

# DRAFT 3

## GUIDELINES FOR IMPLEMENTATION OF THE STATE OF WASHINGTON HOMELAND SECURITY ADVISORY SYSTEM

FOR  
CITIZENS, NEIGHBORHOODS AND FAMILIES



*Developed By The  
Washington Military Department*



# DRAFT 3

For questions or recommendations on improvement of this guide, contact Mr. Joe Huden at (253) 512-8108 or e-mail [joe.huden@mil.wa.gov](mailto:joe.huden@mil.wa.gov). PLEASE NOTE: Additional guides have been prepared for state agencies and offices of elected officials; tribal, county and local government; and, business, critical infrastructure and key assets. You may access these guides on-line at: <http://www.washingtonguard.com>.

# DRAFT 3



## A Message from the Governor

HOLD

# DRAFT 3

This page intentionally left blank

# DRAFT 3

## TABLE OF CONTENTS

<b>Letter of Introduction</b>	<b>Page 3</b>
<b>Instructions to Users</b>	<b>Page 7</b>
<b>Assignment of Threat Conditions</b>	<b>Page 9</b>
<b>Dissemination of Threat Condition Advisories</b>	<b>Page 15</b>
<b>Threat Condition Green –Low Risk</b>	<b>Page 17</b>
<b>Threat Condition Blue –General Risk</b>	<b>Page 17</b>
<b>Threat Condition Yellow –Significant Risk</b>	<b>Page 18</b>
<b>Threat Condition Orange - High Risk</b>	<b>Page 18</b>
<b>Threat Condition Red –Severe Risk</b>	<b>Page 18</b>
<b>Appendix A: Terms and Acronyms</b>	<b>Page 20</b>
<b>Appendix B: Internet Address Links to Referenced Information</b>	<b>Page 22</b>

# DRAFT 3

This page intentionally left blank

# DRAFT 3

## INSTRUCTION TO USERS

This guidebook is designed to assist citizens in initiating standardized actions as the result of increased terrorist Threat Condition levels within the United States and the State of Washington. This guide provides a framework for developing your response plans as well as act as a checklist when changes in the advisory are issued.

These recommendations have been developed in a generic format to allow you to develop specific implementation procedures appropriate for you, your neighborhood or your family. You should review each recommendation and determine if it is applicable and appropriate to you, your neighborhood or your family. Identify only those actions that make sense to your circumstances. You are encouraged to develop additional action steps as appropriate.

Throughout this document various acronyms and terms are used. Throughout this document various terms and acronyms are used. For definitions of these terms and acronyms see Appendix A.


# DRAFT 3

This page intentionally left blank

# DRAFT 3

## ASSIGNMENT OF HOMELAND SECURITY THREAT CONDITIONS

### *The Homeland Security Advisory System*

	Color Code	Description
	<b>RED (SEVERE)</b>	SEVERE RISK of a terrorist attack (a terrorism attack has occurred or intelligence information indicates an imminent attack is probable)
	<b>ORANGE (HIGH)</b>	HIGH RISK of a terrorist attack (potential for an attack is high or intelligence indicates terrorists are actively seeking targets)
	<b>YELLOW (ELEVATED)</b>	SIGNIFICANT RISK of a terrorist attack (possibility of an attack or intelligence indicates terrorist activity)
	<b>BLUE (GUARDED)</b>	GENERAL RISK of a terrorist attack (threats may not be credible or corroborated but warrant a heightened alert)
	<b>GREEN (LOW)</b>	LOW RISK of a terrorist attack (no threats)

### ***Threat Condition Considerations***

Homeland Security Presidential Directive (HSPD)-3 (<http://www.fas.org/irp/offdocs/nspd/hspd-3.htm>) establishing the Homeland Security Advisory System ("HSAS") and the FBI's National Threat Warning System ("NTWS") provide factors for the assignment of threat conditions. The NTWS provides vital information regarding terrorism reaches the U.S. counterterrorism and law enforcement communities. The guidelines governing the NTWS also provide specific policy regarding public notification procedures.

HSPD-3 and NTWS guidelines contain certain criteria that should be considered when assessing threat risks. A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, more than quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. However, despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. Nonetheless, one important factor in determining a threat risk is the quality of the threat

# DRAFT 3

information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

- The credibility of the threat.
- The level of corroboration regarding the threat.
- The degree to which the threat is imminent.
- Threat specificity, to include a specific target.
- The gravity of the consequences if threat is delivered.
- The assessed vulnerability of the target.

## ***Target Vulnerabilities and Consequences***

Terrorist threats range from disruptive vandalism to catastrophic attacks affecting large centers of population and vital infrastructure. With a specific threat of a terrorist attack it is necessary to determine what consequences would be realized if an attack were to occur. Some of the questions to be considered are as follows:

- Is the target strategically significant as to pose a major disruption to vital services and/or a loss of life?
- How would Federal, State and local governments, along with private industry and the American public, react to the loss and/or disruption of a particular target?
- If the threat is imminent, how much time exists for countermeasures to be implemented?
- Can a target be made less attractive through enhanced security measures?
- Can the threat be intercepted and neutralized by law enforcement or other state or federal government resources?
- Can the effected parties be warned and countermeasures implemented prior to the attack, hopefully, averting a loss of life?

At every Threat Condition level, the same critical attention to threat assessment methodology will be applied. It is recommended that all HSAS education and awareness programs emphasize that despite the best decision to assign an appropriate threat condition; there can be no guarantee that a terrorist attack will be prevented.

## ***Federal and State Actions to Changes in Alert***

NOTE: Actions are cumulative starting at GREEN level.

<b>ALERT LEVEL</b>	<b>FEDERAL ACTIONS</b>	<b>STATE ACTIONS</b>
<b>RED (SEVERE)</b>	Response is primarily directed toward public safety and welfare and the preservation of human life, including:	<ul style="list-style-type: none"><li>• If the threat is not specific to Washington State, activate the state Emergency Operations</li></ul>

# DRAFT 3

	<ul style="list-style-type: none"> <li>• Assigning emergency response personnel and pre-positioning of specially trained teams</li> <li>• Monitoring, redirecting or constraining transportation systems</li> <li>• Closing public and governmental facilities</li> <li>• Increasing or redirecting personnel to address critical emergency needs</li> </ul>	<p>Center (EOC) to Phase III operations. If the threat is specific to Washington State, activate the state EOC to Phase IV operations, staffed with applicable state/federal agency representatives.</p> <ul style="list-style-type: none"> <li>• Following assessment of the situation, if the event threatens or actually impacts the State of Washington, the Governor issues a declaration of "State of Disaster."</li> <li>• Activation of a Joint Information Center (JIC) to include representatives from affected areas and agencies.</li> </ul>
<p><b>ORANGE (HIGH)</b></p>	<ul style="list-style-type: none"> <li>• Crisis management response will focus on law enforcement actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat.</li> <li>• Consequence management response will focus on contingency planning and pre-positioning of tailored resources, as required.</li> </ul>	<ul style="list-style-type: none"> <li>• If the threat is not specific to Washington State, provide double State Emergency Operations Officer (SEOO) staffing of the Alert and Warning Center. If the threat is specific to Washington State, activate the state EOC to Phase III operations, staffed with applicable state/federal agency representatives.</li> <li>• Prepare to, and if necessary, activate a JIC near the threatened area. Coordinate the release of information with appropriate local, county, state, tribal and federal agencies.</li> </ul>
<p><b>YELLOW (ELEVATED)</b></p>	<ul style="list-style-type: none"> <li>• Increasing surveillance of critical areas.</li> <li>• Coordinating emergency plans with related agencies.</li> <li>• Assessing further refinement of protective measures within the context of the current threat information.</li> <li>• Implementing, as appropriate, contingency plans and emergency response plans.</li> </ul>	<ul style="list-style-type: none"> <li>• If the threat is not specific to Washington State, activate state EOC to Phase I. If the threat is specific to Washington State, activate the state EOC to Phase II or Phase II enhanced operations and staff with additional SEOO.</li> <li>• Update staff and agency liaison contacts list.</li> <li>• Provide Public Information Officer (PIO) coverage.</li> </ul>
<p><b>BLUE (GUARDED)</b></p>	<ul style="list-style-type: none"> <li>• Checking communications with designated emergency response or command locations.</li> <li>• Reviewing and updating emergency response procedures.</li> <li>• Providing the public with necessary information.</li> </ul>	<ul style="list-style-type: none"> <li>• All state agencies prepared to staff the EOC as required.</li> <li>• Normal operations with 24-hour EOC and SEOO.</li> <li>• Additional staff alerted to the increased threat level.</li> </ul>

# DRAFT 3

<b>GREEN (LOW)</b>	<ul style="list-style-type: none"><li>• Refining and exercising preplanned protective measures.</li><li>• Ensuring personnel receive training on the Homeland Security Advisory System, departmental, or agency-specific protective measures.</li><li>• Regularly assessing facilities with vulnerabilities and taking measures to reduce them.</li></ul>	<ul style="list-style-type: none"><li>• Normal operations with 24-hour EOC and SEOO.</li></ul>
------------------------	---	--

## ***State Emergency Operations Center Phases***

### **Phase I - Routine Operations**

Incidents are handled only by the SEOOSEOO in the Alert & Warning Center in cooperation with other local, state and federal agencies. Other staff may be involved as advisors if needed for specific expertise. The SEOOSEOO responds to incidents following established Standard Operating Procedures (SOPs) as outlined in the Washington Military Department Emergency Management Division SEOOSEOO Standard Operating Procedures

### **Phase II - Enhanced Operations (Alert Stage)**

An incident is or could potentially grow beyond the capability of the SEOO to handle. In this instance the SEOO, along with select staff, are tasked to support the incident from the state EOC.

During this phase, the SEOO will continue to monitor and process other requests for assistance, separate from the incident that has caused activation of the EOC.

As a general rule, transition from Phase I to Phase II will automatically occur when:

- A local jurisdiction has activated its EOC
- The Division has deployed staff to the field
- Intelligence data indicates the potential for an emergency that is or may grow beyond the capability of affected local jurisdictions

At this phase, one or more persons may be initially tasked to provide specific emergency functions.

If additional staff support is required, the EOC Supervisor will have the authority to escalate to Phase III EOC activation or any intermediate level of staffing that the situation may dictate.

# DRAFT 3

## **Phase III - Full Operation**

An incident's size and complexity requires representation in the EOC by all appropriate state and outside agencies and organizations to support expanded operations. The number of staff and the agencies represented will vary by incident. In this phase, the level of activity dictates that normal Emergency Management Division staff functions cease and all personnel respond in support of the incident.

## **Phase IV –Catastrophic Operations**

A major catastrophic event has occurred that exceeds the capability of state and local government to provide timely and effective response to meet the needs of the situation. An event of this magnitude would cause numerous casualties, property loss, and disruption of normal life support systems and significantly impact the regional economic, physical, and social infrastructures. As a general rule, transition to this phase occurs when the EOC is conducting response operations.

# DRAFT 3

This page intentionally left blank

# DRAFT 3

## DISSEMINATION OF THREAT CONDITION ADVISORIES WITHIN THE STATE OF WASHINGTON

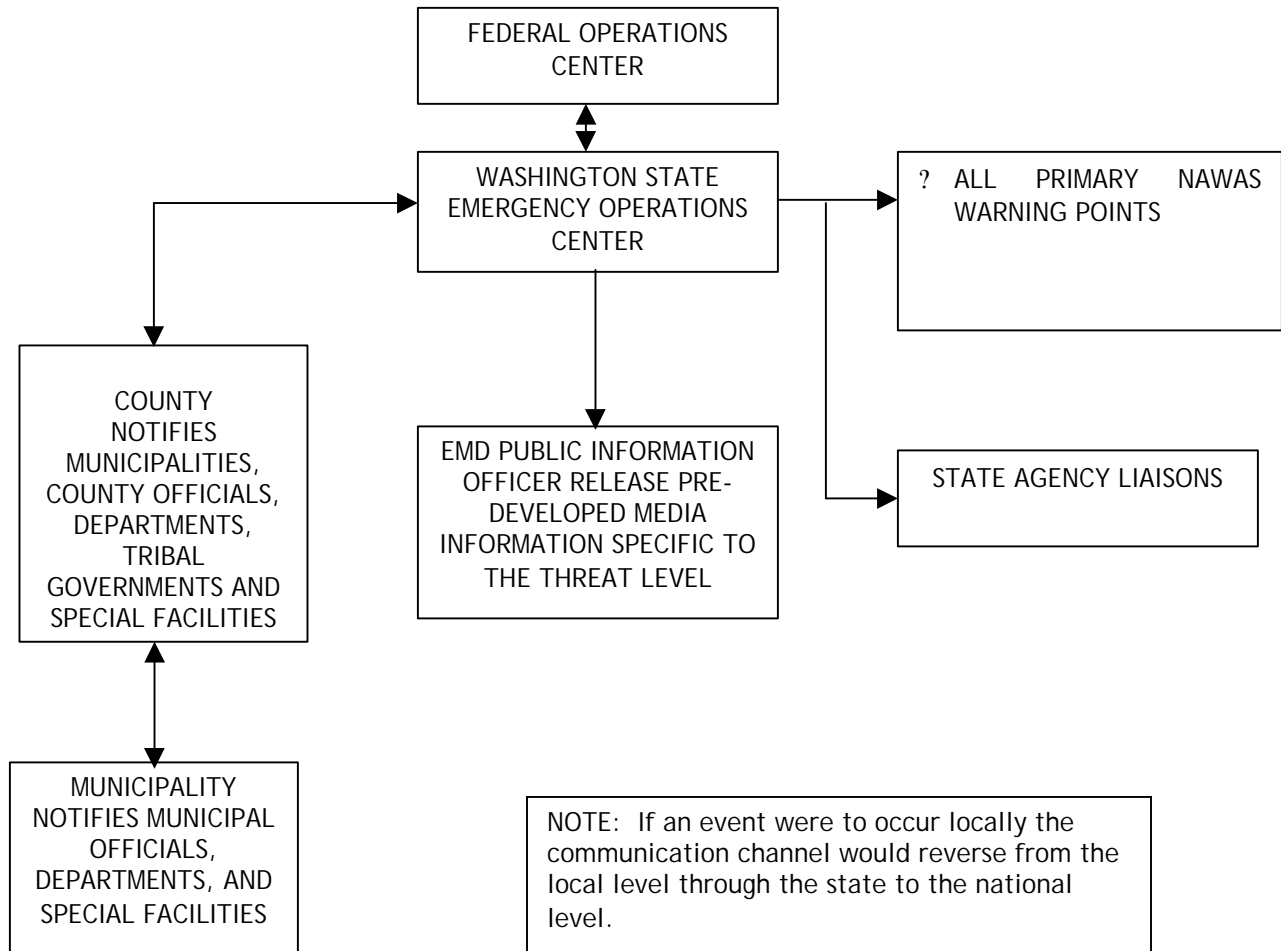
Following notification of a change in the Threat Condition from the federal government, the Federal Operations Center will broadcast threat condition notifications over the National Warning System ("NAWAS") to all fifty states, including local warning points.

The State of Washington will disseminate threat condition advisory messages and other related strategic information within the state in the following manner:

1. The Washington Military Department, Emergency Management Division (EMD) will alert the following:
  - a. Notify all Primary Warning Points using the National Warning System ("NAWAS").
  - b. Disseminate the threat advisory via the statewide A Central Computerized Enforcement Service System ("ACCESS") message to all ACCESS terminals.
  - c. Notify state government agency liaison's who will in turn be responsible for notifying their district and/or satellite offices.
2. Each county will be responsible for disseminating the Threat Condition advisory to appropriate county officials, departments and agencies, special facilities, tribal governments and designated municipal warning entry points (one per municipality).
3. Each municipality will be responsible for disseminating the Threat Condition advisory to its municipal officials, departments and to identified special facilities (schools, hospitals, industries, etc.)
4. Within thirty minutes after initial dissemination by EMD, the EMD Public Information Officer will authorize the release of pre-developed media information appropriate for the identified Threat Condition.

# DRAFT 3

FIGURE 1 – THREAT CONDITION DISTRIBUTION SYSTEM



# DRAFT 3

## RECOMMENDED CITIZEN, NEIGHBORHOOD AND FAMILY PROTECTIVE MEASURES

NOTE: Protective measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a higher alert level.

Action Number	Checklist		GREEN-LOW (LOW RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
G-1			Inform family and neighbors about the Threat Condition GREEN advisory.
G-2			Be alert to suspicious activities and / or individuals and report it to proper authorities or law enforcement agencies. Be suspicious of person(s) taking photographs of critical facilities, asking detailed questions about physical security or are dressed inappropriately for weather conditions.
G-3			Continue to enjoy individual freedom. Participate freely in travel, work and recreational activities.
G-4			Continue to include safety and common sense practices in daily routines.
G-5			Obtain copy of <a href="#">Terrorism: Preparing for the Unexpected</a> brochure from your local Red Cross chapter. Obtain a copy of the <a href="#">United for a Stronger America: Citizens' Preparedness Guide</a> from the National Crime Prevention Council ( <a href="http://www.weprevent.org">http://www.weprevent.org</a> ).
G-6			Develop a personal disaster plan and disaster supplies kit using Red Cross brochures <a href="#">Your Family Disaster Plan</a> and <a href="#">Your Family Disaster Supplies Kit</a> . Know how to turn off your power, gas and water service to your house.
G-7			Examine volunteer opportunities to assist and support the community emergency response agencies (e.g. Red Cross, social services, Neighborhood Crime Watch, Community Emergency Response Team ("CERT"), Community Policing ("COP") or Amateur Radio Emergency Service ("ARES") programs. Contact your local emergency management office or visit these web sites: <a href="http://www.redcross.org">http://www.redcross.org</a> , <a href="http://www.citizencorps.gov">http://www.citizencorps.gov</a> , <a href="http://www.ares.org">http://www.ares.org</a> .
G-8			Take a Red Cross Cardio-Pulmonary Resuscitation (CPR)/Automated External Defibrillator (AED) and first aid courses.
G-9			Family members should have appropriate immunizations and preventative health care updated.

Action Number	Checklist		BLUE – GUARDED (GENERAL RISK of a terrorist attack) Recommended Protective Measures:
	Yes	No	
B-1			Inform family and neighbors about the Threat Condition BLUE advisory. Monitor local and national news for terrorist alerts.
B-2			Continue all measures listed in Threat Condition GREEN Advisory.
B-3			Develop emergency communication plan with family, neighbors and friends that everyone can understand.
B-4			Establish an alternate meeting place away from home with family or friends.
B-5			Review stored disaster supplies and replace items that are outdated.
B-6			Ensure that all private vehicles are secured.
B-7			When handling mail, courier, and package deliveries, remain vigilant and report any concerns or suspect items.
B-8			Ask the local Red Cross chapter to provide a " <a href="#">Terrorism: Preparing</a>

# DRAFT 3

for the Unexpected" presentation at your workplace or neighborhood.

Action Number	Checklist		YELLOW –ELEVATED (SIGNIFICANT RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
Y-1B			Inform family and neighbors about the Threat Condition YELLOW advisory. Resume normal activities but expect some delays, baggage searches and restrictions to some facilities.
Y-2B			Continue all measures listed in the Threat Condition GREEN and BLUE Advisories.
Y-4B			Check telephone numbers and e-mail addresses in your personal communication plan and update as necessary. If not known to you, contact schools to determine their emergency notification and evacuation plans for your children, if appropriate.
Y-5B			Develop alternate routes to / from work / school and practice them.
Y-6B			Have a neighborhood meeting to identify neighbors who are elderly or have special needs. Assist them in development of a personal disaster plan and disaster supplies kit if necessary.

Action Number	Checklist		ORANGE –HIGH (HIGH RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
O-1			Inform family and neighbors about the Threat Condition ORANGE advisory. Resume normal activities but expect some delays, baggage searches and restrictions to some facilities.
O-2			Continue all measures listed in the Threat Condition GREEN, BLUE and YELLOW Advisories.
O-3			Review disaster plan with all family members.
O-4			Exercise caution when traveling. Be alert to your surroundings, avoid placing yourself in a vulnerable situation and monitor the activities of your children. Avoid leaving unattended packages, back packs, brief cases or bags in public areas.
O-5			Have shelter in place, materials on hand, and review procedures in the Red Cross <a href="#">Terrorism: Preparing for the Unexpected</a> brochure.
O-6			Check on neighbors who are elderly or have special needs to ensure they are okay. Review disaster plan with them.
O-7			Listen to news regarding the heightened threat and security procedures, local contingency operations / plans / evacuations and personal safety messages.

Action Number	Checklist		RED –SEVERE (SEVERE RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
R-1			Inform family and neighbors about the Threat Condition RED advisory. Expect delays, searches and restricted access to buildings. Expect traffic delays and restrictions. Avoid crowded public areas and gatherings.
R-2			Continue all measures listed in the Threat Condition GREEN, BLUE, YELLOW and ORANGE Advisories.
R-3			Maintain and monitor communications and warning systems. Listen to radio / TV for current information / instructions.
R-4			Contact business / school to determine status of work / school day.
R-5			Adhere to any travel restrictions announced by local governmental authorities.
R-6			Be prepared to shelter in place or evacuate and assist neighbors who are elderly or have special needs if instructed to do so by local

# DRAFT 3

			governmental authorities.
--	--	--	---------------------------

# DRAFT 3

## APPENDIX A

### TERMS AND ACRONYMS USED IN THIS DOCUMENT

The following terms and acronyms are used within this document. For further clarification you may contact the Washington Military Department at (253) 512-8108 or by e-mail at [joe.huden@mil.wa.gov](mailto:joe.huden@mil.wa.gov).

**ACCESS** refers to A Central Computerized Enforcement Service System which is the primary means of notifying emergency management functions and personnel throughout the state.

**AED** refers to Automated External Defibrillator and the training provided by the Red Cross.

**ARES** refers to the Amateur Radio Emergency Service program, contact your local Amateur Radio Club or visit the web site at: <http://www.ares.org/>

AWC Alert & Warning Center

**CERT** refers to Community Emergency Response Teams, contact the local emergency management agency for details.

**COP** refers to Community Policing programs, contact your local law enforcement office for programs in your area.

**CPR** refers to Cardio-Pulmonary Resuscitation and the training provided by the Red Cross.

**Critical Infrastructure** means systems and assets within the state's jurisdiction, whether physical or virtual, so vital to the United States or the State of Washington that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national or state economic security, national or state public health or safety, or any combination of those matters, including:

**Energy** - (electrical generation / switching / load dispatch, gas and oil production, nuclear power plants, etc)

**Emergency Services** - (emergency operations centers, fire, law enforcement, emergency medical services, etc)

**Information and Telecommunications** - (9-1-1 centers, critical tower sites, telephone and communications infrastructure, IT systems, radio and television transmission sites, EAS activation points, etc)

**Transportation** - (terminals, bridges, ferries, etc)

**Water** - (distribution systems and treatment plants, etc)

# DRAFT 3

**Banking and Finance** - (including processing facilities, etc)

**Government** - (facilities, elected officials, etc)

**Agriculture** - (grain storage, animal feed lots, fertilizer storage, etc)

**Food** - (food processors, food shippers, etc)

**Public Health** - (hospitals, labs, public health districts, etc)

**Defense Industry** - (manufacturing, military facilities, etc)

**Chemical Industry** - (production, storage, movement, etc)

**Postal and Shipping** - (post offices, parcel delivery services, trucking, etc)

**EAS** refers to the Emergency Alert System used in coordination with the broadcast industry to provide alert type information essential to the public concerning an emergency.

**EMD** refers to the Emergency Management Division of the State Military Department.

**EOC** refers to the state or local Emergency Operations Center for directing activities based on the threat advisory.

**EOP** refers to Emergency Operations Plan.

**HSAS** refers to the Homeland Security Advisory System.

**HSPD** refers to Homeland Security Presidential Directives followed by a dash and number (e.g. HSPD-3).

**JIC** refers to a Joint Information Center of government public information officials.

**Key Assets** refer to (office buildings (especially multi-national corporations), religious institutions, public areas, schools, national and local symbols, historical attractions, monuments and icons).

**NTWS** refers to the Federal Bureau of Investigation National Terrorism Warning System.

**PIO** refers to a government Public Information Officer.

**SEOO** refers to the State Emergency Operations Officer who directs emergency operations at the State Emergency Operations Center (EOC).

**SOG** refers to Standard Operating Guides.

**SOP** refers to Standard Operating Procedures.

# DRAFT 3

## APPENDIX B

### INTERNET ADDRESS LINKS TO REFERENCED INFORMATION

On-line version of this guide

<http://www.washingtonguard.com/guide.pdf>

Homeland Security Presidential Decision (HSPD)-3

<http://www.fas.org/irp/offdocs/nspd/hspd-3.htm>

National Office of Homeland Security Web Site

<http://www.whitehouse.gov/homeland/>

National Department of Homeland Security

<http://www.dhs.gov/dhspublic/>

Terrorism: Preparing for the Unexpected

<http://www.redcross.org/services/disaster/keepsafe/terrorism.pdf>

Preparing Your Business for the Unthinkable

<http://www.redcross.org/services/disaster/beprepared/unthinkable2.pdf>

Emergency Management Guide for Business and Industry

[http://www.redcross.org/services/disaster/beprepared/busi\\_industry.html#fema](http://www.redcross.org/services/disaster/beprepared/busi_industry.html#fema)

"Masters of Disaster" K-12 Education Curriculum

<http://www.redcross.org/disaster/masters/>

"Masters of Disaster" K-12 Education Curriculum- "Facing Fear: Helping Young People Deal with Terrorism and Tragic Events"

<http://www.redcross.org/disaster/masters/facingfear/>

Your Family Disaster Plan

<http://www.redcross.org/services/disaster/beprepared/fdpall.pdf>

Your Family Disaster Supplies Kit

<http://www.redcross.org/disaster/safety/fdsk.pdf>

Citizen Corps

<http://www.citizencorps.gov/>

Citizen Preparedness Guide

<http://www.weprevent.org/usa/cover.pdf>

Amateur Radio Emergency Services System

<http://www.ares.org/>

Community Emergency Response Team ("CERT") Materials

<http://training.fema.gov/EMIWeb/CERT/mtrls.asp>

Are You Ready? A Guide to Citizen Preparedness

<http://www.fema.gov/areyouready/>