
Domestic Security Executive Group
State Patrol
Assn of Sheriffs & Police Chiefs
Dept of Ecology
Building Officials
Military Department
Search and Rescue
City Officials
Local EM Directors
Local Fire Chiefs
Fire Protection Bureau
State EM Directors
Dept of Health
County Sheriffs
Dept of Natural Resources
Private Industry
Assn of County Officials
Member-at-large
➢TAG/Director, Military Department (Chair)
➢Director, Emergency Management Division
➢Chief, Washington State Patrol
➢Secretary of Health
➢Secretary of Transportation
➢Director, Department of Agriculture
➢Director, Department of Ecology
➢Director, Department of Information Services
➢Director, Office of Financial Management
➢Governor's Senior Staff
EMC Committee on Homeland Security
E-911 Advisory Committee
Core Membership
Dept of Ecology
Dept Social & Health Services
Dept of Health
Office of Attorney General
Dept of Transportation
Local Emergency Management
Local Emergency Medical
Local Fire Departments
Local Law Enforce (Chiefs)
Local Law Enforce (Sheriffs)
Local Public Works
Assn of WA Business
Urban Cities
Dept of Agriculture
National Guard
Dept Information Services
Office of Financial Mgmt
WA State Patrol
Emergency Mgmt Division
Fire Protection Bureau
Dept of Labor & Industries
WA State Hospital Assn
Local Public Health
WA Public Ports Assn
Homeland Security Regions
Advisory
FBI
FEMA
Public Health Services
Dept s of Personnel & Employ. Sec
U.S. Coast Guard
Dept of Defense
EPA
Tribal Liaison
APCO
Assn of WA Cities-East
Fire Protection Policy Board
Large Urban Counties-East
Member At Large
Qwest Communications
VoiceStream Wireless
WA Fire Commissioners Assn
WA State Ambulance Assn
WA Emergency Mgmt Assn
WUTC
State Assn of Counties-West
State Council of Fire Fighters
Officers
Small Rural Counties-East
Small Rural Counties-West
Assn of WA Cities-West
King County
Large Urban Counties-West
National Emer. Number Assn
Verizon
WA Assn of Sheriffs & Chiefs
WA Independent Tel. Assn
State Dept of Health
Washington State Patrol
State Assn of Counties-East
State Assn of Fire Chiefs
State Council of Police
State Interoperability Executive Committee
TAG/Mil Dept Dir
WSP
State EMD
DOT
DIS
Fire Chiefs/ Marshals
Sheriffs/Police Chiefs
Cities/Counties
City/County EMD
As of Mar 2005

APPENDIX B

Regional Homeland Security Coordination Districts (RHSCD)



[1]**Note: These coincide with Local Health Regions for Public Health Emergency Planning and Coordination.**

APPENDIX C

METROPOLITAN MEDICAL RESPONSE SYSTEM (MMRS)	
GOAL: To ensure EMS services are effectively and appropriately dispatched, and provide pre-hospital triage, treatment, transport and tracking of patients, and documentation of the incident while maintaining the capabilities of the EMS system for continued operations.	
MMRS OBJECTIVES	**CROSSWALK TO SUPPORTING HLS OBJECTIVE**
Increase operational efficiency in mass casualty triage, pre-hospital treatment and transportation to appropriate definitive care facilities for all-hazard events.	5.4.5-5.4.6, 7.1.1-7.2.1
Develop appropriate dispatch and support of emergency medical care personnel and resources.	7.1.1, 7.1.2
Establish NIMS compliant medical command and control.	5.1.1
Increase logistical capabilities to address equipment, safety, transportation and PPE requirements of responders as well the need to organize and distribute medical supplies.	5.5.1, 5.5.2
Increase Quarantine and Isolation preparedness for a large number of persons and sizeable geographic area(s).	7.1.4
Explore the types of GIS data available through the Federal Geospatial-One-Stop portal and its applications to MMRS systems.	4.1.4
Build Pharmaceutical Cache Management and Status Reporting capability.	7.2.1
Conduct initial and on-going pre-hospital triage to include a patient tracking system, adequate decontamination prior to treatment and transportation, and movement to secure and adequate pre-hospital treatment areas.	7.1.5
Provide adequate field treatment by establishment of immediate, minor and delayed treatment areas. Ensure documentation of patient treatment and conditions per mass casualty protocols.	7.1.6
Develop radiological medical and health effects preparedness to manage exposed and contaminated victims, population protection, and environmental health impacts of a radiological release/nuclear detonation by terrorists.	7.1.3
EMERGENCY MANAGEMENT PERFORMANCE GRANT (EMPG)	
PROGRAM GOALS/OBJECTIVES	**CROSSWALK TO SUPPORTING OBJECTIVE**
1. To facilitate the identification, development, implementation, and evaluation of hazard vulnerabilities and risks that may impact the State of Washington.	4.1.1
2. Enhance disaster resistance of Washington communities by facilitating the development, implementation, and evaluation of hazard mitigation strategies and activities to reduce statewide vulnerability to the effects of identified hazards.	4.1.1
3. To facilitate a coordinated planning process integrating emergency management plans to include federal, state, and local governments, tribal nations, communities, and the private sector.	1.1.1
4. To coordinate emergency operations facilities and resources to assist local governments, tribes, and state agencies to effectively and efficiently respond to emergencies and disasters.	1.1.2
5. Manage, maintain, repair, and upgrade telecommunications systems to support EMD's strategic objectives for integrated emergency management.	2.2.1
6. Periodically review and improve emergency management telecommunications plans, policies and practices with internal and external partners to improve emergency management telecommunications readiness.	2.2.1
7. Provide quality "all-hazard" training, which meets customers' needs through cooperative partnerships and innovative practices.	5.6.1
8. Develop, conduct, and evaluate disaster related exercises that maximize emergency management proficiency for State and Local governments.	5.4.3
9. To coordinate a partnership of state agencies, local governments and the private sector to educate the public in emergency and disaster preparedness.	5.6.1
10. To ensure EMPG strategic goals, objectives, operational capabilities, and resource requirements are in support of day-to-day preparedness, response, and recovery activities.	5.1.1-5.6.2, 6.1.1-6.1.3

APPENDIX D

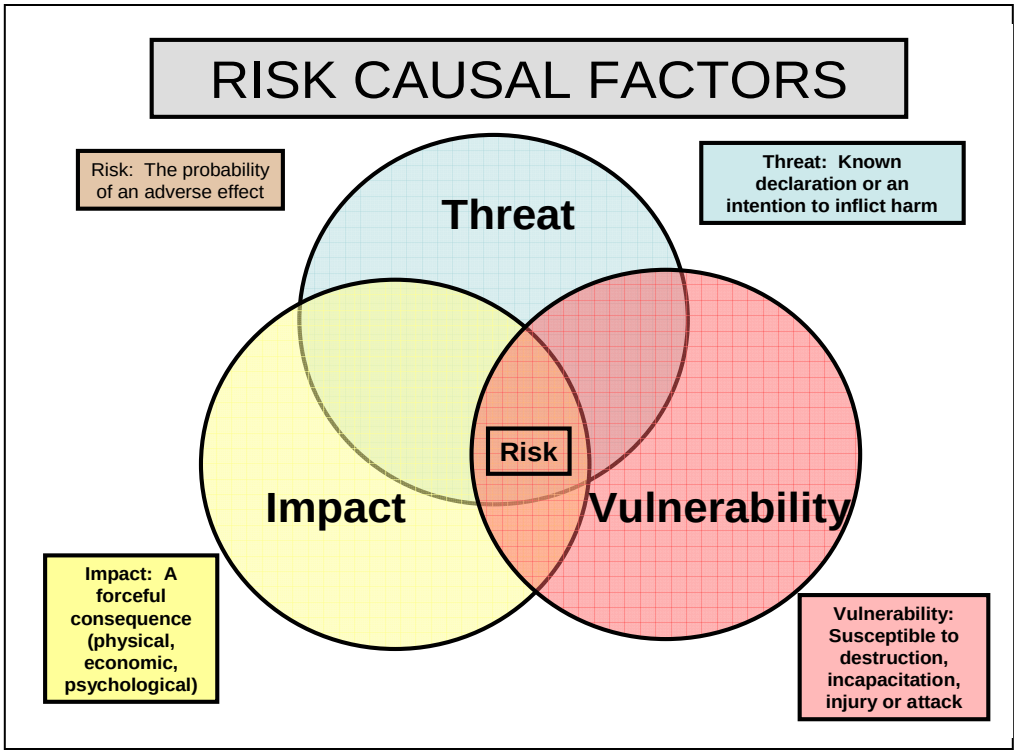
We would like to acknowledge the TEAM WASHINGTON partners for the tremendous statewide input that we received.

- Governor's Domestic Security Executive Group
- Washington State Emergency Management Council (EMC)
- EMC Task Force on Local Programs
- Committee on Homeland Security
- Washington State Emergency Management Division
- Washington National Guard and U.S. Northern Command
- Washington Military Department
- Regional Homeland Security Coordination Group
- Washington State Board for Community and Technical Colleges
- Washington State Emergency Management Association
- Washington Comprehensive Emergency Management Plan (CEMP)
- Emergency Support Function (ESF) Points of Contact
- Association of Washington Businesses
- Pacific Northwest Economic Region
- American Red Cross
- Native American Tribes and Governor's Office of Indian Affairs
- Governor's Policy Advisor and Budget Assistant
- Federal Emergency Management Agency (FEMA) Region X
- Region 6 Emergency Management Advisory Council
- Pacific Northwest National Laboratory
- Washington Labor Council
- Washington State Cities and Counties
- Washington State Patrol
- Washington State Fire Marshal
- Washington State Department of Health
- Washington State Department of Information Services
- Washington State Office of the Attorney General
- Washington State Department of Transportation
- Washington State Department of Agriculture
- Washington State Department of Licensing
- Washington State Office of the Superintendant of Public Instruction
- Washington Citizen Corps/CERT Coordinator
- Washington Commission for National & Community Service/State Citizen Corps Councils
- Washington Public Ports Association
- Washington State Ferries
- Emergency responders (Fire, EMS, Health, Police, Sheriff, E911, Search and Rescue Emergency Managers)
- Washington Association of Sheriffs & Police Chiefs
- Washington State Association of Fire Chiefs
- Washington Association of Hospitals
- Association of Washington Cities
- Association of Washington Counties
- Washington Wing, Civil Air Patrol
- Washington Association of Contingency Planners
- Washington State Hospital Association
- Washington Public Ports Association
- Washington State Association of Local Public Health Officials
- Washington Poison Center
- Washington EMS and Trauma Care Steering Committee
- Washington Computer Incident Response Center (WACIRC)
- Association of County/City Information Services (ACCIS)
- American Public Works Association
- Washington Voluntary Organizations Active in Disasters
- Washington Water and Sewer Association
- Washington State Water Resources Association
- Pierce College Homeland Security Center of Excellence

APPENDIX E

RISK, THREAT, VULNERABILITY & IMPACT

To assess Washington State risk, we are collaboratively working to define, evaluate, and analyze our domestic security environment. We define "risk" to be the probability of an adverse effect within the state that is the result of the combined effects of threat, vulnerability, and impacts. "Threats" are the known intentions of terrorist actors to inflict harm. Correspondingly, "Vulnerability" is the degree of susceptibility to attack resulting in destruction, incapacitation, and injury. "Impact" is the resulting destructive consequence, which can be physical, cyber, environmental, economic, and psychological or a combination of these or other consequences. As we analyze and evaluate, we must consider all components - threats, vulnerability and impacts - to determine the complete picture of risks to the state. We must continually access the degree of risk on whether we are susceptible to known or suspected threats and these potential consequences.



Within the terrorism spectrum, there have been numerous documented terrorist threats, extremist group activities, and incidents of terrorist cells operating within our borders. The specific threats and events involved conventional weapons, improvised or high-yield explosive devices, bioterrorism hoaxes, and attempted cyber attacks. The statewide strategy addresses all aspects of the threat spectrum to include a developing framework for the prevention of terrorism and improving our ability to respond rapidly to restore normalcy, thereby preventing a terrorist from "succeeding" in any attempt to harm state interests.

Terrorism

Terrorists use many conventional means to achieve their objectives - of greatest concern, is the use of Weapons of Mass Destruction (WMD). Experts generally agree that there are five categories of WMD: chemical, biological, radiological, nuclear, and explosive (CBRNE).

Chemical, Biological, Radiological, Nuclear, High-Yield Explosive (CBRNE)

Chemical agents are potentially lethal, relatively inexpensive, and easy to produce. Washington State hosts an extensive, legitimate chemical industry that produces chemicals that can also be used as terrorist weapons. A chemical attack is defined as the deliberate release of a toxic agent (gaseous, liquid, or solid) that can poison people or the environment. The effects of chemical agents absorbed through the skin or mucous membranes are usually immediate, obvious, and require rapid mobilization of all levels of emergency responders. Readily available, these weapons have been used in terrorist acts, such as the 1995 Tokyo subway incident perpetrated by the Aum Shinrikyo cult.

Biological agents are also lethal, accessible, and capable of being weaponized for mass dissemination of small-particle aerosols. Many biological agents can be adapted by terrorists and released into a population or environment. The effects may not be immediately known, giving the infectious agent time to rapidly spread. A biological incident will most likely be recognized in a hospital emergency room, medical examiner's office, or within the public health community long after the initial release. Biological outbreaks require rapid procurement and mass distribution of drugs and vaccines to treat, and contain the outbreak to avoid mass casualties and panic.

Radiological weapons or "dirty bombs" combine radioactive material with conventional explosives to create a radiological dispersion device. Radioactive materials range from highly-controlled uranium or plutonium to low-grade materials commonly used to treat illness, sterilize equipment, inspect welding seams, and irradiate food. The force of the explosion and radioactive contamination will be more localized than in a nuclear blast. The presence of radiation may not be detected until trained personnel with specialized equipment are on the scene. With limited exposure, it is unlikely that radioactive materials contained in a dirty bomb would result in serious health effects or death, which would more likely occur as a result of the explosion itself.

Nuclear threats include the actual detonation of a nuclear bomb or device. Detonation of a nuclear device would produce high temperatures, sharp increases in atmospheric pressure, flying debris, and radiation emissions. Injuries could include massive trauma, burns, blunt and puncture wounds, fractures, lacerations, flash blindness, scarring of the retinas and radiation exposure. A nuclear attack would create a public health crisis calling for immediate treatment and subsequent fallout responses. Additionally, of a nuclear device generates Electro Magnetic Pulse (EMP) and Transient Radiation Effects on Electronics (TREE), which both affect communications and computer systems causing widespread system failures and blackout expanding device effects beyond the Collateral Damage Distance (CDD) of the device.

Explosive incidents account for 70 percent of all terrorist attacks worldwide. Incendiary devices are mechanical, electrical, or chemical devices used to intentionally initiate combustion and start fires. The Internet and local libraries provide ample information on the design and construction of explosive devices. Targets range from small gatherings (suicide bombers) to structures containing thousands of people (vehicle bombs). These devices may be used singularly or in combination and can cause death, injury, and chaos within our communities. Additionally, manufacturing activities often involve hazardous materials that have a potential for use by terrorists as explosives. Equally dangerous is the explosive potential of terrorist acts against shipments of hazardous materials such as fuels or other flammable products.

Cyber-Terrorism

Cyber-terrorism is a relatively new method of attack that can seriously disrupt our society and exploit our reliance on computers and telecommunication networks. Cyber-terrorism threatens the electronic infrastructure supporting the social, health, and economic well-being of Washington state's population. Interlinked computer networks regulate the flow of power, water, financial services, medical care, telecommunication networks, and transportation systems. These networks are vulnerable to attack, and it is difficult to distinguish a singular hacker-type incident from a cyber-terrorist attack or to determine the source of an attack. The tools for conducting cyber-terrorism are widely available, broadly advertised, and easily used. The consequences can be quite severe causing chaos, panic, disruption of operations, and economic losses.

Agriterrorism

Agriterrorism is the malicious use of plant insect pests or pathogens, or animal pathogens to cause devastating damage in the agricultural sector. The introduction of chemical, biological, radiological substances to cause either real or perceived damage to agriculture and aquaculture in Washington could cause irreparable harm to our economy. Anti-livestock pathogens are of the greatest concern because they can be introduced relatively easily and spread quickly. The insect pests and plant pathogens designed to attack existing crops are thought to be less effective weapons because they spread slowly and unreliably, and are highly influenced by weather. It would be difficult to cause the widespread destruction of a crop because most crops are not grown in isolation and have already been exposed to many pathogens, thereby increasing their resistance to infection. The infection of seed may also be a source of introduction. There are several factors that increase the state and nation's vulnerability to agriterrorism to include:

- Many agents are lethal and highly contagious to animals.
- Several agents are non-zoonotic allowing transport by a terrorist without special precautions or training.
- Antibiotic and steroid programs, and husbandry programs designed to improve quality and quantity of meat, have made U.S. livestock more susceptible to exotic disease.
- Animal populations are highly concentrated, and large herds make ideal targets for infection and contagion.
- Animal populations are highly mobile, creating conditions where animals that are incubating disease can increase the spread of disease during transport.
- Agricultural facilities are not highly secure, and the U.S. currently has limited detection capabilities.
- Aquaculture and aquaculture facilities are not highly secure with limited detection capabilities and can be easily affected by deliberate contamination.

The impact of an agriterrorism or aquaculture attack would be the economic impact of agricultural losses and subsequent impacts to our economy. One in eight jobs nationally depends on food production. In addition, a successful agriterrorism attack would undermine confidence in our ability to protect the citizens of this country.

Natural Disasters

Earthquake: An earthquake is the sudden release of stored energy; most earthquakes occur along a fracture within the earth, called a fault. The shaking caused by this sudden shift is often very small, but occasionally large earthquakes produce very strong ground shaking. It is this strong shaking and its consequences – ground failure, landslides, liquefaction – that damages buildings and structures and upsets the regional economy.

Tsunami: The Pacific Coast, Strait of Juan de Fuci, Puget Sound, and large lakes are at risk from tsunamis, trains of waves that threaten people and property along shorelines. Sudden raising or lowering of the Earth's crust during earthquakes generally causes a tsunami, although landslides and underwater volcanic eruptions also can generate them. Movements of the sea floor or lakebed, or rock fall into an enclosed body of water, displace the water column, setting off a series of waves that radiate outward as pond ripples. Only as a tsunami approaches land does it become a hazard; in shallow water, it gains height as its waves slow and compress.

Floods: Floods cause loss of life and damage to structures, crops, land, flood control structures, roads, and utilities. Floods also cause erosion and landslides, and can transport debris and toxic products that cause secondary damage. Flood damage in Washington State exceeds damage by all other natural hazards. There have been 28 Presidential Major Disaster Declarations for floods in Washington State from 1956 through October 2003. Every county has received a Presidential Disaster Declaration for flooding since 1970. While not every flood creates enough damage to merit such a declaration, most are severe enough to warrant intervention by local, state or federal authorities.

Wildland Fires: Wildland fires are fires caused by nature or humans that result in the uncontrolled destruction of forests, brush, field crops, grasslands, and real and personal property. The wildland fire season in Washington usually begins in early July and typically culminates in late September with a moisture event; however, wildland fires have occurred in every month of the year. Drought, snow pack,

and local weather conditions can expand the length of the fire season. The early and late shoulders of the fire season usually are associated with human-caused fires. Lightning generally is the cause of most fires in the peak fire period of July, August and early September.

Volcano: A volcano is a vent in the earth's crust through which magma, rock fragments, gases, and ash are ejected from the earth's interior. Over time, accumulation of these erupted products on the earth's surface creates a volcanic mountain. Washington State has five major volcanoes in the Cascade Range – Mount Baker, Glacier Peak, Mount Rainier, Mount St. Helens and Mount Adams. Volcanoes can lie dormant for centuries between eruptions, and the risk posed by volcanic activity is not always apparent. When Cascades volcanoes do erupt, high speed avalanches of hot ash and rock called pyroclastic flows, lava flows, and landslides can devastate areas 10 or more miles away, while huge mudflows of volcanic ash and debris called lahars can inundate valleys more than 50 miles downstream.

Mount Rainier (above) and the Olympic National Park (right)

Photos courtesy of Access Washington

APPENDIX F

HOMELAND SECURITY ACRONYM KEY

AAPA	American Association of Port Authorities
AAR	After Action Report
AASHTO	American Association of State Highway and Transportation Officials
AC	Hydrogen Cyanide (a blood agent)
ACCIS	Association of County/City Information Services
ACOE	Army Corps of Engineers
ACS	Automated Case System (FBI)
ADIS	Arrival Departure Information System
ADNET	Anti-Drug Network
AEL	Authorized Equipment List
AGILE	Advanced Generation of Interoperability for Law Enforcement
AGO	WA State Attorney General's Office
AIS	Automatic Identification System (Maritime)
ALI	Automatic Location Identification
AMC	Army Material Command (U.S. Army)
AMI	Air and Marine Interdiction Program
AMS	Automated Manifest System
ANSI	American National Standards Institute
AOR	Area of Responsibility
APCO	Association of Public-Safety Communications Officials
APHIS	Animal & Plant Health Inspection Service (DHS)
APHL	Agency for Public Health Laboratories
APIS	Advance Passenger Information System
APTA	American Public Transportation Association
ARAC	Atmospheric Release Advisory Capability (DOE)
ARC	American Red Cross
ARES	Amateur Radio Emergency Services
ARG	Accident Response Group (DOE)
ASCR	Advanced Scientific Computing Research
ASP	Alternative Security Program (Non-SOLAS Vessels)
ASCR	Advanced Scientific Computing Research
ASTHO	Association of State and Territorial Health Officials
ATAC	Anti-Terrorism Advisory Council
ATIX	Anti-Terrorism Information Exchange
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATSDR	Agency for Toxic Substances and Disease Registry
ATTF	Anti-Terrorism Task Force
AVIC	Area Veterinary in Charge
AWB	Association of Washington State Business
AWC	Association of Washington Cities
AWI	Asymmetric Warfare Initiative
BATFE	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BATS	Bombing and Arson Tracking System (ATF)
BCBP	Bureau of Customs & Border Security
BCIS	Bureau of Citizenship and Immigration Services
BCRT	Regional Drug Task Force Biological/Chemical Response Team
BCS	Border Cargo Selectivity
BDRP	Biological Defense Research Program (U.S. Navy)
BER	Biological and Environmental Research
BERT	Public Health Bioterrorism Emergency Response Team
BICE	Bureau of Immigration and Customs Enforcement
BOLO	Be On the Lookout
BRAC	Bioterrorism Response Advisory Committee

BRTC	Border Research Technology Center
BSI	Base Support Installation
BSIR	Biannual Strategy Implementation Reports (Grants)
BT	Bioterrorism
BTS	Border & Transportation Security Directorate (DHS)
BW	Biological Warfare
BZPP	Buffer Zone Protection Plan
C2	Command and Control
CA	Civil Affairs
CAC	Crisis Action Center
CAEC	County Animal Emergency Coordinator
CAIRA	Chemical Accident/Incident Response and Assistance
CAP	Civil Air Patrol
CAP	Corrective Action Plan
CAPR	Categorical Assistance Progress Reports (Grants)
CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability
CAW	Center for Asymmetric Warfare
CBIRF	Chemical and Biological Incident Response Force (U.S. Marine Corps)
C/B-RRT	Chemical Biological Rapid Response Team (U.S. Army)
CBDCOM	Chemical Biological, Defense Command (U.S. Army)
CBO	Community Based Organizations
CBP	Customs and Border Protection (part of DHS)
CBPMO	Customs and Border Patrol Modernization Office
CBRED	Chemical, Biological, Radiological, Environmental Defense Response (U.S. Navy)
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCP	Citizen Corps Program
CCRF	Commissioned Corps Readiness Force (PHS)
CD	Communicable Disease
CDC	Centers for Disease Control and Prevention
CDRG	Catastrophic Disaster Response Group
CDAT	Columbia Data Analysis Team
CDC	Center for Disease Control and Prevention
CDP	Center for Domestic Preparedness
CEMNET	Comprehensive Emergency Management Network
CEMP	Comprehensive Emergency Management Plan
CERCLA	Comprehensive Environmental Response, Compensation and Liability Act
CERFP	Chemical, Biological, Radiological, Nuclear and High Yield Explosives Enhanced Response Force Package
CERT	Community Emergency Response Teams
CFA	Capability Focus Area
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulation
CG	Phosgene (a choking agent)
CHER-CAP	Comprehensive HAZMAT Emergency Response – Capability Assessment Program
CHIP	Computer Hacking and Intelligence Property
CHS	Committee on Homeland Security (Washington State)
CIAO	Critical Infrastructure Assurance Office
CI/KR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIRA	Catastrophic Incident Response Annex
CIRC	Computer Incident Response Center
CIRG	Critical Incident Response Group
CIP	Critical Infrastructure Protection
CIS	Citizenship and Immigration Services
CISM	Critical Incident Stress Management
CIVA	Critical Infrastructure Vulnerability Assessment
CK	Cyanogen Chloride (a blood agent)
CLASS	Consular Lookout and Support System
CLOREP	Chlorine Emergency Plan

CMT	Crisis Management Team
COA	Course of Action
COG	Continuity of Government
CONPLAN	U.S. Government Interagency Domestic Terrorism Concept of Operations Plan
COOP	Continuity of Operations
COPS	Office of Community Oriented Policing Services (DOJ)
COP	Common Operating Picture
CPARM	Contingency Planning and Recovery Management Group
CPTED	Crime Prevention Through Environmental Design
CPX	Command Post Exercise
CRRA	Capabilities Review and Risk Assessment
CS	Civil Support
CSEPP	Chemical Stockpile Emergency Preparedness Program
CSA	Customs Self-Assessment
CSI	Container Security Initiative
CSID	Centralized Scheduling and Information Desk (ODP Desk for Reports)
CSG	Council of State Governments
CST	Civil Support Team
CSTARC	Cyber Security Tracking Analysis and Response Center
CSTE	Council of State and Territorial Epidemiologists
CT	Counter-Terrorism
CTAC	Counter-Drug Technology Assessment Center
CTC	Counter-Terrorism Center
C-TPAT	Customs-Trade Partnership Against Terrorism
CX	Phosgene Oxime (a blister agent)
DAE	Disaster Assistance Employee (also called SAE for Stafford Act Employee)
DCD	Disease Conditions Database
DCE	Defense Coordinating Element
DCO	Defense Coordinating Officer
DDO	Deputy Director for Operations
DEA	Drug Enforcement Administration
DEM	Director of Emergency Management
DEST	Domestic Emergency Support Team
DFO	Disaster Field Office
DHS	United States Department of Homeland Security
DHHS	United States Department of Health and Human Services
DIA	Defense Intelligence Agency
DIS	Washington State Department of Information Services
DIST	Disaster Information Systems Clearinghouse
DMAT	Disaster Medical Assistance Team (FEMA)
DMORT	Disaster Mortuary Operational Response Team (FEMA)
DNR	Washington State Department of Natural Resources
DPETAP	Domestic Preparedness Equipment Technical Assistance Program
DSHS	Washington State Department of Social and Health Services
DOC	United States Department of Commerce
DOD	United States Department of Defense
DOE	United States Department of Energy
DOI	United States Department of the Interior
DOJ	United States Department of Justice
DOS	United States Department of State
DOT	United States Department of Transportation
DRC	Disaster Recovery Center
DRM	Disaster Recovery Manager
DSEG	Governor's Domestic Security Executive Group
DT	Domestic Terrorism
DUNS	Data Universal Numbering System (Grants)
DWI	Disaster Welfare Inquiry
EAO	Energy Assurance Office
EAS	Emergency Alert System

EC	Emergency Coordinator
EDI	Electronic Data Interchange
EEG	Exercise Evaluation Guide
EEI	Essential Elements of Information
EFSEC	Energy Facility Site Evaluation Council
EFR	Emergency Responder
EHP	Environmental Health Program, Health Department
EICC	Emergency Information and Coordination Center (FEMA)
EIS	Epidemic Intelligence Service
EMA	Emergency Management Agency (local)
EMC	Washington Emergency Management Council
EMD	Washington State Emergency Management Division
EMAC	Emergency Management Assistance Compact
EMPG	Emergency Management Performance Grants
EMRT	Emergency Medical Response Team
EMS	Emergency Medical Services
EO	Executive Order
EOC	Emergency Operations Center
EOD	Explosive Ordnance Disposal
EOF	Emergency Operations Facility
EOP	Emergency Operations Plan or Procedures
EPA	U.S. Environmental Protection Agency
EPCRA	Emergency Planning Community Right-to-Know Act
EPLO	Emergency Preparedness Liaison Officer
EP&R	Emergency Preparedness and Response (DHS)
EPW	Exercise Planning Workshop
EPZ	Emergency Planning Zone
ERAMS	Environmental Radiation Ambient Monitoring System (EPA)
ERC	Emergency Response Coordinator
ERDO	Emergency Response Duty Officer
ERT	Emergency Response Team
ERT	Evidence Response Team (FBI)
ERT	Environmental Response Team (EPA)
ERT-A	Emergency Response Team – Advanced Element
ERT-N	National Emergency Response Team
ESA	Energy Security and Assurance
ESA	Environmentally Sensitive Area
ETC	Emergency Telecommunications
ESD	Educational Service Districts
ESF	Emergency Support Function
EST	Emergency Support Team (FEMA)
ESSENCE	Electronic Surveillance System for the Early Notification of Community-based Epidemics
FAA	Federal Aviation Administration
FAMS	Federal Air Marshall Service
FAR	Federal Acquisition Regulations
FAS	Federation of American Scientists
FAST CORRIDOR	Freight Action Strategy for the Everett-Seattle-Tacoma Corridor
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	U.S. Food and Drug Administration
Fed CIRC	Federal Computer Incident Response Center
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FERC	FEMA Emergency Response Capability
FESC	Federal Emergency Support Coordinator
FHWA	Federal Highway Administration
FID	Flame Ionization Detector
FINCEN	Financial Crimes Enforcement Network

FIRECOM	Fire Communications
FLETC	Federal Law Enforcement Training Center
FMAC	Freight Mobility Advisory Committee
FMSIB	Freight Mobility Strategic Investment Board
FOA	Field Operating Agency
FOC	FEMA Operations Center
FOG	Field Operations Guide
FOIA	Freedom of Information Act
FPF	Fallout Protective Factor
FRA	Federal Railroad Association
FRP	Federal Response Plan
FRERP	Federal Radiological Emergency Response Plan
FRMAC	Federal Radiological Monitoring and Assessment Center
FPS	Federal Protective Service
FS	Fire Service
FSE	Full Scale Exercise
FSR	Financial Status Report (Grants)
FSS	Federal Supply Service
FTA	Federal Transit Administration
FTTTF	Foreign Terrorist Tracking Task Force
FTS	Federal Telecommunications System
FY	Fiscal Year
GA	Governmental Administrative
GA	Tabun (a nerve agent)
GAN	Grant Adjustment Notice
GB	Sarin (a nerve agent)
GCJIN	Global Criminal Justice Information Network
GC/MS	Gas Chromatograph/Mass Spectrometer
GD	Soman (a nerve agent)
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information Systems
GMDSS	Global Maritime Defense and Safety System
GMS	Grants Management System
GPS	Global Positioning System
GTIN	Global Trade Identification Number
H	Impure Sulfur Mustard (a blister agent)
HACCP	Hazard Analysis and Critical Control Point
HAZCAT	Hazard Categorizing
HAZMAT	Hazardous Material
HAN	Health Alert Network
HAN LAP	Health Alert Network Local Health Assistance Project
HC	Health Care
HD	Homeland Defense
HD	Distilled Sulfur Mustard (a blister agent)
HDER	Homeland Defense Equipment Reuse Program
HEAR	Hospital Emergency Administrative Radio
HEICS	Hospital Emergency Incident Command System
HEPA	High Efficiency Particulate Air
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
HIVA	Hazard Identification and Vulnerability Assessment
HHS	Department of Health and Human Services
HLS	Homeland Security
HLT	Hurricane Liaison Team (FEMA)
HLW	High Level Waste
HMRU	Hazardous Materials Response Unit (FBI)
HN	Nitrogen Mustard (a blister agent)
HP	Health Physicist
HRSA	Health Resources and Services Administration

HSAS	Homeland Security Advisory System
HSARPA	Homeland Security Advanced Research Projects Agency
HSC	Homeland Security Council
HSEEP	Homeland Security Exercise and Evaluation Program
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HSPTAP	Homeland Security Preparedness Technical Assistance Program
HSOC	Homeland Security Operations Center
HUMINT	Human Intelligence
HZ	Hazardous Materials Personnel
HazMat	Hazardous Materials
IA	Information Analysis
IAB	Interagency Board
IAEA	International Atomic Energy Agency
IACP	International Association of Chiefs of Police
IAD	Information Assurance Directorate
IAFC	International Association of Fire Chiefs
IAFIS	Integrated Automated Fingerprint Identification System
IAIP	DHS Information Analysis and Infrastructure Protection Directorate
IALEIA	International Association of Law Enforcement Intelligence Analysts
IAP	Incident Action Plan
IC	Incident Command
ICAP	Incident Communications Action Plan
ICDDC	Interstate Civil Defense and Disaster Compact
ICE	Immigration and Customs Enforcement
ICP	Incident Command Post
ICRI	Incident Commander's Radio Interface
ICS	Incident Command System
IDD	Industrial Development District
IDENT	Automated Biometric Identification System (INS)
IED	Improvised Explosive Device
IGA	Intergovernmental Agreement
IGN	Intergovernmental Network
IIMG	Interagency Incident Management Group
IIPO	Information Integration Program Office
IIT	Nuclear Regulatory Commission's Incident Investigation Team
IMPC	International Materials Protection & Cooperation
IMS	Incident Management System
IMSA	International Municipal Signal Association, Inc.
IMT	Incident Management Team
IND	Improvised Nuclear Device
INRP	Initial National Response Plan
INS	Immigration and Naturalization Service
INSPASS	INS Passenger Accelerated Service System
IO	Information Operations
IOF	Interim Operating Facility
IP	Infrastructure Protection
IP	Improvement Plan
IPFO	Interim Principal Federal Official
IR	Incident Response
IRIS	Incident Response Information System
IS	Information Superiority
ISA	Importer Self Assessment
ISAC	Information Sharing Analysis Centers
ISO	International Standards Organization
ISPS	International Ship and Port Facility Security Code
ISR	Intelligence, Surveillance, and Reconnaissance
IST	Incident Support Team

IT	International Terrorism
ITI	International-to-International Transit Program
ITDS	International Trade Data System
ITS	Institute for Telecommunications Sciences
IW	Information Warfare
IWG	Infrastructure Working Group
IWN	Integrated Wireless Network
JCN	Justice Consolidated Network
JDCC	Joint Data Coordination Center
JFO	Joint Field Office
JHOC	Joint Harbor Operations Center
JIC	Joint Information Center
JIS	Joint Information System
JOC	Joint Operations Center
JPA	Joint Powers Authority
JRAC	Joint Rear Area Coordinators
JRIES	Joint Regional Information Exchange System
JTF	Joint Task Force
JTTF	Joint Terrorism Task Force
JTWG	Joint Terrorism Working Group
JWICS	Joint World-wide Intelligence Communication System
LCAT	Logistics Closeout Assistance Teams
L	Lewisite (a blister agent)
LE	Law Enforcement
LEA	Law Enforcement Agency
LEISP	Law Enforcement Information Sharing Program
LEIU	Law Enforcement Intelligence Unite
LEO	Law Enforcement Online
LEOC	Local Emergency Operations Center
LEPC	Local Emergency Planning Committee
LERC	Local Emergency Response Coordinator
LERN	Law Enforcement Radio Network
LETPP	Law Enforcement Terrorism Prevention Program
LFA	Lead Federal Agency
LHJ	Local Health Jurisdictions
LIMS	Laboratory Information Management System
LLEA	Lead Law Enforcement Agency
L-LERC	Local Lead Emergency Response Coordinator
LLIS	Lessons Learned Information Sharing System
LLW	Low Level Waste
LNO	Liaison Officer
LOCES	Letter of Credit Electronic Certification System
LPHA	Local Public Health Agency
LPHS	Local Public Health System
LRN	Laboratory Response Network
MAA	Mutual Aid Agreement
M & A	Management and Administrative Costs (Grants)
MAC Group	Multi-Agency Coordinating Group
MACA	Military Assistance to Civil Authorities
MACS	Multi-Agency Coordination Systems
MARIP	Multiple Agency Radio Interoperability Program
MARSEC	Maritime Security Level
MCBAT	Medical Chemical and Biological Advisory Teams (U.S. Army)
MCTFER	Military-Civilian Task Force for Emergency Response
MEDNET	Medical Emergency Delivery Network
MILES	Miles Integrated Laser Engagement System
MIPT	National Memorial Institute for the Prevention of Terrorism
MLAT	Mutual Legal Assistance Treaty
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
MMRS	Metropolitan Medical Response System
MRC	Medical Reserve Corps
MRTE	Medical Readiness, Training and Education Committee
MS&G	Models, Simulations or Games
MTCR	Missile Technology Control Regime
MTSA	Maritime Transportation Security Act
MSA	Metropolitan Statistical Area
MSCA	Military Support to Civil Authorities
NABC	National Agricultural Bio-Security Center
NAC	Nebraska Avenue Complex
NACCHO	National Association for County and City Health Officials
NAED	National Academy of Emergency Dispatch
NAWAS	National Warning System
NBDAC	National Bio-Weapons Defense Analysis Center
NCAP	National Customs Automation Program
NCC	National Coordinating Center
NCIC	National Crime Information Center
NCID	National Center for Infectious Disease
NCIS	Naval Criminal Investigative Services
NCJA	National Criminal Justice Association
NCHRP	National Cooperative Highway Research Program
NCP	National Oil and Hazardous Substances Pollution Contingency Plan
NCPHP	Northwest Center for Public Health Preparedness
NCJRS	National Criminal Justice Reference Service
NCP	National Contingency Plan
NCPHP	Northwest Center for Public Health Preparedness
NCR	National Capitol Region
NCRP	National Council on Radiation Protection and Measurements
NCS	National Communications System
NCSD	National Cyber Security Division
NCSL	National Conference of State Legislatures
NDMOC	National Disaster Medical Operations Center
NDMS	National Disaster Medical System
NDPC	National Domestic Preparedness Consortium
NEDSS	National Electronic Disease Surveillance System
NEIS	National Earthquake Information Service
NENA	National Emergency Number Association
NEMA	National Emergency Managers Association
NEOC	National Emergency Operations Center (FEMA)
NERRTC	National Emergency Response and Rescue Training Center
NERP	National Emergency Repatriation Plan
NEST	National Emergency Search Team (DOE)
NFDA	National Funeral Directors Association
NFPA	National Fire Protection Association
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NGO	Non-Governmental Organization
NIAID	National Institute of Allergy & Infectious Disease
NIBRS	National Incident-Based Reporting System
NIC	NIMS Integration Center
NIC	National Incident Commander
NICC	National Interagency Coordination Center
NICS	National Instant Criminal Background Check System
NIFCC	National Interagency Fire Coordination Center
NIH	National Institute of Health
NIJ	National Institute of Justice
NIMA	National Imagery and Mapping Agency
NIMS	National Incident Management System

NIIMS	National Interagency Incident Management System
NIIS	Non-Immigrant Information System
NIIT	Non-Intrusive Inspection Technology
NIOSH	National Institute for Occupational Safety & Health
NIPC	National Infrastructure Protection Center
NIPP	National Infrastructure Protection Plan
NIRT	Nuclear Incident Response Team
NISA	National Infrastructure Simulation & Analysis
NIST	National Institute of Standards & Technology
NLECTC	National Law Enforcement and Corrections Technology Centers
NLETS	National Law Enforcement Telecommunications System
NMRT	National NBC Medical Response Team (HHS)
NOAA	National Oceanic and Atmospheric Administration
NORTHCOM	United States Northern Command
NODP	National Office of Domestic Preparedness
NPS	National Pharmaceutical Stockpile
NRC	Nuclear Regulatory Commission
NRCC	National Resource Coordination Center
NRDA	National Resource Damage Assessment
NRP	National Response Plan
NRS	National Response System
NSA	National Security Agency
NSC	National Security Council
NSDI	National Spatial Data Infrastructure
NSEERS	National Security Entry-Exit Registration System
NSEP	National Security Emergency Preparedness
NSF	National Strike Force
NSFCC	National Strike Force Coordination Center
NSRP	National Search and Rescue Plan
NSSE	National Security Special Event
NSTS	National Secure Telecommunications System
NTAC	United States Secret Service National Threat Assessment Center
NTIA	National Telecommunications and Information Administration
NTRO	National Terrorism Response Objectives
NTSB	National Transportation Safety Board
NVAC	National Visual Analytics Center
NVOAD	National Voluntary Organizations Active in Disasters
NVOCC	Non Vessel Common Carrier
NVRD	Non-Proliferation and Verification R&D
NW WARN	Northwest Warning, Alert and Response Network
ODP	Office of Domestic Preparedness
OEP	Office of Emergency Preparedness
OER	Office of Emergency Response (DHHS)
OES	Office of Emergency Services
OGC	Office of General Counsel
OHS	Office of Homeland Security
OIA	Office of International Affairs
OJP	Office of Justice Programs
OLA	Office of Legislative Affairs
OMB	Office of Management and Budget
ONCRC	Office of National Capital Region Coordination
OPHP	Office of Public Health Preparedness (DHHS)
OPSC	Office of Private Sector Coordination
OPS-CAN	Olympic Public Safety Communications Alliance Network
OPSEC	Operational Security
OSC	On-Scene Coordinator/Commander
OSC	Operation Safe Commerce
OSCL	Office of State and Local Coordination
PA	Primary Agency

PAD	Protective Action Decision
PADO	Public Affairs Duty Office
PAG	Protective Action Guide
PAPR	Powered Air Purifying Respirator
PAPRS	Phone Activated Paperless Request System
PAPS	Pre-Arrival Processing System
PAR	Protective Action Recommendation
PASS	Personal Alert Safety System
PCAPA	Pacific Coast Association of Port Authorities
PCII	Protected Critical Infrastructure Information
PDA	Preliminary Damage Assessment
PDD	Presidential Decision Directive
PFA	Primary Federal Agency
PFO	Principal Federal Official
PHEPR	Public Health Emergency Preparedness and Response
PHL	Public Health Labs
PHIMS	Public Health Issues Management System
PHIN	Public Health Information Network
PHPPO	Public Health Practice Program Office (CDC)
PHS	Public Health Service
PHTN	Public Health Training Network
PIR	Priority Intelligence Requirements
PIO	Public Information Officer
PIP	Partners In Protection
PNEMA	Pacific Northwest Emergency Management Arrangement
PNR	Passenger Name Record
PNWER	Pacific Northwest Economic Region
POE	Port of Entry
POD	Port of Debarkation
PODO	Press Office Duty Officer
POLREP	Pollution Report
PNNL	Pacific Northwest National Laboratory
PPA	Principal Planning Agent
PPC	Prevention and Preparedness Council
PPDS	Pre-Positioned Disaster Supplies Program
PPE	Personal Protective Equipment
PSA	Public Safety Announcement
PSAP	Public Safety Answering Point
PSC	Public Safety Communications
PSCC	Public Safety Coordinating Council
PSCDG	Primary State Core Decision Group
PSWAC	Public Safety Wireless Advisory Committee
PSWN	Public Safety Wireless Network
PTE	Potential Threat Element
PVMS	Prophylaxis and Vaccine Management System
PVO	Private Voluntary Organization
PW	Public Works
PWR	Pressurized Water Reactor
R	Roentgen
RACES	Radio Amateur Civil Emergency Services
RAD	Radiological Absorbed Dose
RAD	Risk Assessment Division
RAIN	King County Regional Automated Information Network
RAP	Radiological Assistance Program (DOE)
RAPTR	Radio Analysis Prediction Tool Repository
RCECC	Regional Communications and Emergency Coordination Center
RCP	Regional Contingency Plan
RDD	Radiological Dispersal Devices
REAC/TS	Radiation Emergency Assistance Center/Training Site (DOE)

REOC	Regional Emergency Operations Center
ROC	Regional Operations Center
ROSS	Resource Ordering and Status System
RERT	Radiological Emergency Response Team (EPA)
RETCO	Regional Emergency Transportation Coordinator
RFI	Request for Information
RFID	Radio Frequency Identification Cards
RHSCD	Regional Homeland Security Coordination Districts (WA State)
RISS	Regional Information Sharing System
RKB	Responder Knowledge Base
ROC	Regional Operations Center (FEMA)
ROSS	Resource Ordering and Status System
RPA	Regional Planning Agent
RRCC	Regional Response Coordination Center
RRIS	Rapid Response Information System (FEMA)
RRT	Regional Response Team
RRTF	Washington State Recovery and Restoration Task Force
RTF	Response Task Force (DOD)
RTII	Regional Technology Integration Initiative
RQ	Reportable Quantity
SA	Support Agency
SAA	State Administrative Agency (Grants)
SAC	Special Agent in Charge (FBI)
SAFECOM	Project Safe Communications (U.S.)
SAR	Search and Rescue
SARDA	State and Regional Disaster Airlift Plans
SBU	Sensitive But Unclassified
SCBA	Self Contained Breathing Apparatus
SCI	State Critical Infrastructure
SCIF	Sensitive Compartmented Information Facility
SCM	Survivable Crisis Management
SCO	State Coordinating Officer
SDWG	Strategy Development Working Group (CHS)
SEB	Staphylococcus Entreotoxin B (a tox)
SEL	Standardized Equipment List
SENTRI	Secure Electronic Network for Traveler Rapid Inspection
SEOC	State Emergency Operations Center
SERC	State Emergency Response Commission
SERRP	State Emergency Response and Recovery Plan
SEVIS	Student and Exchange Visitor Information System
SFLEO	Senior Federal Law Enforcement Official
SGSGP	State Homeland Security Grant Program
SIEC	State Interoperability Executive Committee (Washington State)
SIOC	Strategic Interagency Operations Center
SIPRNET	Secret Internet Protocol Router Network
SITREP	Situation Report
SGSGP	State Homeland Security Grant Program
SHSAS	State Homeland Security Assessments and Strategies
SHSP	State Homeland Security Program
SHSS	State Homeland Security Strategy
SL	State and Local Government Representative
SLA	State and Local Assistance
SLGCP	Office of State and Local Government Preparedness
SLPS	State and Local Programs and Support Directorate (FEMA)
SME	Subject Matter Expert
SNS	Strategic National Stockpile
SOLAS	International Convention Act for the Safety of Life As Sea (1974)
SOP	Standard Operating Procedures
SoR	Statement of Requirements

SPOC	Single Point of Contact (Grant Review)
SRO	School Resource Officers
SSA	Sector Specific Agency
SSCDG	Secondary State Core Decision Group
S&T	Science and Technology
START	Scientific and Technical Analysis and Response Team
STISAC	Surface Transportation Information Sharing and Analysis Center
STRACNET	Strategic Rail Corridor Network
SWAT	Special Weapons and Tactics
SWO	Senior Watch Officer
TA	Technical Assistance
TARU	Technical Advisory Response Unit
TAT	Technical Assistance Team
TC	Trauma Care
TCL	Target Capabilities List
TCP	Transmission Control Protocol
TCV	Total Containment Vessel
TEA	Threat Environment Assessment
TEDE	Total Effective Dose Equivalent
TEU	Technical Escort Unit (U.S. Army)
TEW	Terrorist Early Warning
TIA	Terrorist Incident Annex
TIIAP	Telecommunications and Information Infrastructure Assistance Program
TIP	Department of State Terrorist Interdiction Program
TIPS	Terrorism Information and Preventive Systems
TLD	Thermo luminescent Dosimeter
TMSARM	Transportation Security Administration Maritime Self-Assessment Risk Model
TOPOFF	Top Officials Exercise
TRM	Technical Reference Model
TSA	Transportation Security Administration
TSARM	TSA Self Assessment Risk Modules
TSC	United States Terrorist Screening Center
TSOB	Transportation Security Oversight Board
TSWG	Technical Support Working Group
TTIC	Terrorist Threat Integration Center
TWIC	Transportation Worker Identification Card
TWOV	Transit Without Visa Program
UA	Urban Area (UASI)
UAC	Unified Area Command
UACG	Urban Area Core Group (UASI)
UASI	Urban Area Security Initiative
UAWG	Urban Area Working Group (UASI)
UC	Unified Command
UC/IC	Unified Command/Incident Command
UCR	Uniform Crime Reports
UCS	Unified Command System
US	United States
USAR	Urban Search and Rescue
USCG	United States Coast Guard
USFA	United States Fire Administration (FEMA)
USFS	United States Forest Service
USRT	Urban Search and Rescue Team (FEMA)
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indication Technology System
UTL	Universal Task List
VACIS	Vehicle and Cargo Inspection System
VIPS	Volunteers in Police Service
VMI	Vendor Managed Inventory (SNS)
VX	A nerve agent

WAC	Washington Administrative Code
WACII	Washington State Criminal Intelligence Index
WACIRC	Washington Computer Incident Response Center
WACO	Washington Association of County Officials
WADDL	Washington Animal Disease Diagnostic Laboratory
WAEMD	Washington State Emergency Management Division
WAJAC	Washington Joint Analytical Center
WAMA	Washington Airport Managers Association
WAOL	Washington On-Line
WA SECURES	Washington State Electronic Communications and Urgent Response Exchange System
WASERC	Washington State Emergency Response Commission
WASPC	Washington Association of Sheriffs and Police Chiefs
WAPHL	Washington State Public Health Laboratories
WAVOAD	Washington Volunteer Organizations Active in Disasters
WCCMA	Washington City/County Management Association
WCIT	Washington Council on International Trade
WCNCS	Washington Commission for National & Community Services.
WEDSS	Washington Electronic Disease Surveillance System
WEIC	Washington Emergency Information Center
WMD	Weapons of Mass Destruction
WMD – CST	Weapons of Mass Destruction Civil Support Teams
WPPA	Washington Public Ports Association
WSAC	Washington State Association of Counties
WSAFC	Washington State Association of Fire Chiefs
WSALPHO	Washington State Assoc. of Local Public Health Officials
WSDA	Washington State Department of Agriculture
WSDOE	Washington State Department of Ecology
WSDOH	Washington State Department of Health
WSDA	Washington State Department of Agriculture
WSEMA	Washington State Emergency Management Association
WSPHA	Washington State Public Health Association
WSDOT	Washington State Department of Transportation
WSHA	Washington State Hospital Association
WSP	Washington State Patrol

APPENDIX G

HOMELAND SECURITY GLOSSARY

Links to Related Glossaries:

National Mutual Aid and Resource Management Initiative Glossary of Terms and Definitions (FEMA)
http://www.fema.gov/doc/preparedness/glossaryterms.doc

JCS Pub 1-02 Department of Defense Dictionary of Military and Associated Terms
http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

National Incident Management System (NIMS) Glossary of Key Terms
http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf

911 (9-1-1): Used to describe the 911 telephone systems, Public Safety Answering Points and associated radio and data systems used to receive calls for assistance from the public, catalog and triage information, direct responders to emergency locations and provide support to field responders until event closure or until particular functions are assumed by others under ICS.

Adversary: Often used as a term to describe enemies; the term enemy is reserved to indicate adversaries engaged in lethal operations against US forces.

Agency: A division of government with a specific function offering a particular kind of assistance. In ICS, agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance (NIMS, March 1, 2004)

All-Hazards Preparedness: Refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies. (Source—HSPD-8)

Anti-Terrorism: Preventive in nature and it entails using "passive and defensive measures… such as education, foreign liaison training, surveillance, and counter-surveillance, designed to deter terrorist activities." It is an "integrated, comprehensive approach … to counter the terrorist threat. The concept has two phases: proactive and reactive. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident." (JCS Pub 1-02)

Area Command (Unified Area Command): An organization established (1) to oversee the management of multiple incidents that are each being handled by an ICS organization or (2) to oversee the management of large or multiple incidents to which several Incident Management Teams have been assigned. Area Command has the responsibility to set overall strategy and priorities, allocate critical resources according to priorities, ensure that incidents are properly managed, and ensure that objectives are met and strategies followed. Area Command becomes Unified Area Command when incidents are multi-jurisdictional. Area Command may be established at an emergency operations center facility or at some location other than an incident command post. (NIMS, March 1, 2004)

Assessment: The evaluation and interpretation of measurements and other information to provide a basis for decision making (NIMS, March 1, 2004).

Assisting Agency: An agency or organization providing personnel, services or other resources to the agency with direct responsibility for incident management. (NIMS, March 1, 2004)

Asset: Anything that has value to the organization (ISO I3335-1:1996)

Attack: A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it.

Awareness: The continual process of collecting, analyzing, and disseminating intelligence, information, and knowledge to allow organizations and individuals to anticipate requirements and to react effectively. (NRP, Dec 2004)

Available Resources: Resources assigned to an incident, checked in, and available for use, normally located in a Staging Area. (NRP, Dec 2004)

Biological Agents: The FBI WMD Incident Contingency Plan defines biological agents as microorganisms or toxins from living organisms that have infectious or noninfectious properties that produce lethal or serious effects in plants and animals.

Bioshield (Project): In his State of the Union Address, President Bush announced Project BioShield - a comprehensive effort to develop and make available modern, effective drugs and vaccines to protect against attack by biological and chemical weapons or other dangerous pathogens.

Bioterrorism: The intentional use of microorganisms, or toxins, derived from living organisms, to produce death or disease in humans, animals, or plants.

Bioterrorism Response Advisory Committee (BRAC): Committee consisting of the Department of Health partners and stakeholders that advises the Department of Health on the creation of its plan for bioterrorism preparedness and response.

Block Grant: Federal grant funds that are allocated based on a predetermined statutory formula.

Capability: A capability provides the means to accomplish one or more tasks under specific conditions and to specific performance standards. A capability may be delivered with any combination of properly planned, organized, equipped, trained and exercised personnel that achieves the intended outcome. (Implementing Guidance - National Preparedness Goal)

Catastrophic Incident: Any natural or manmade incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. (NRP Dec 2004)

Category "A" Diseases/Agents: The possible biological terrorism agents having the greatest potential for adverse public health impact with mass casualties. High-priority agents include organisms that pose a risk to national security because they can be easily disseminated or transmitted from person to person; result in high mortality rates and have the potential for major public health impact; might cause public panic and social disruption; and require special action for public health preparedness. The Category "A" agents are: smallpox, anthrax, plague, botulism, tularemia, and viral hemorrhagic fevers (e.g., Ebola and Lassa viruses)

Category "B" Diseases/Agents: Second highest priority agents include those that are moderately easy to disseminate; result in moderate morbidity rates and low mortality rates; and require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance. Category B diseases are: Brucellosis, epsilon toxin of *Clostridium perfringens,* food safety threats (e.g., *Salmonella* species, *Escherichia coli* O157:H7, and *Shingella)*, glanders, melioidosis, psittacosis, Q fever, ricin toxin, staphylococcal enterotoxin B, typhys fever, viral encephalitis (e.g., Venezuelan equine encephalitix, eastern and western encephalitis), and water safety threats (e.g., *Vibrio cholerae, Cryptosporidium parvum).*

Category "C" Diseases/Agents: Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of the availability; ease of production and dissemination; and potential for high morbidity and mortality rates and major health impact. The CDC cites Nipah virus and hantavirus as examples.

C-DAT: Columbia Data Analysis Teams. Pilot project sponsored by the FBI and U.S. Department of Justice. C-DAT will be a complete information sharing and integration initiative, compiling data from all possible law enforcement agencies – local, state, and federal in a tri-state area (Washington, Oregon, and Idaho).

Chain of Command: A series of command, control, executive, or management positions in hierarchical order of authority. (NRP, Dec 2004)

Channel of Communication: The official conduit for information flow and coordination of plans, resources, and activities.

Chemical Agents: The Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Incident Contingency Plan defines chemical agents as solids, liquids, or gases that have chemical properties that produce lethal or serious effects in plants and animals.

Choking Agents: Compounds that injure an unprotected person chiefly in the respiratory tract (the nose, throat and particularly the lungs). In extreme cases, membranes swell, lungs become filled with liquid, and death results from lack of oxygen; thus these agents "choke" an unprotected person. Choking agents include phosgene, diphosgene, and chlorine.

Civil Support: Department of Defense support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called CS. (JCS Pub 1-02)

Command and Control: The exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; command and control functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directly coordinating, and controlling forces and operations in the accomplishment of the mission (JCS Pub 1-02).

Common Operating Picture: A broad view of the overall situation as reflected by situation reports, aerial photography, and other information or intelligence (NIMS, March 1, 2004 and NRP Dec, 2004).

Communications: A method or means of conveying information of any kind from one person or place to another (JCS Pub 1-02).

Communication Recovery: In the context of the NRP and its annexes, the process of assessing the effects of an Incident of National Significance, defining resources and developing and implementing a course of action to restore and revitalize the socioeconomic and physical structure of a community. (NRP, Dec 2004)

Communications Security: The protection resulting from all measures designed to deny unauthorized persons information of value, which might be derived from possession, and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes crypto security, transmission security, emission security, and physical security of communications security materials and information. (JCS Pub 1-02).

Competitive Grant: A grant program where eligible applicants are solicited to submit concept papers. At the conclusion of the solicitation period, all received concept papers are assessed and ranked. The highest ranked applicants are then eligible for an award upon their completion of all necessary administrative requirements. Their award amount may be linked to their ranking.

Comprehensive Emergency Management Network (CEMNET): Dedicated 2-way Very High Frequency (VHF) low-band radio system. Provides direction and control capability for state and local jurisdictions for administrative use, and during an emergency or disaster. This is an

emergency management net belonging to and managed by the Washington State Military Department, Emergency Management Division.

Computer Emergency Response Team: An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems (DoDD 5160.54).

Consequence Management: Predominately an emergency management function and included measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. The requirements of consequence management and crisis management are combined in the *NRP. (See also crisis management.)* (NRP, Dec 2004)

Container Security Initiative (CSI): Designed to help protect the United States and a large portion of the global trading system from terrorists who might use container transport to hide weapons of mass destruction and related materials without disrupting legitimate flow of cargo.

Continuity of Government (COG): Planning to ensure the continuity of essential functions in any state security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records: and establishment of emergency operating capabilities.

Continuity of Operations: Efforts taken within an entity (i.e., agency, company, association, organization, business) to assure continuance of minimum essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological and/or attack-related emergencies.

Cooperating Agency: An agency supplying assistance other than direct operational or support functions or resources to the incident management effort. (NIMS, March 1, 2004)

Coordinate: To advance systematically an analysis and exchange of information among principals who have or may have a need to know certain information to carry out specific incident management responsibilities. (NIMS, March 1, 2004)

Counterintelligence: Those activities, which are concerned with identifying and counteracting the threat to security posed by hostile services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism (JCS Pub 1-02).

Counter-terrorism: Strategic and tactical measures taken, in a collective effort to prevent acts of terrorism as defined by the U.S. Department of Justice.

Credible Threat: A potential terrorist threat that, based on a threat assessment, is credible and likely to involve WMD. (NRP, Dec 2004)

Crisis Management: Predominantly a law enforcement function and included measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. *(See also consequence management)* (NRP, Dec 2004)

Critical Agents: The biological and chemical agents likely to be used in weapons of mass destruction and other bio-terrorist attacks. Current lists may be found on the Centers for Disease Control and Prevention Web site: http://www.bt.cdc.gov/Atent/Agentlist.asp and http://www.bt.cdc.gov/Agent/AgentlistChem.asp.

Critical Information: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (JCS Pub 1-02).

Critical Infrastructure: Systems and resources – whether physical or virtual, so vital to the United States that their incapacity or destruction of such systems and resources would have a

debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (NRP, Dec 2004)

Critical Task: Critical tasks are defined as those prevention, protection, response, and recovery tasks that require coordination among an appropriate combination of Federal, State, local, tribal, private sector, and non-governmental entities during a major event in order to minimize the impact on lives, property, and the economy. (Implementing Guidance - National Preparedness Goal).

Cyber: Pertaining to computers and their support systems, such as servers, routers, and switches that support critical infrastructure. (NRP, Dec 2004).

Cyber Infrastructure: Within our critical infrastructure sectors those cyber related (continuum of computer networks) IT systems and resources; e.g. interconnected computer networks, automated control systems, information systems, servers, routers switches and fiber optic cables that allows our critical infrastructure systems to function (see critical infrastructure definition and the National Strategy to Secure Cyberspace).

Cyberspace: Describes the world of connected computers and the society that surrounds them.

Cyberterrorism: A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Data: Data is unprocessed, unanalyzed raw observations and facts.

Deterrence: The prevention of action by fear of the consequences. Deterrence is a state of mind brought about by the existence of threat of unacceptable counter action. (JCS Pub 1-02). Deterrence in the homeland security threat spectrum means an enemy does not even try faced with the evidence of planning, preparation, public mobilization, and training capable of stopping their objectives.

Disease Condition Database: Washington State's electronic repository for a wide range of health data including notifiable conditions (in development).

Disaster: As used in this plan, this term is broadly defined to include disasters and emergencies that may be caused by any natural or man-made event. A large emergency event is that one beyond a community's ability to address within its own and mutual aid resources.

Disaster or Emergency Declaration: A declaration by the President, which authorizes supplemental Federal assistance under the Stafford Act. The declaration is in response to a Governor's request and may cover a range of response, recovery and mitigation assistance for state and local governments, eligible private non-profit organizations, and individuals.

Disaster Medical Assistance Team (DMAT): A DMAT is a deployable national asset that can provide triage, medical or surgical stabilization, and continued monitoring and care of patients until they can be evacuated to locations where they will receive definitive medical care. Specialty DMATS can also be deployed to address mass burn injuries, pediatric care requirements, chemical injury or contamination, etc. The DMAT program is managed by the Department of Homeland Security in coordination with the Department of Health and Human Services.

Disaster Mortuary Operational Response Team (DMORT): A DMORT is a deployable national asset that can assist local authorities in providing victim identification and mortuary services, including: temporary morgue facilities; victim identification by fingerprint, forensic dental, and/or forensic pathology/anthropology methods; and processing, preparation, and disposition of remains. The DMORT program is managed by the Department of Homeland Security in coordination with the Department of Health and Human Services.

Disaster Recovery Center: A facility established in a centralized location within or near the disaster area at which disaster victims (individuals, families, or businesses) applies for disaster aid. (NRP, Dec 2004)

Discretionary Grant: Federal grant funds that are distributed to states, units of local government or private organizations at the discretion of the agency administering the funds. Most discretionary grants are competitive and usually have limited funds available and a large number of potential recipients.

Domain: A major grouping of activities related to the "life cycle" of a domestic incident. The four domains are prevention, preparedness, response and recovery.

Domestic Terrorism: Domestic terrorism involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction.

Emergency: As defined by the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. (Source—NRP, December 2004)

Emergency Management Assistance Compact (EMAC): A legally binding mutual aid agreement and partnership between the States that allows them to assist one another during emergencies and disasters.

Emergency Management: The process by which the state and nation prepares for emergencies and disasters, mitigates their effects, and responds to and recovers from them.

Emergency Operations Center (EOC): The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g. fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or some combination thereof. (NIMS, March 1, 2004)

Emergency Operations Plan (EOP): A planning document that 1) assigns responsibility to organizations and individuals for implementing specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency; 2) sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated; 3) identifies personnel, equipment, facilities, supplies, and other resources available for use during response and recovery operations; and 4) identifies steps to address mitigation issues during response and recovery activities.

Emergency Public Information: Information that is disseminated primarily in anticipation of an emergency or during an emergency. In addition to providing situation information to the public, it also frequently provides directive actions required to be taken by the general public. (NRP Final Draft, July 27, 2004).

Emergency Response Provider: Includes Federal, State, local and tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities. (See section 2 (6), Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (2002).) Also known as emergency responders. (NRP Dec, 2004).

Emergency Response Coordinator: Person authorized to direct implementation of an agency's emergency response plan.

Emergency Services: A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level. In addition, state and federal response plans define emergency support functions to assist in response and recovery.

Emergency Support Function: A grouping of government and certain private-sector capabilities into an organizational structure to provide the support, resources, program implementation, and services that are most likely to be needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims and communities return to normal, when feasible, following domestic incidents. The ESFs serve as the primary operational-level mechanism to provide assistance to State, local, and tribal governments or to Federal departments and agencies conducting missions of primary Federal responsibility. (NRP, Dec 2004)

Evacuation: Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas. (NIMS, March 1, 2004)

Event: A significant event or designated special event requiring security, such as inaugurals, State of the Union addresses, the Olympics, and international summit conferences. (NRP Final Draft, July 27, 2004)

Event: A planned, non-emergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.

U.S. and Canada Free and Secure Trade (FAST): FAST is a harmonized clearance process for shipments of known compliant importers. FAST is for shipments destined to the United States (from Canada or Mexico) using highway mode of transport. For trucks to use FAST lane processing, the Mexican manufacturer must be C-TPAT approved, the U.S. importer (of record) must be C-certified, and the commercial driver must possess a valid FAST Commercial License. The cargo release methods for FAST shipments are the National Customs Automated Prototype (NCAP) and the Pre-Arrival Processing System (PAPS).

Federal Coordinating Officer (FCO): The Federal officer who is appointed to manage Federal resource support activities related to *Stafford Act* disasters and emergencies. The FCO is responsible for coordinating the timely delivery of Federal disaster assistance resources and programs to the affected State and local governments, individual victims, and the private sector. (NRP Dec, 2004)

Federal Emergency Communications Coordinator (FECC): That person, assigned by the GSA, who functions as the principal Federal manager for emergency telecommunications requirements in major disasters, emergencies, and extraordinary situations, when requested by the FCO or FRC. (NRP Dec, 2004)

Federal On-Scene Coordinator (FOSC or OSC): The Federal official predesignated by the EPA or the USCG to coordinate responses under subpart D of the NCP, or the government official designated to coordinate and direct removal actions under subpart E of the NCP. (NRP Dec, 2004)

Federal Response Coordinator (FRC): The Federal official appointed to manage Federal resource support activities related to non-*Stafford Act* incidents. The FRC is responsible for coordinating support from other Federal departments and agencies using interagency agreements and MOUs. (NRP Dec, 2004)

Federal Radiological Emergency Response Plan: The plan that describes the Federal response to the radiological and on-site technical aspects of an emergency in the United States and identifies the lead federal agency for the event.

Federal Response Plan (FRP): The plan was designed to address the consequences of any disaster or emergency situation in which there is a need for Federal assistance under the

authorities of the Stafford Act. The FRP was super-ceded by the National Response Plan (NRP) in Dec 2004.

FINCEN: Financial Crimes Enforcement Network. A US Department of Treasury program established in 1990 to implement and oversee policies related to money laundering. FINCEN provides information sharing and strategic analysis of domestic and worldwide money laundering developments, trends, and patterns.

Fire Service (FS): Individuals, who on a full-time, volunteer, or part-time basis provide life safety services including fire suppression, rescue, arson investigation, public education, and prevention.

First Responder: Local and nongovernmental police, fire, and emergency personnel who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) as well as emergency management, public health, clinical care, public works and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations. First responders may include personnel from Federal, State, local, tribal, or nongovernmental organizations. (NRP-December 2004).

Force Protection: Force protection is often used by the military to mean a security program designed to protect our own service members, civilian employees, family members, facilities, and equipment in all locations and situations. (Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Pub 3-07.2, 17 March 1998)

Fusion Center: An organized structure to coalesce data and information for the purpose of analyzing, linking and disseminating intelligence. A model process is like to include: extract unstructured data, extract structured data and fuse structured data. Fused data are then analyzed to generate intelligence products and summaries for tactical, operational, and strategic commanders. Types of analysis typically conducted in a fusion center include; association charting, temporal charting, spatial charting, link analysis, financial analysis, content analysis and correlation analysis.

G-Series Nerve Agents: Chemical agents of moderate to high toxicity developed in the 1930s. Examples include tabun (GA), sarin (GB), soman (GD), and GF.

Hazard: Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome. (NIMS and NRP)

Hazardous Material: For the purposes of ESF #1, hazardous material is a substance or material, including a hazardous substance, that has been determined by the Secretary of Transportation to be capable of posing a unreasonable risk to health, safety, and property when transported in commerce, and which has been so designated (see 49 CFR 171.8). For the purposes of EXF #10 and the Oil and Hazardous Materials Incident Annex, the term is intended to mean hazardous substances, pollutant, and contaminants as defined by the NCP (NRP, Dec 2004)

Hazardous Materials Personnel (HZ): Individuals, who on a full-time, volunteer, or part-time basis identify, characterize, provide risk assessment, and mitigate/control the release of a hazardous substance or potentially hazardous substance.

Health Alerts: Urgent messages from the CDC to health officials requiring immediate action or attention. The CDC also issues health advisories containing less urgent information about a specific health incident or response that may or may not require immediate action, and health updates, which do not require action.

Homeland Defense: Homeland defense is the protection of US sovereignty, territory, domestic population and critical defense infrastructure against external threats and aggression. The

Department of Defense is responsible for homeland defense. (Strategy for Homeland Defense and Civil Support, 2005).

Homeland Security: (1) A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security p.2)
(2) The preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggressions directed towards US territory, sovereignty, domestic populations, and infrastructure; as well as crisis management, consequence management, and other domestic civil support. Also called HLS. See also homeland defense and civil support (JCS approved definition).

Homeland Security Operations Center (HSOC): The HSOC serves as the primary national-level multi-agency hub for domestic situational awareness and operational coordination. The HSOC also includes DHS components, such as the National Infrastructure Coordinating Center (NICC), which has primary responsibility for coordinating communications with the Nation's critical infrastructure during an incident.

Hospital Emergency Incident Command System (HEICS): HEICS is the Incident Command System (ICS) framework specific to hospitals. The system was developed by the State of California and is used by many hospitals in Washington State. It specifies the chain of command and functional positions that may be required during a hospital's response to an emergency situation.

Impact: A forceful consequence (physical, economic, psychological).

Incapacitating Agents: An agent that produces temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days and victims usually do not require medical treatment; however, such treatment does speed recovery.

Incident: An occurrence, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies and other occurrences requiring an emergency response. (NIMS and NRP Final Draft, July 27, 2004)

Incident Action Plan (IAP): An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods. (NIMS, March 1, 2004).

Incident Commander (IC): The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site. (NIMS, March 1, 2004)

Incident Command Post (ICP): The field location at which the primary tactical-level, on-scene command functions are performed. The ICP may be co-located with the incident base or other incident facilities and is normally identified by a green rotating or flashing light. (NIMS, March 1, 2004)

Incident Command System: A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. (NIMS, March 1, 2004)

Incident Management Team: The Incident Commander and appropriate Command and General Staff personnel assigned to an incident. (NIMS, March 1, 2004)

Incident Mitigation: Actions taken during an incident designed to minimize impacts or contain the damages to property or the environment. (NRP, December 2004)

Incident Objectives: Statements of guidance and direction necessary for selecting appropriate strategy(s) and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow strategic and tactical alternatives. (NIMS, March 1, 2004)

Incident of National Significance: Based on criteria established in HSPD-5 (paragraph 4), an actual or potential high impact event that requires a coordinated and effective response by an appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private-sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities. (NRP Dec, 2004)

Initial Actions: The actions taken by those responders first to arrive at an incident site (NIMS, March 1, 2004 and NRP Dec 2004).

Initial Response: Resources initially committed to an incident. (NIMS, March 1, 2004 and NRP Dec 2004)

Information: Processed fact: reporting with or without analysis. It is often prepared for publication or dissemination in some form and is intended to inform rather than warn or advise.

Information Security: The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Also called INFOSEC (JCS Pub 1-02).

Information System: The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information (JCS Pub 6-0).

Information Warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks (CJCSI 3210.01).

Infrastructure: The manmade physical systems, resources, projects, and structures, publicly and/or privately owned, that are used by or provide benefit to the public. Examples of infrastructure include utilities, bridges, levees, drinking water systems, electrical systems, communications systems, dams, sewage systems, and roads. (NRP Dec, 2004)

Intelligence: The product of adding value to information and data through analysis. Intelligence is created for a purpose. It is the process by which analysis is applied to information and data to inform policy-making, decision-making, including decisions regarding the allocation of resources, strategic decisions, operations and tactical decisions.

Intelligence Cycle: The process by which information and data is collected, evaluated, stored, analyzed and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, and consumer.

Intelligence Products: The means by which intelligence is communicated to those who will use it. Intelligence products are not limited to written digests or summaries, reports or notes, and can also include oral warnings, alerts, advisories or notices given to the consumer when justified.

Interagency Incident Management Group (IIMG): A tailored group of senior federal interagency experts who provide strategic advice to the Secretary of Homeland Security during an actual or potential Incident of National Significance.

International Terrorism: Involves groups or individuals whose terrorist activities are foreign-based and/or directed by countries or groups outside the United States whose activities transcend national boundaries.

Interoperability: The ability of systems or communications to work together.

Joint Field Office (JFO): A temporary federal facility established locally to provide a central point for Federal, State, local, and Tribal executives with responsibility for incident oversight, direction, and/or assistance to effectively coordinate protection, prevention, preparedness, response, and recovery actions. The JFO will combine the traditional functions of the FBI JOC, the FEMA DFO, and the JIC within a single Federal facility. (NRP Dec, 2004).

Joint Information Center (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media at the scene of the incident (NIMS, March 1, 2004 and NRP Dec 2004).

Joint Information System (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, timely information during crisis or incident operations (NIMS, March 1, 2004)

Joint Operations Center (JOC): The JOC is the focal point for all investigative law enforcement activities during a terrorist or potential terrorist incident or any other significant criminal incident, and is managed by the SFLEO. The JOC integrates into the JFO when the NRP is activated. (NRP Dec, 2004)

Jurisdiction: A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, state or federal boundary lines) or functional (e.g., law enforcement, public health). (NIMS, March 1, 2004 and NRP Dec, 2004).

Key Resources: Key resources represent a broad array of unique facilities, sites, and structures whose disruption or destruction could have significant consequences across multiple dimensions. Examples include: national monuments, symbols or icons, b) representatives of economic power and technology (nuclear power plants, dams, government buildings), and c) prominent commercial centers, sports stadiums. (National Strategy for the Physical Protection of CI//KA, p. 71)

Liaison Officer: An agency official sent to another agency to facilitate interagency communications and coordination. (NRP Final Draft, July 27, 2004)

Law Enforcement (LE): Individuals, full-time, or on a voluntary basis, who work for agencies at the local, municipal and state levels with responsibility as sworn law enforcement officers.

Local Emergency Planning Committee (LEPC): A term used in the Emergency Planning and Community Right-to-Know Act (EPCRA) (42 U.S.C. 11001: 1986). EPCRA also known as Title III of SARA (Superfund Amendments and Reauthorization Act), was enacted by Congress as the national legislation on community safety. It was designed to help local communities, state and tribal governments protect public health, safety, and the environment from chemical hazards.

Local Government: A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional, or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. (See

Section 2 (10), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002) and NRP Dec, 2004.

Logistics: Providing resources and other services to support incident management. (NIMS)

Major Disaster: As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is: any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby. (NRP Dec, 2004)

Major Event: Refers to domestic terrorist attacks, major disasters, and other emergencies. (Source—HSPD-8)

Materiel Management: Requisitioning and sourcing (requirements processing); acquisition, asset visibility (resource tracking), receipt, storage, and handling; security and accountability; inventory, deployment, issue, and distribution; and recovery, reuse, and disposition. (NRP Dec, 2004)

Metropolitan Medical Response System: The MMRS program assists designated localities with funding to write plans, develop training, purchase equipment and pharmaceuticals, and conduct exercises related to catastrophic incidents, whether terrorist or natural disaster. The MMRS program enables jurisdictions to achieve an enhanced local capability to respond to mass casualty events during the first hours of a response until significant external assistance can arrive. MMRS jurisdictions are prepared to respond to the range of mass casualty incidents – from weapons of mass destruction, epidemic outbreaks, natural disasters, and large-scale hazardous materials events.

Mitigation: Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during or after an incident (NIMS, March 1, 2004 and NRP Dec 2004).

Mobilization: The process and procedures used by all organizations federal, State, and local for activating, assembling, and transporting all resources that have been requested to respond to or support an incident. (NIMS, March 1, 2004 and NRP Dec, 2004)

Multi-jurisdictional Incident: An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under Unified Command. (NRP Dec, 2004)

Mutual Aid Agreement: Written agreement between agencies and/or jurisdictions that they agree to assist one another upon request, by furnishing personnel, equipment, and/or expertise in a specified manner. (NRP Dec, 2004)

National Disaster Management Medical System: A coordinated partnership between the DHS, HHS, DOD, and the Department of Veterans Affairs established for the purpose of responding to the needs of victims of a public health emergency. NDMS provides medical response resources and the movement of patients to health care facilities where definitive medical care is received when required. (NRP Dec, 2004))

National Incident Management System (NIMS): A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and tribal governments; the private-sector, and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size or complexity. To provide for interoperability and compatibility among Federal, State, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as

the ICS; multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking and reporting of incident resources. (NIMS, March 1, 2004 and NRP Dec 2004)

National Response Coordination Center: The NRCC, a functional component of the HSOC, is a Multi-agency center that provides overall federal response coordination.

National Response Plan (NRP): A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan. (NIMS, March 1, 2004)

National Response System: Pursuant to the NCP, it is the mechanism for coordinating response actions by all levels of government (40CFR 300.21)

National Response Team (NRT): The NRT, comprised of the 16 Federal agencies with major environmental and public health responsibilities, is the primary vehicle for coordinating Federal agency activities under the NCP. The NRT carries out national planning and response coordination and is the head of a highly organized Federal oil and hazardous substance network. EPA serves as the NRT Chair, and the DHS-USCG serves as the Vice Chair. (NRP Final Draft, July 27, 2004

National Security Emergency: Any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States (Executive Order 12656).

Need-to-Know: The determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (CIA Directive 1/7. (1998). Security Controls on the Dissemination of Intelligence Information.)

Nongovernmental Organization: An entity with an association that is based on interests of its members, individuals, or institutions and that is not created by a government, but may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross. (NIMS, March 1, 2004)

Northwest Warning, Alert & Response Network (NWWARN): A local and regional information sharing and coordination system pilot project by leveraging present functioning information systems or creating a system where none exists. NWWARN is a network of professionals dedicated to protecting the region's population and critical infrastructure. The purpose is to provide credible information regarding alerts, threats, and warnings to public and private infrastructure stakeholders, law enforcement and emergency services. NWWARN disseminates and collects information using a broadcast or targeted methodology to include the use of voice, e-mail, mobile text and website updates based on the priority of the message. NWWARN also includes the ability to provide citizens the ability to pass suspicious information tips to the FBI.

Nuclear Weapons: The Effects of Nuclear Weapons (DOE, 1977) defines nuclear weapons as weapons that release nuclear energy in an explosive manner as the result of nuclear chain reactions involving fission and/or fusion of atomic nuclei.

Pacific Northwest Economic Region: The Pacific Northwest Economic Region (PNWER) is a Public-Private Partnership consisting of the American states and Canadian provinces of Alaska, Alberta, British Columbia, Idaho, Montana, Oregon, Washington, and the Yukon. PNWER's mission is to foster sustainable economic development throughout the entire region.

Physical Infrastructure: Within our critical infrastructure sectors (agriculture and food, water, healthcare and public health, emergency services, government facilities, defense manufacturing capability, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping) those tangible systems and resources;

e.g., basic facilities, installations, equipment and personnel needed for a functioning system (see critical infrastructure definition).

Potential Threat Element (PTE): Any group or individual in which there are allegations or information indicating a possibility of the unlawful use of force or violence, specifically the utilization of a WMD, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of a specific motivation or goal, possibly political or social in nature. This definition provides sufficient predicate for the FBI to initiate an investigation.

Pre-Arrival Processing System (PAPS): A U.S. Customs Automated Commercial System (ACS) border cargo release mechanism that utilizes barcode technology to expedite the release of commercial shipments while processing each shipment through Border Cargo Selectivity (BCS) and the Automated Targeting System (ATS).

Preempt: Acting to eliminate an opponent's ability to take a specific action. We stop them before they try with our efforts in surveillance, detection, intelligence gathering/sharing, cooperation, early warning and effective command and control.

Preparedness: The existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events {which include domestic terrorist attacks, major disasters, and other emergencies}. The term 'readiness' is used interchangeably with preparedness. (HSPD-8)

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents (NIMS, March 1, 2004).

Prevention: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice.(NIMS, March 1, 2004 and NRP Dec, 2004).

Priority Intelligence Requirements: Those intelligence requirements for which a commander has anticipated and stated priority in the task of planning and decision making. Also called PIRs (JCS Pub 1-02).

Principal Federal Official (PFO): The Federal official designated by the Secretary of Homeland Security to act as his/her representative locally to oversee, coordinate, and execute the Secretary's incident management responsibilities under HSPD-5 for Incidents of National Significance. (NRP Dec, 2004)

Private Sector: Organizations and entities that are not part of any governmental structure. It includes for-profit and not-for-profit, and formal and informal structures, commerce and industry, and private voluntary organizations (PVO). (NIMS, March 1, 2004 and NRP Dec, 2004)

Protect: Protection consists of five groups of activities: hardening of positions; protecting personnel; assuming mission oriented protective posture; hardening of positions (infrastructure); protecting people; using physical defense measure; and reacting to an attack. (JCS Pub 1-02) In the event of a strike we successfully defend.

Protection: Involves actions to reduce the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks (HSPD 7)

Public Health: Protection, safety, improvement, and interconnections of health and disease prevention among people, domestic animals and wildlife. (NRP, Dec 2004)

Public Health Regions: Local health jurisdictions are organized into 9 regions. Each region will develop a plan for resource sharing and coordinated emergency response that will align to the state emergency management plan and will include hospitals, emergency medical services, law enforcement and fire protection districts.

Public Information Officer (PIO): A member of the Command Staff responsible for interfacing with the public and media or with other agencies with incident related information requirements. (NRP Dec, 2004)

Public Works: Work, construction, physical facilities, and services provided by governments for the benefit and use of the public. (NRP Dec 2004)

Push Package: A delivery of medical supplies and pharmaceuticals sent from the National Pharmaceutical Stockpile to a state undergoing an emergency within 12 hours of federal approval of a request by the state's Governor

Radiological Dispersal Devices (RDD): A conventional explosive device incorporating radioactive material(s) sometimes referred to as a "dirty bomb."

Radiological Emergency Response Teams (RERTs): Teams provided by EPA's Office of Radiation and Indoor Air to support and respond to incidents or sites containing radiological hazards. These teams provide expertise in radiation monitoring, radionuclide analyses, radiation health physics, and risk assessment. RERTs can provide both mobile and fixed laboratory support during a response. (NRP, Dec 2004)

Rapid Response Information System (RRIS): A system of databases and links to Internet sites providing information to federal, state, and local emergency officials on federal capabilities and assistance available to respond to a consequences of a WMD/terrorism incident.

Reasonable Suspicion: When information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. (28 CRF 23.20 (c).

Recovery: The development, coordination, and execution of service-and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents (NIMS, March 1, 2004 and NRP Dec 2004).

Region: As used in the National Preparedness Goal, "region" generally refers to a geographic area consisting of contiguous State, local, and tribal entities located in whole or in part within a designated planning radius of a core, high threat Urban Area. The precise boundaries of a region are self-defined.

Regional Response Teams (RRTs): Regional counterparts to the National Response Team, the RRTs comprise regional representatives of the Federal agencies on the NRT and representatives of each State within the region. The RRTs serve as planning and preparedness bodies before a response, and provide coordination and advice to the Federal OSC during response actions. (NRP, Dec 2004)

Regional Response Coordination Center (RRCC): At the regional level, the RRCC coordinates regional response efforts and implements local federal program support until a Joint Field Office is established.

Red Team: A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.

Resources: Personal and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC. (NRP, Dec 2004)

Response: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. (NIMS, March 1, 2004 and NRP Dec, 2004).

Risk: Risk is the product of threat, vulnerability, consequence, and likelihood of occurrence. (Implementing Guidance – National Preparedness Goal).

Risk Management Based Intelligence: An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policy making especially regarding vulnerabilities and counter-measures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations. (David Schwendiman, *Risk Management Model).*

State and Local Government: The terms "State," and "local government," when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101). (HSPD 8)

HSA 2002 – **Local** means "(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity."

HSA 2002 - **State** means "any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands and any possession of the United States. See section 2 (14) of the Homeland Security Act of 2002, Pub.L. 107-296, 116 Stat.2135, (2002).

Strategic: Strategic elements of incident management are those characterized by continuous long-term, high-level planning by organizations headed by elected of other senior officials. These elements involve the adoption of long-range goals and objectives, the setting of priorities, the establishment of budgets and other fiscal decisions, policy development, and the application of measures of performance or effectiveness. (NRP Dec, 2004)

Strategic Goal: Broad statement that describes what we must be able to do to successfully accomplish our mission. A high-level, issue-oriented statement of an organizations' desired future direction or desired state. Goals elaborate on the organization's vision statement, articulating an organization's desired future direction or desired state. (OFM Guidelines for Strategic Plans and Performance Measures).

Strategic Mission Statement: The mission statement describes an agency or organization's reason for existence in general terms that capture its unique purpose and functions. It typically

describes the organization, what it does, why it does it, and for whom. (OFM Guidelines for Strategic Plans and Performance Measures)

Strategic Performance Measure/Benchmark: A statement of how attainment of the goal will be measure; the benchmark specifies the criterion for success. What we measure, count and report.

Strategic Planning: The systematic identification of opportunities and threats that lie in the future environment, both external and internal, which, in combination with other relevant data such as threats, vulnerabilities and risks, provides a basis to make better current decisions to pursue opportunities and to avoid threats. It is an orderly process, which, sets for basic objectives and goals to be achieved, and strategies to reach those goals and objectives with supporting action plans to make sure that strategies are properly implemented.

Strategic Target: The level we want to achieve within a performance measure/benchmark.

Strategic Vision: An idealized statement of the best possible future.

Surge Capacity: Ability of institutions such as clinics, hospitals or public health laboratories to sharply increased demand for their services during an emergency.

System: A combination of facilities, equipment, personnel, procedures, and communications integrated into a common organizational structure to achieve a mission or outcome.

Target Capabilities Lists: Identifies capabilities (or resource packages) that provide a means to perform the tasks that are most essential to achieve a reasonable assurance of a successful outcome for a scenario. The Target Capabilities List will be organized by Tier, to account for reasonable differences in expected capability levels among jurisdictions based on assessments of population density, critical infrastructure, and other significant risk factors. (National Preparedness Goal, March 2005)

Terrorism: Any activity that (1) involves an act that (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (b) is a violation of the criminal laws of the United States or of any State or other subdivision of the United State; and (2) appears to be intended (a) to intimidate or coerce a civilian population; (b) to influence the policy of a government by intimidation or coercion; or (c) to affect the conduct of a government by mass destruction, assassination or kidnapping. (NRP, Dec 2004))

Terrorist Incident: The FBI defines a terrorist incident as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population or any segment thereof in furtherance of political or social objectives.

Threat: An indication of possible violence, harm or danger. (NRP Dec, 2004)

Tier: Groupings of jurisdictions that account for reasonable differences in expected capability levels among entities based on assessments of total population, population density, critical infrastructure, and other significant risk factors.

Tribal Government: For the purposes of this document a Tribal Government is a federally recognized Indian Tribe within the State of Washington. Through regulations, federally recognized tribes have the same role as States in the development of chemical emergency preparedness programs under the Emergency Planning and Community Right-to-Know Act (EPCRA). A Tribal Government is the appropriate implementing authority of emergency management in Indian Country. The Centennial Accord of 1989 provides a framework for a Government-to-Government relationship between the State of Washington, through its Governor and the signatory Tribes. Additional information is available from the Governor's Office of Indian Affairs at www.goia.wa.gov.

Unified Command: An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies ad/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP. (NIMS, March 1, 2004)

Unity of Command: The concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. (NIMS, March 1, 2004).

Universal Task List: A menu of tasks from all sources that may be performed in major events such as those illustrated by the National Planning Scenarios. Entities at all levels of government should use the UTL as a reference to help them develop proficiency through training and exercises to perform their assigned missions and tasks in major events. (Implementing Guidance – National Preparedness Goal).

Volunteer: Any individual accepted to perform services by an agency that has authority to accept volunteer services when the individual performs services without promise, expectation, or receipt of compensation for services performed. See 16 U.S.C. 742f(c)) and 29 CFR 553.101. (NIMS, March 1, 2004 and NRP Dec, 2004)

Vulnerability: Susceptible to destruction, incapacitation, injury or attack**.** (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system that cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (3) In information operations, a weakness in information systems security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (JCS Pub 1-02).

Vulnerability Assessment: A vulnerability assessment provides a measure to indicate the relative likelihood that a particular facility or incident within the jurisdiction may become the target of a terrorist attack.

Watchout Situations: In fire management and fire service, watchout situations are indicators or trigger points that remind firefighters to reanalyze or to re-evaluate their suppression strategies and tactics.

Weapons of Mass Destruction: As defined in Title 18, USC 2332a: (1) any explosive, incendiary or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, or a missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or device similar to the above; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;(3) any weapon involving disease organism, or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (NRP, Dec 2004)

APPENDIX H

HOMELAND SECURITY REFERENCES

National Strategies

- National Strategy for Homeland Security – July 2002.
  http://www.whitehouse.gov/homeland/book/
- National Security Strategy of the United States – March 2006
  http://www.whitehouse.gov/nsc/nss.html
- National Strategy for Combating Terrorism – February 2003
  http://www.whitehouse.gov/news/releases/2003/02/20030214-7.html
- National Strategy for Physical Protection of Critical Infrastructures and Key Resources – Feb 2003 http://www.whitehouse.gov/pcipb/physical.html
- National Strategy to Secure Cyberspace – February 2003
  http://www.whitehouse.gov/news/releases/2003/02/20030214-7.html
- National Border Patrol Strategy – February 2003
  http://www.immigration.gov/graphics/shared/lawenfor/bpatrol/strategy.htm
- National Drug Control Strategy – February 2003
  http://www.whitehousedrugpolicy.gov/policy/ndcs.html

Homeland Security Presidential Directives

- HSPD 1 Organization and Operation of the Homeland Security Council – 29 Oct 01
  http://www.whitehouse.gov/news/releases/2001/10/20011030-1.html
- HSPD 2 Combating Terrorism Through Immigration Policies – 29 Oct 01
  http://www.whitehouse.gov/news/releases/2001/10/20011030-2.html
- HSPD 3 Homeland Security Advisory System – 11 March 02
  http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html
- HSPD 4 National Strategy to Combat Weapons of Mass Destruction – 11 Dec 02
  http://www.fas.org/irp/offdocs/nspd/nspd-17.html
- HSPD 5 Management of Domestic Incidents – 28 Feb 03
  http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html
- HSPD 6 Integration and Use of Screening Information – 16 Sep 03
  http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html
- HSPD 7 Critical Infrastructure Identification, Prioritization, and Protection – 17 Dec 03
  http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- HSPD 8 National Preparedness – 17 Dec 03
  http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html
- HSPD 9 Defense of the United States Agriculture and Food – 30 Jan 04
  http://www.whitehouse.gov/news/releases/2004/02/20040203-2.html
- HSPD 10 Biodefense for the 21st Century – 28 April 04

http://www.fas.org/irp/offdocs/nspd/biodef.html

- HSPD 11 Comprehensive Terrorist-Related Screening Products – 27 Aug 04 http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html

- HSPD 12 Policy for a Common Identification Standard for Federal Employees and Contractors http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

- HSPD 13 Maritime Security Policy – 21 December 04 http://64.233.179.104/search?q=cache:i46ofCZYtf4J:www.fas.org/irp/offdocs/nspd/nspd41.pdf+HSPD+13+Maritime+Policy&hl=en

National Preparedness System

- The National Incident Management System (NIMS) March 1, 2004 http://www.fema.gov/nims/

- National Response Plan – December 2004 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml

- National Preparedness Goal – March 2004 https://www.llis.dhs.gov

- National Preparedness Guidance *(HSPD-8 National Preparedness)* https://www.llis.dhs.gov

- National Planning Scenarios – July 2004 https://www.llis.dhs.gov

- Target Capabilities List 2.0 – November 2005 https://www.llis.dhs.gov

- Universal Task List 2.0 – December 17, 2004 https://www.llis.dhs.gov

- National Infrastructure Protection Plan – February 2006 https://www.llis.dhs.gov

Statutes (State and Federal)

Washington State

- Chapter 38.52 Revised Code of Washington (RCW) The Washington State Legislature - Emergency Management http://www.leg.wa.gov/RCW/index.cfm?fuseaction=chapterdigest&chapter=38.52

- Title 118 Washington Administrative Code (WAC) Military Department http://www.leg.wa.gov/wac/index.cfm?fuseaction=title&title=118

Federal

- Homeland Security Act of 2002, Public Law 107-296, 6 U.S.C. 101 *et seq*.,http://www.cio.gov/documents/pl_107_296_nov_25_2003.pdf

- The Maritime Transportation Security Act http://users.mo-net.com/district8wr/public/MTSA_Port_Presskit.pdf

- The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121-5206http://www.ak-prepared.com/serc/acrobat_docs/Stafford_Act_part_1.pdf

- National Mutual Aid and Resource Management Initiative Glossary of Terms and Definitions, Dec 2003, http://www.fema.gov/pdf/preparedness/glossaryterms.pdf

- The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law 107-188, 42 U.S.C. 247d and 300hh, June 12, 2002 http://tis.eh.doe.gov/biosafety/library/PL107-188.pdf

- The Defense Production Act of 1950 (DPA) as amended by P.S. 102-558, 106 Stat. 4201, 50 U.S.C. App. 2062 http://www.access.gpo.gov/uscode/title50a/50a_75_.html

- The Economy Act, 31 U.S.C. 1535 & 1536http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t29t32+1837+0++(The%20Economy%20Act)%20%20AND%20((31)%20ADJ%20USC):CITE%20AND%20(USC%20w/10%20(1535%20&%201536)):CITE

- The Posse Comitatus Act http://www4.law.cornell.edu/uscode/18/1385.html

- National Emergencies Act of 1976 http://www4.law.cornell.edu/uscode/50/1601.html

- The National Communications Act of 1934, 47 U.S.C. 309 *et seq* http://www.dinf.ne.jp/doc/english/Us_Eu/ada_e/telcom_act/47/ch5.htm

- The Defense Against Weapons of Mass Destruction (WMD) Act, 50 U.S.C. 2301 *et seq* http://www.dtra.mil/news/deskbook/Full%20text%20documents/US%20code/50%20USC%202301%20et%20seq.doc

- Emergencies Involving Chemical or Biological Weapons 10 U.S.C. 382http://resource.lawlinks.com/Content/Legal_Research/US_code/Title_18/title_18_10.htm

- Emergencies Involving Nuclear Materials http://www4.law.cornell.edu/uscode/18/831.html

- The Public Health Service Act http://www.fda.gov/opacom/laws/phsvcact/phsvcact.htm

Federal Plans

- National Incident Management System (March 1, 2004) http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf

- The National Response Plan (Dec 2004) http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml

- National Plan for Information Systems Protection http://www.dtra.mil/news/deskbook/Full%20text%20documents/Federal%20Plans/000107national_plan.pdf

- Department of Health and Human Services Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological (C/B) Terrorism http://www.dtra.mil/news/deskbook/Full%20text%20documents/Federal%20Plans/C-BHMPlan.pdf

- Federal Radiological Emergency Response Plan (FRERP)—Operational Plan http://www.dtra.mil/news/deskbook/Full%20text%20documents/Federal%20Plans/FRERP.doc

- Interagency Domestic Terrorism CONPLAN http://www.dtra.mil/news/deskbook/Full%20text%20documents/Federal%20Plans/Interagency%20Domestic%20Terrorism%20CONPLAN.pdf

Washington State Emergency Management Planning

- Washington State Comprehensive Emergency Management Plan – May 2002
  http://emd.wa.gov/3-map/a-p/cemp/01-cemp-idx.htm

- Comprehensive Emergency Management Planning Guide – March 2003 http://emd.wa.gov/3-map/a-p/plan-guide/01-plan-guide-idx.htm

- Washington State Hazard Identification and Vulnerability Assessment – 2001
  http://emd.wa.gov/3-map/a-p/hiva/03-hiva-director.htm

- Washington State Emergency Operations Plan (EOP)
  http://emd.wa.gov/6-rr/rr-forms-pubs/e-ops/eop/eop-idx.htm

- Guidelines for Implementation of the State of Washington Homeland Security Advisory System – March 2003
  http://emd.wa.gov/site-general/wahsas/wa-hsas-idx.htm

- Emergency Management Assistance Compact
  http://emd.wa.gov/1-dir/emac/emac-2001.htm

- Washington State Recovery Plan
  http://emd.wa.gov/3-map/a-p/recoveryplan/recoveryplantoc.htm