



WASHINGTON  
COURTS

---

**WASHINGTON STATE  
COURTHOUSE  
PUBLIC SAFETY  
STANDARDS  
2009**

---

By the

**BOARD FOR JUDICIAL ADMINISTRATION**

**Court Security Committee**

# WA State Courthouse Public Safety Standards Table of Contents

## INTRODUCTION

<b>SECTION 1</b> .....	<b>1</b>
ADMINISTRATIVE STANDARDS.....	1
1.1 <i>Standing Court Security Committee</i> .....	1
1.2 <i>Court Security Plan</i> .....	1
1.3 <i>Court Security Coordinator</i> .....	2
1.4 <i>Security Training for All Court Employees</i> .....	2
1.5 <i>Incident Reporting</i> .....	2
<b>SECTION 2</b> .....	<b>4</b>
SECURITY POLICIES.....	4
2.1 <i>Security Policy Restricting Weapons</i> .....	4
2.2 <i>Screening for Weapons</i> .....	4
2.3 <i>Duress and Intrusion Alarms</i> .....	4
2.4 <i>Testing of Security Equipment</i> .....	5
2.5 <i>Access to Caller ID or Call Trace on Phones</i> .....	5
2.6 <i>Use of Force Policy</i> .....	5
2.7 <i>Threat Assessment/Response</i> .....	6
<b>SECTION 3</b> .....	<b>7</b>
ACCESS CONTROL STANDARDS.....	7
3.1 <i>Limited Access - Maint Entrance and Exit</i> .....	7
3.2 <i>Employee Identification Cards</i> .....	7
3.3 <i>Locking Mechanisms</i> .....	8
<b>SECTION 4</b> .....	<b>9</b>
PHYSICAL STANDARDS .....	9
4.1 <i>Facility and Office Design</i> .....	9
4.2 <i>Installation of Physical Barriers</i> .....	9
4.3 <i>Secure Parking</i> .....	9
4.4 <i>Holding Areas</i> .....	10
4.5 <i>Building Controls</i> .....	10

## APPENDICES

<b>APPENDIX A</b> .....	<b>A-1</b>
SECURITY OF THE MAIL.....	A-1
<b>APPENDIX B</b> .....	<b>A-6</b>
RCW 9.41.300.....	A-6
<b>APPENDIX C</b> .....	<b>A-9</b>
CALL TRACE PROCEDURES.....	A-9
<b>APPENDIX D</b> .....	<b>A-10</b>
THREAT ASSESSMENT/RESPONSE.....	A-10
<b>APPENDIX E</b> .....	<b>A-11</b>
SECURITY & SAFETY MODEL CHECKLIST.....	A-11

## **INTRODUCTION**

Courts are intended to be peaceful, safe places to resolve disputes. Washington's court facilities typically are. But unfortunately, both locally and nationally, security breaches are occurring more and more regularly. Violence in our courthouses has resulted in lives being lost and injuries suffered by those targeted, as well as others who have just been in the wrong place at the wrong time. People who come to the courts as litigants, jurors, witnesses, attorneys, and staff must feel safe and be safe, if courts are to remain the forum for resolving disputes peacefully. If our courthouses are not safe and secure, access to justice is jeopardized. Because of this reality, the Board for Judicial Administration created a Court Security Committee that first convened in March 2006.

The Board for Judicial Administration (BJA) Court Security Committee prepared the Courthouse Public Safety Standards embodied in this document. The standards update, expand, and replace the Courthouse Public Safety Standards created by the Washington Supreme Court's 1995 Courthouse Security Task Force.

In preparing the Standards, the Committee reviewed standards of other states. The Standards identify basic fundamentals for safe and secure courthouses, beginning with the creation of local court security committees. These Standards require time and commitment from courts and their stakeholders, but are not necessarily dependent on budget expenditures. The Standards also identify best practices, some of which will not be feasible for all courts due to cost and facility configurations. While acknowledging this reality, the Standards are intended to be aspirational for all sizes of courts and for all jurisdictions.

## **SECTION 1** **ADMINISTRATIVE STANDARDS**

### **1.1 Standing Court Security Committee**

Each court should have a Security Committee with a membership and charges substantially as outlined. The Security Committee may be jointly operated by the courts within a judicial district pursuant to the provisions of GR 29 (j).

The Security Committee should be responsible for implementing the Washington State Courthouse Public Safety Standards. The Security Committee should prepare and maintain a security manual as well as local court security policies and procedures. The Security Committee should meet regularly and not less than every four months. The Security Committee should be charged with conducting an annual security audit of the court security plans, and the security needs of the facilities and the surrounding areas. Whenever possible, but not less than once every three years, this audit should be conducted by an entity independent of the court and the county or city government with which the court(s) is associated. The results of the security audit should be made available to the county or city executive and legislative authority. Those aspects of the audit that would compromise the safety of persons or court operations should be confidential.

The Security Committee should be chaired by a Presiding Judge or a judge appointed by the Presiding Judge. Other members of the Security Committee should represent or be comprised of, but not limited to, the following:

- At least one additional judge so that the superior and courts of limited jurisdiction are represented.
- Superior Court Clerk.
- Court Security Coordinators (see Standard 1.3) from the superior and courts of limited jurisdiction.
- Juvenile Court Administrator.
- Sheriff's department or any other law enforcement agency that provides security for the courts.
- County executive and/or legislative authority.
- Lead staff for any court security unit.
- Corrections or other department responsible for the transporting of in-custody defendants for court hearings.
- Representatives of each agency housed in the court building and/or those who use the courthouse.
- Members of the Washington State Bar Association.

### **1.2 Court Security Plan**

A written court security plan that addresses the elements listed below should be prepared for each court building and distributed to all court personnel and selected staff of other cooperating entities. A court security plan should contain, at a minimum:

- Policies and procedures that implement the Washington State Courthouse Public Safety Standards.
- Routine security operations, including a physical security plan that addresses features such as security screening for persons entering the court, secure storage of weapons not permitted in the courthouse, parking, landscaping, interior and exterior lighting, interior and exterior doors, intrusion and detection alarms, window security, protocol for building access for first responders, and provision of building floor plans for first responders.
- Security & Safety Quick Reference Checklist tailored for local courts (See Appendix E-Model Checklist.)
- Procedures that address the needs for high risk trials that emphasize security and emergency responses.
- Emergency procedures that address assaults; escapes; bomb threats; hostage situations; civil disturbances; and other situations. Procedures should address situations where facility lock downs or evacuations are necessary.
- Court security officer duties.
- Movement and courtroom security of in-custody defendants.
- Mail handling procedures including threatening or inappropriate correspondence. (see Appendix A)
- Incident reporting procedures.

### **1.3 Court Security Coordinator**

Each court should appoint a Court Security Coordinator.

The Court Security Coordinator should be responsible for recommending ongoing updates to the Court Security Plan, monitoring the implementation of the Plan, training court staff on the Plan, and being a liaison to other organizations to implement and change the Plan.

### **1.4 Security Training for All Court Employees**

All court staff should receive training on the Court Security Plan promptly after becoming a court employee. All court staff should receive annual supplemental training.

### **1.5 Incident Reporting**

Courts should immediately report all security incidents to the local law enforcement agency. Courts should also report all security incidents to the local Court Security Committee and the AOC Security Coordinator using the AOC website: <http://inside.courts.wa.gov/index.cfm?fa=cntlCourtResources.showIncidentReportForm> (This website requires court employee login.)

- Local policy may also require that incident information be provided to the county or city risk manager.
- “Incident” is defined as a threat to or assault against the court or court community, including court personnel, litigants, attorneys, witnesses, jurors or others using the

courthouse. It also includes any event or threatening situation that disrupts the court or compromises the safety of the court or the court community.

A security incident is not limited to a violation of law, but may include any act or circumstance that may interfere with the administration of justice. Examples include but are not limited to:

- Threats from the public
- Threats from an employee
- Disruptive behavior on court property
- Assaults, robberies, intimidation or threats to the court community either on or away from court property
- Assaults, robberies, intimidation or threats adjacent to the courthouse that affect access to the courthouse
- Work space quarrels between employees leading to acts of violence

## **SECTION 2**

### **SECURITY POLICIES**

#### **2.1 Security Policy Restricting Weapons**

Each court should establish a security policy that restricts weapons or other items that pose a security risk in the court facility.

RCW 9.41.300 (see Appendix B) prohibits weapons in courts. The local judicial authority should designate and clearly mark those areas where weapons are prohibited, and should post notices at each entrance to the building, both outside the courthouse and just inside the court entrance in appropriate languages. (A general rule of thumb is that the sign should be readable from 20 feet.)

Notices should also state that individuals and their belongings will be, or are subject to being, searched.

#### **2.2 Screening for Weapons**

Weapons screening is an essential part of court security. All courts should screen for weapons at every access point. All persons entering a courthouse should be subject to security screening.

Weapons screening stations should have:

- Adequate room for people to congregate inside, out of the weather, without being so crowded as to present additional security problems.
- A magnetometer, x-ray equipment, and hand-held magnetometers for backup screening.
- A duress alarm to summon additional help if needed.
- Closed circuit television monitoring of the access point.
- Adequate staffing of at least two trained staff to monitor traffic flow and at least one officer with a weapon to observe and respond to emergencies.
- Access to a private area to conduct more thorough searches using same gender personnel.

The court's weapons screening policy should include:

- A list of restricted items.
- A secondary screening policy for people who have not successfully passed through after two tries.
- Storage and disposal of confiscated or unauthorized items.
- Protocol for an appropriate response to attempts made to bring in weapons.
- Protocols for dealing with law enforcement personnel.

#### **2.3 Duress and Intrusion Alarms**

The court should have both intrusion and duress alarms. Duress alarms are designed to signal for immediate help. Recommended locations include: judges' benches and/or

staff positions in the courtroom, chambers, cashier stations, probation offices, and any office where staff may meet alone with the public.

Key issues with duress alarms are:

- Staff must be trained in both the locations and use of the alarms.
- The alarm should sound at the court's security station and at the responding law enforcement agency.
- Clear response protocols must be established with responding agencies. The court should accept only a response protocol that includes immediate assistance and no verification or cancellation by telephone.
- An armed officer should be on duty along with other security personnel.

Door alarms should also be placed in all exits from the building. Unsecured doors should be marked, "Emergency exit only; alarm will sound."

Court policy should address:

- The process for activating and deactivating the building alarms.
- Response to building alarms after hours and requirements for notifying court staff.

Intrusion alarms are designed to alert the court to unauthorized entry after hours. The alarms can be of several varieties, including space alarms, vibration alarms, and door contact alarms. The alarm system can be set to produce a loud sound to alert law enforcement and deter entry, or alarms can be silent to alert law enforcement only.

## **2.4 Testing of Security Equipment**

All courts should have a schedule for maintaining and testing security equipment.

Equipment should be properly maintained and tested on a recurring schedule to ensure that it works properly. High cost equipment, such as x-ray, should be included in the counties' or cities' Equipment Repair and Replacement (ERR) accounts.

## **2.5 Access to Caller ID or Call Trace on Phones**

All courts should have access to "Caller ID" or "Call Trace" on their phone systems (see Appendix C).

Caller ID and Call Trace allow courts to identify individuals who call in bomb threats or make other threatening calls to the court. Although Caller ID can be blocked, law enforcement may have access to Call Trace. For Caller ID and Call Trace to work, the local Private Branch Exchange (PBX) must support those functions.

## **2.6 Use of Force Policy**

The Security Committee should encourage the establishment of a courthouse "use of force" policy and be familiar with the terms of that policy.

The Security Committee should coordinate with the Sheriff's department or local law enforcement agency that provides security for the court in developing and understanding these policies.

## **2.7 Threat Assessment/Response**

Any judge or staff that has been threatened should request, and be provided, a threat assessment by local law enforcement (see Appendix D).

## **SECTION 3** **ACCESS CONTROL STANDARDS**

### **3.1 Limited Access - Main Entrance and Exit**

Courts should limit access to one main entrance and exit; however, if multiple entrances are used, each entrance should have weapon screening. Everyone entering the court should pass through a screening process.

Courts should make all reasonable efforts to have a separate access for judges and any other person subject to threat, in a particular proceeding. Attorneys, prosecutors, and staff may be accommodated by a separate screening line. These entrances should also be screened.

Limiting access/egress to one area allows better observation and detection, and reduces the cost of weapon screening equipment and staff. If the staff and judiciary use a non-public entrance, provisions should also be made for weapon screening at this entrance.

Entrances without screening should be locked and equipped with an alarm and a sign reading, "Emergency exit only; alarm will sound."

Courts with loading docks should make arrangements with all suppliers to provide necessary identification for drivers and to notify the court before making deliveries. The loading dock area should have personnel and equipment available to screen all incoming materials. All packages, when possible, should be x-rayed (including UPS, Federal Express, and USPS – see Appendix A).

Prisoner transport/access areas should be secured and used for prisoners only.

Multi-use buildings create special problems. Courts should make all reasonable efforts to reach agreements with all entities sharing a building. If the court cannot agree with other tenants and the funding unit, the court needs to clearly define and secure its space. Anyone entering the court area should pass through a single point for observation and screening.

### **3.2 Employee Identification Cards**

All court building employees should wear a visible identification card while in the courthouse or secured areas.

Identification cards allow courts to identify legitimate workers from visitors and others. Employees should wear a picture ID at all times. This ID may also be used as a cardkey for access to offices, etc. The ID should only show the employee's first name.

Courts should require a list of authorized personnel from jails and police or sheriff departments, so security personnel can verify the authenticity of law enforcement badges and staff identification.

### **3.3 Locking Mechanisms**

All locking mechanisms should be as sophisticated as electronic access cards or better.

Strict control of all locking devices should be maintained. The cleaning staff should not have unsupervised access to the court after hours. Keys and keypad locks are too easily compromised. New locking technology provides better security and easier replacement when compromised. The system should be administered by someone directly responsible to the court administrator or presiding judge.

Cardkey or Electronic Access Cards should be given to each employee. This is an individualized card that is programmed to allow access only to identified areas, during specific times. The access card also provides a record of each employee's movement in the building.

## **SECTION 4**

### **PHYSICAL FACILITY STANDARDS**

#### **4.1 Facility and Office Design**

Facility and office design should address security issues. Buildings should be designed to be secure and to protect against attack.

New facilities should be designed with three separate zones whenever possible: 1) public zone, 2) private zone for judges and staff, and 3) a secure zone for moving prisoners. These zones should not cross. Additionally, the design of offices, where staff meets regularly with clients or the public, should provide an escape route, either with a second exit or by strategic placement of the office furniture.

Current facilities should identify any areas, such as courtroom judges' benches, staff workstations, jury box, and public counters, which require additional protection. There are various options for adding security protection, such as bullet-resistant material, which fall within broad cost ranges.

Courts should also identify what rooms could be used as "safe rooms" where staff and jurors can go during an incident. The use of safe rooms should be included in initial and refresher staff training.

When necessary, and in all Domestic Violence cases, courts should provide security or an adequate secured area for the physical separation of adverse parties while waiting for trials or appearances.

#### **4.2 Installation of Physical Barriers**

All courts should make arrangements to install physical barriers around the court building when necessary to limit the approach of cars and trucks.

Each court should decide, in cooperation with local law enforcement, whether physical barriers are or may be required. Use of barriers can range from temporary, for high risk trials, to permanent structures. Information about where to get barriers and how they will be deployed should be part of a court security plan.

#### **4.3 Secure Parking**

All courts should have secured parking for any judge, staff, juror or party who has been or feels threatened.

Security incidents can occur in parking areas before the victim even reaches the courthouse. Judges and staff, who are vulnerable to attack simply by virtue of their positions, need secure parking. Jurors and threatened witnesses also need secure parking if they are to fulfill their roles in the justice system. However, jurors and witnesses should not park in the judge/staff parking area. Parking areas should be well

lighted with appropriate landscaping to prevent possible incidences. An escort to the parking area should be provided for any judge, staff, juror or party that has been or feels threatened.

Ideally, parking would be in a fenced area, with vehicle and pedestrian access limited by a gate, controlled by a cardkey or other access control device. Judges and/or staff should have direct access to secured corridors or elevators from the parking area. As an alternative, the court may reserve parking spaces for staff and provide patrols and monitoring. Judicial parking should be in reserved spots adjacent to the building. Signs reserving parking should in no way indicate who is parking in the space.

#### **4.4 Holding Areas**

All courts should have a secure, temporary holding area for prisoners.

Courts need secure holding areas where prisoners can be locked up and isolated while waiting to appear in court or be returned to jail. Holding areas should:

- Be constructed to lessen the possibility of self-inflicted injury.
- Be inspected daily for contraband.
- Include doors that allow for easy observation.
- Include toilet facilities.
- Be frequently checked by staff or law enforcement.
- Have CCTV monitoring, if possible.
- Have a self-contained breathing apparatus.

Courts should work with their local law enforcement to develop emergency procedures for prisoner control and evacuation.

#### **4.5 Building Controls**

All building controls (power, phone, environmental, computer, etc.) in court facilities should be secured, with access restricted to authorized personnel.

In order to avoid tampering and sabotage, access to controls for heating, air-conditioning, ventilation, etc., should be limited to authorized staff. Areas or rooms containing electrical or computer controls or maintenance equipment, should not be accessible by the public and should be secured at all times.

Outside air intake mechanisms should also be secured so they cannot be used as access to the building or as a conduit for biochemical attack.

---

# **APPENDICES**

---

## APPENDIX A

### SECURITY OF THE MAIL



## Security of the Mail

Best Practices for Mail Center Security

### **Incoming and Outgoing Operations**

*Presented by the United States Postal Inspection Service*

There are millions of businesses that use the mail. The vast majority of these have only 'one to a few' person(s) responsible for mail center-type operations. Of these millions of businesses, there are thousands of large, complex corporate mail center operations.

The best practices listed below are a summary of well-developed mail center security procedures that can be used by any mail center. **Procedures applicable primarily to large mail centers are identified as such, and *in bold*.**

These recommendations come from businesses that use the mail and have been shared with the USPS for distribution to its customers. Since needs and resources are often different, every suggestion may not apply to all businesses. Mailers should determine which are appropriate for their company and conduct periodic security reviews of their operation to identify needed improvements. The list below contains general security concepts and a few specific examples of how to accomplish them.

#### **General Mail Operation preventive measures recommendation:**

- Appoint a Mail Security Coordinator (and an alternate if a large mail center).
- Organize a Mail Security Response Team, as practical, depending on the size of the mail center staff.
- Create, update and/or review SOPs, Security Procedures, Disaster Plans, and Operating Plans. **Keep a back-up copy of plan(s) off-site.**
- Train personnel in policies and procedures relative to mail security, i.e. biological, chemical, weapons or natural disasters.
- Include from the staff, when possible, certified firefighters, biohazard handlers, and/or corporate safety, environment and health personnel, or, train personnel in these duties.
- Members of the team should be equipped with cell phones/pagers and should be available up to 24 hours a day, 7 days a week, as is appropriate for the situation.

- Information, and updates, about the personnel and response procedures should be published and distributed company-wide.
- Federal Government Mail Managers should also refer to the General Services Administration (GSA) web site for specific and updated information concerning federal mail management policies and procedures.
- Publish an After-Action Report or Incident Report after every incident.
- Have senior management buy-in/sign-off on company's mail security procedures.

### **General Safety and Security Procedures for Incoming/Outgoing Mail Areas**

- Notify internal and external customers, as appropriate, of steps taken to ensure safety of mail.
- Control or limit access of employees, known visitors and escorted visitors to the mail center with sign-in sheets, badges, and/or card readers. **(For large mail operations, include plant, workroom floor, etc.)**
- Subject to emergency exit safety requirements, lock all outside doors and/or prohibit doors from being propped open.
- Require deliveries to be made in a restricted, defined area.
- Restrict drivers (rest areas) to an area that is separate from the production/mail center facilities.
- Use video cameras inside and outside the facility/docks, as feasible.
- Keep the area for processing incoming and outgoing mail separate from all other operations, as feasible.
- If a separate processing area is used, it should not be part of the central ventilation system.
- Shut-off points of processing area's ventilation system should be mapped and should be part of an emergency procedures handout.
- Separate processing area should include appropriate personnel protection equipment and disposal instructions for such equipment, as approved by the CDC.
- Designate and publish/post evacuation routes for emergency situations.
- Conduct training, emergency preparedness drills, and information update meetings, as necessary.
- **X-ray all incoming mail. (Large mail centers.)**
- Maintain a Suspicious Package Profile.

- Ensure appropriate emergency access numbers are posted by or on every phone. Such numbers should include: call 911; CDC at 770-488-7100; local Postal Inspector; or local police or fire department.
- Maintain updated employee lists (name, address, phone/cell phone), and keep back-up copy off-site.
- Provide only vacuum systems for cleaning equipment, not forced air systems.
- If not already done, alter receiving procedures to require a manifest with all shipments and practice the acceptance of "complete" shipments only.
- Discarded envelopes, packages, boxes should be placed in a covered container and transported to the loading dock for removal. (Ensure local arrangements are in place for disposal of such material.)

### **Access to Information - Education and Communications**

- Maintain a library of publications, videos, brochures, from appropriate information sources, and facilitate employee access to them as needed. Sources should include USPS, CDC, and OSHA.
- Maintain and publish a list of useful websites from appropriate authoritative sources. Bookmark appropriate web sites for easy access, i.e. CDC, OSHA, USPS, and GSA. Monitoring twice a day is a minimum recommendation, as situations warrant.
- Maintain and publish list of phone numbers to call in an emergency - Postal Inspectors, Fire Dept., CDC, OSHA, Police, etc.
- Present updated Best Practices from CDC, OSHA, GSA, USPS, and Fire Dept.
- Company-wide communications concerning mail center security procedures should be implemented.
- Require/encourage applicable employees to attend all local meetings pertaining to mail security issues.

### **Guidelines for Mail Center Theft Prevention**

Mail is sometimes lost or stolen from company mail centers, or while en route to or from the Post Office. Much of this mail is quite valuable, containing cash, jewelry, and other high-value items. Needless to say, such losses are costly to the company and its investors. The following are some suggestions for improving theft prevention in your mail center operation:

- Know your employees. Don't put your new hires in your mail center without a criminal record check.
- Secure your mail center. Prevent access by unauthorized persons. Keep locked whenever possible, especially when no one is on duty. Maintain a sign-in sheet for

persons entering and leaving the mail center, including times of arrival and departure.

- Registered Mail™. Keep separate from other mail. Document transfer of Registered Mail by requiring the receiver to sign for custody.
- Protect company funds. If company funds are handled as part of the mail center operations, establish adequate controls to fix individual responsibility for any losses that may occur.
- Keep postage meters secure. Postage meters should be secured when not in use. Check mails periodically to determine if employees are using company postage meters for their personal mail.
- Vary times and lines of travel between post office and plant. If currency or other valuable mail is sent or received, check periodically to see if mail messengers are making unauthorized stops, or leaving mail unattended in unlocked vehicles.

Employees caught stealing should be prosecuted. There is no greater deterrent to a potential thief than the fear that he/she may go to jail. The Postal Inspection Service will extend its full cooperation.

### **Employee Security Procedures**

- Maintain good hiring practices.
  - Provide in-depth screening/background checks when hiring new employees.
  - Make arrangements with one or two temporary employment agencies to ensure that a restricted, pre-screened group of individuals is available when needed to supplement the workforce.
  - Enforce/institute probationary period for evaluation of employees.
- Establish a strict employee identification/personnel security program.
  - Require employees to wear photo ID badges at all times.
  - Instruct employees to challenge any unknown person in a facility.
  - Where provided to employees, utilize uniforms with names and logos stitched on them for employees to wear at work.
  - Provide a separate and secure area for personal items (e.g., coats and purses). Prohibit employees from taking personal items into the main workspace.
  - Establish incoming/outgoing personal mail procedures.
  - **Hire or designate security personnel for mail center area. (Primarily for large mail centers.)**
- Establish health safety procedures.
  - **Have on-site medical personnel (large mail center) or arrange for off-site facility/personnel**
  - Encourage employees to wash hands regularly, especially prior to eating.

- Encourage employees to see doctor if suspicious symptoms occur.
- Encourage employee attendance in health seminars, talks, info updates.
- As practical, establish or take advantage of company health programs, i.e. shots, check-ups.
- Provide approved personal protection equipment according to CDC guidelines.

**Some Critical Websites** - bookmark for quick reference: (include your various suppliers/vendors).

US Postal Service - [www.usps.com](http://www.usps.com)

Centers for Disease Control (CDC) - [www.cdc.gov](http://www.cdc.gov)

Occupational Safety and Health Administration (OSHA) - [www.osha.gov](http://www.osha.gov)

General Services Administration (GSA) - [www.gsa.gov](http://www.gsa.gov)

Federal Bureau of Investigation (FBI) - [www.fbi.gov](http://www.fbi.gov)

Bureau of Alcohol, Tobacco and Firearms (BATF) - [www.atf.treas.gov](http://www.atf.treas.gov)

***The above information was obtained from the US Postal Service website at <http://www.usps.com/communications/news/security/bestpractices.htm>***

## **APPENDIX B**

### **RCW 9.41.300**

Weapons prohibited in certain places—local laws and ordinances—exceptions—penalty.

(1) It is unlawful for any person to enter the following places when he or she knowingly possesses or knowingly has under his or her control a weapon:

(a) The restricted access areas of a jail, or of a law enforcement facility, or any place used for the confinement of a person (i) arrested for, charged with, or convicted of an offense, (ii) held for extradition or as a material witness, or (iii) otherwise confined pursuant to an order of a court, except an order under chapter 13.32A or 13.34 RCW. Restricted access areas do not include common areas of egress or ingress open to the general public;

(b) Those areas in any building which are used in connection with court proceedings, including courtrooms, jury rooms, judge's chambers, offices and areas used to conduct court business, waiting areas, and corridors adjacent to areas used in connection with court proceedings. The restricted areas do not include common areas of ingress and egress to the building that is used in connection with court proceedings, when it is possible to protect court areas without restricting ingress and egress to the building. The restricted areas shall be the minimum necessary to fulfill the objective of this subsection (1)(b).

In addition, the local legislative authority shall provide either a stationary locked box sufficient in size for pistols and key to a weapon owner for weapon storage, or shall designate an official to receive weapons for safekeeping, during the owner's visit to restricted areas of the building. The locked box or designated official shall be located within the same building used in connection with court proceedings. The local legislative authority shall be liable for any negligence causing damage to or loss of a weapon either placed in a locked box or left with an official during the owner's visit to restricted areas of the building.

The local judicial authority shall designate and clearly mark those areas where weapons are prohibited, and shall post notices at each entrance to the building of the prohibition against weapons in the restricted areas;

(c) The restricted access areas of a public mental health facility certified by the department of social and health services for inpatient hospital care and state institutions for the care of the mentally ill, excluding those facilities solely for evaluation and treatment. Restricted access areas do not include common areas of egress and ingress open to the general public;

(d) That portion of an establishment classified by the state liquor control board as off-limits to persons under twenty-one years of age; or

(e) The restricted access areas of a commercial service airport designated in the airport security plan approved by the federal transportation security administration, including passenger screening checkpoints at or beyond the point at which a passenger initiates the screening process. These areas do not include airport drives, general parking areas and walkways, and shops and areas of the terminal that are outside the screening checkpoints and that are normally open to unscreened passengers or visitors to the airport. Any restricted access area shall be clearly indicated by prominent signs indicating that firearms and other weapons are prohibited in the area.

(2) Cities, towns, counties, and other municipalities may enact laws and ordinances:

7(a) Restricting the discharge of firearms in any portion of their respective jurisdictions where there is a reasonable likelihood that humans, domestic animals, or property will be jeopardized. Such laws and ordinances shall not abridge the right of the individual guaranteed by Article I, section 24 of the state Constitution to bear arms in defense of self or others; and

(b) Restricting the possession of firearms in any stadium or convention center, operated by a city, town, county, or other municipality, except that such restrictions shall not apply to:

(i) Any pistol in the possession of a person licensed under RCW 9.41.070 or exempt from the licensing requirement by RCW 9.41.060; or

(ii) Any showing, demonstration, or lecture involving the exhibition of firearms.

(3)(a) Cities, towns, and counties may enact ordinances restricting the areas in their respective jurisdictions in which firearms may be sold, but, except as provided in (b) of this subsection, a business selling firearms may not be treated more restrictively than other businesses located within the same zone. An ordinance requiring the cessation of business within a zone shall not have a shorter grandfather period for businesses selling firearms than for any other businesses within the zone.

(b) Cities, towns, and counties may restrict the location of a business selling firearms to not less than five hundred feet from primary or secondary school grounds, if the business has a storefront, has hours during which it is open for business, and posts advertisements or signs observable to passersby that firearms are available for sale. A business selling firearms that exists as of the date a restriction is enacted under this subsection (3)(b) shall be grandfathered according to existing law.

(4) Violations of local ordinances adopted under subsection (2) of this section must have the same penalty as provided for by state law.

(5) The perimeter of the premises of any specific location covered by subsection (1) of this section shall be posted at reasonable intervals to alert the public as to the existence of any law restricting the possession of firearms on the premises.

(6) Subsection (1) of this section does not apply to:

(a) A person engaged in military activities sponsored by the federal or state governments, while engaged in official duties;

(b) Law enforcement personnel, except that subsection (1)(b) of this section does apply to a law enforcement officer who is present at a courthouse building as a party to an action under chapter 10.14, 10.99, or 26.50 RCW, or an action under Title 26 RCW where any party has alleged the existence of domestic violence as defined in RCW 26.50.010; or

(c) Security personnel while engaged in official duties.

(7) Subsection (1)(a) of this section does not apply to a person licensed pursuant to RCW 9.41.070 who, upon entering the place or facility, directly and promptly proceeds to the administrator of the facility or the administrator's designee and obtains written permission to possess the firearm while on the premises or checks his or her firearm. The person may reclaim the firearms upon leaving but must immediately and directly depart from the place or facility.

(8) Subsection (1)(c) of this section does not apply to any administrator or employee of the facility or to any person who, upon entering the place or facility, directly and promptly proceeds to the administrator of the facility or the administrator's designee and obtains written permission to possess the firearm while on the premises.

(9) Subsection (1)(d) of this section does not apply to the proprietor of the premises or his or her employees while engaged in their employment.

(10) Any person violating subsection (1) of this section is guilty of a gross misdemeanor.

(11) "Weapon" as used in this section means any firearm, explosive as defined in RCW 70.74.010, or instrument or weapon listed in RCW 9.41.250.

[2004 c 116 § 1; 2004 c 16 § 1; 1994 sp.s. c 7 § 429; 1993 c 396 § 1; 1985 c 428 § 2.]

Notes:

Reviser's note: This section was amended by 2004 c 16 § 1 and by 2004 c 116 § 1, each without reference to the other. Both amendments are incorporated in the publication of this section under RCW 1.12.025(2). For rule of construction, see RCW 1.12.025(1).

Finding—Intent—Severability—1994 sp.s. c7: See notes following RCW 43.70.540.

Effective date—1994 sp.s. c7 §§ 401-410, 413-416, 418-437, and 439-460: See note following RCW 9.41.010.

Severability—1985 c 428: See note following RCW 9.41.290.

## APPENDIX C

### CALL TRACE PROCEDURES

Contact your local telephone service provider and the local agency that provides telephone services to your county or city for information on Caller ID and Call Trace features. Some local Private Branch Exchange (PBX) systems may not support this service.

(Information was obtained from Qwest)

#### CALL TRACE

With Call Trace, you can receive assistance from your local phone company or police department if you receive harassing or threatening phone calls. This service is available to most customers on a pay per use basis.

#### To Use Call Trace

- Lift the receiver and press \*57 (or dial 1157 on a rotary phone) immediately after hanging up from the call.
- Follow the recorded instructions to take appropriate action.
- The telephone number of the caller will be recorded by the phone company. Deterrent action can be taken by local law enforcement agencies after one threatening call or your phone company after three harassing calls from an identified number.
- You will not be given the name or the telephone number of the person who called you. However, law enforcement agencies can be given this information.
- If it is a life threatening situation, contact the police immediately after completing the \*57 call, or have someone else call 911 while you complete the call trace procedures.

If you receive a threatening phone call at your home, take the same actions as above and call the local police.

## APPENDIX D

### THREAT ASSESSMENT/RESPONSE

There are three standard threat assessment methods:

1. The threat assessment should include a determination of the suspect's intent, motive, and ability regarding the threat.
  - How was the threat delivered?
  - Is the suspect known or anonymous?
  - Who is the focus of the communication?
  - What is the immediacy of the threat?
  - What outcome is requested?
  - Is the suspect incarcerated?
  - Is the suspect affiliated with a group?
  - Does the suspect appear to know personal details about his/her target such as home address and family members?
2. *The Dietz 10* should be applied. Park Dietz is a psychiatrist who studied risk to public figures. He identified 10 characteristics common to assassins. He opines that up to three characteristics can be found in any individual. Four to six characteristics is cause for concern and more than seven should cause grave concern.
3. JACA - is an acronym for a method used by the U.S. Marshal's Office. It stands for Justification, Alternatives, Consequences, and Ability. This method was developed by Gavin de Becker who developed the software used by the Marshal's Analytical Support Center for threat assessment.

The agency doing the assessment should provide a safety bulletin, as appropriate, to the threatened person, surrounding personnel, and the personnel in charge of screening those who enter the courthouse. The bulletin should include a photo and description of the suspect, if available. Part of the assessment should include an investigation of criminal history, anti-harassment, and protection/no-contact order history, mental health history, access to weapons and firearm records, and other databases available to law enforcement.

## **APPENDIX E – MODEL CHECK LIST**

### **Public Safety & Security Quick Reference Checklist (tailored for the Local Court)**

#### **General Public Security Emergency/Disturbance in Courtroom/Staff Area**

- Press Duress alarm, if available.
- Get judge/jurors and staff out of courtroom/general facility as quickly as possible.
- Call building security / local law enforcement / 911.
- Complete an incident report form. Email incident report form to:  
[Courtsecurity@courts.wa.gov](mailto:Courtsecurity@courts.wa.gov), or fax form to (360)586-8869 attn: Court Security.

#### **Remands into custody**

- Before announcing that a defendant will be remanded into custody, contact local law enforcement / building security to determine if an officer is available to take the defendant into custody.

#### **Anticipated Security Risk in Courtroom**

- For major events (i.e., high-profile trial; additional media attention; emotionally charged trial) notify Court Security or local law enforcement prior to hearing date.

#### **Bomb Threats and Personal Threats**

- If you receive a bomb threat by telephone, immediately call law enforcement and security personnel, and put into action any policies your facility may have regarding such an incident.
  
- Make sure to record the following information:
  - Telephone number at which the threat was received
  - Time of the threat
  - The words of the caller
  
- Ask the following questions:
  - When will the bomb explode?
  - Where is the bomb?
  - What does the bomb look like?
  - What kind of bomb is it?
  - Why did you plant the bomb?
  - Where are you calling from?
  - What is your name?
  - What is your address?
  - What is your telephone number?
  
- Make special note of the caller's voice (calm, excited, disguised, accent, etc.); the caller's gender; the caller's age (as indicated by voice); if the caller's voice was familiar; and any background noise during the call.

- If you receive a personal threat via the telephone, follow the same basic procedures as outlined above for a bomb threat, but make sure to ask what the caller wants and make note of any related threats and inform law enforcement of any reason you suspect the threat was made.
- If the threat was left on voice mail or email, save the message and contact local law enforcement immediately.
- Complete an incident report form. Email incident report form to: [Courtsecurity@courts.wa.gov](mailto:Courtsecurity@courts.wa.gov), or fax form to (360)586-8869 attn: Court Security.

### **Suspicious Packages or Mail:**

#### ➔ Suspicious characteristics to look for:

- An unusual or unknown place of origin
- No return address
- Excessive postage or excessive tape
- Oily stains, discoloration or crystallization on wrapper
- Wires or stings protruding from, or attached to an item
- Incorrect spelling on label
- Odd looking or foreign-style handwriting or misspelled or incorrect address or title
- Different postmark and return address
- Strange odor (Many explosives smell like shoe polish or almonds.)
- Unusual package weight
- Uneven balance or odd shape
- Springiness in the top, bottom, or sides

#### NEVER DO THE FOLLOWING:

- ✗ Never cut tape, strings, or wrapping on a suspicious package.
- ✗ Never immerse a suspicious package or letter in water, as either of these actions could cause an explosive device to detonate.
- ✗ Never touch or move a suspicious package or letter.

#### ➔ Actions to Take:

- Report any suspicious packages or mail to local law enforcement immediately.
- Complete an incident report form. Email incident report form to: [Courtsecurity@courts.wa.gov](mailto:Courtsecurity@courts.wa.gov), or fax form to (360)586-8869, Attn: Court Security.

### **Building Evacuation:**

- Evacuate immediately unless told to remain where you are for safety reasons.
- Bailiffs – Take list of juror’s names/phone numbers.
- Supervisors – Take list of employees’ names for roll call.
- Gather at a pre-designated site and check in with Supervisor who will conduct roll call and give further instructions.

**Security at Building Entrances:**

- Use only authorized entrances and exits.
- If your facility utilizes employee identification badges, make sure to always display your badge when entering the facility. Never allow anyone else to use your employee badge, and never use your badge to provide entry to visitors.

**Security Inside Buildings:**

- Make sure all doors leading to public areas have secure locking mechanisms.
- Use an organized key control system to track possession of keys. A key inventory should be conducted semi-annually and, if any keys are missing, locks should be replaced.
- Maintain a list of emergency contacts for all employees at your facility.
- If your facility is equipped with alarms, know their location and how to use them.
- Do not admit unexpected visitors, including repair and delivery people, without checking with your supervisor or security personnel first.
- Keep security doors locked at all times.
- Keep sensitive files, valuable items, and valuable personal property under lock and key at all times.
- Do not leave personal property in locations where it can be stolen or tampered with.
- Be alert for strange objects and packages in and around your facility. Report any such package or object to law enforcement and/or security personnel immediately.
- Try to be inconspicuous when using public facilities and transportation. Do not wear clothing that calls attention to your official position. Your mannerisms and conduct should not attract attention.

## Building Security Quick Reference

### 1. Emergency Telephone Numbers

For all emergencies, call 911 (or 9-911 depending on your jurisdiction's telephone system.) Additionally:

- a. For Fire, call \_\_\_\_\_
- b. For Medical, call \_\_\_\_\_
- c. For Police, call \_\_\_\_\_
- d. For Security, call \_\_\_\_\_
- e. For immediate Security response call \_\_\_\_\_

### 2. Duress alarms

Duress alarms are to be used when an immediate need for emergency assistance occurs. Depression of the duress alarm will result in immediate police dispatch to the area in which the duress alarm was activated. After depressing duress alarm, contact Police at \_\_\_\_\_ to provide details regarding the emergency.

- a. Duress alarm(s) at the public counter Yes \_\_\_\_\_ No \_\_\_\_\_
- b. Duress alarm(s) in the courtroom(s) Yes \_\_\_\_\_ No \_\_\_\_\_
- c. Duress alarm(s) in chambers Yes \_\_\_\_\_ No \_\_\_\_\_
- d. Duress alarm in \_\_\_\_\_
- e. If you accidentally depress a duress alarm, immediately call Police at \_\_\_\_\_ to cancel the Police response.

## **Court Personnel - Home & Personal Security Checklist**

### **Residential Security:**

- Arrange for an unlisted home telephone number so your address will not be as readily accessible.
- Check your phone number using google.com, and if your address (and a map) appear you can request that google.com remove it.
- Change or re-key the locks if the keys are ever lost or stolen. Also, remember to change the locks when moving into a previously occupied home.
- Refuse any unordered packages and any unrequested deliveries.
- Post emergency numbers by the phone, i.e. local law enforcement, hospitals, doctors, and the fire department.
- Do not answer your home phone with your name or official title.
- Report all threatening phone calls to local law enforcement.
- Consider using an answering machine to screen your phone calls, and do not include your name or phone number in your answering machine message.
- Do not put your name on the outside of your residence or mailbox.
- Make sure your home is well lit and use security (motion sensing) lighting.
- Control vegetation and landscaping to eliminate hiding places and prevent obstruction of lines of sight. Trim trees at least 6 feet from the ground.
- Consider varying route and travel times to and from work.
- Consider having your local law enforcement or Sheriff conduct a security assessment of you residence.

### **Identification:**

- Do not use personalized plates that identify you by name or official position.
- Do not have your name or title displayed at your office parking place.

### **Identity Theft Protection:**

- Separate personal and professional email accounts; update antivirus software.
- Shred or destroy documents and paperwork with personal information before you discard the documents.
- Never provide personal information on the phone, via mail, or via the internet unless you are dealing with an entity you know and trust.
- Never click on links in unsolicited e-mails, or provide any personal or financial information unless you type in the web address. Make sure you use effective internet security measures that are up to date like anti-virus software, antispyware programs, and a personal firewall. Also, make frequent back-up copies of important data on a removable disk and store it in a safe place.

- Be particularly wary of “phishing” e-mails which may appear to come from your bank or another company with which you do business, and request you click on a link to “verify personal information.”
- Make sure passwords and pin numbers are not obvious or easily guessed, and change passwords frequently.
- Do not leave mail in your mailbox overnight or on weekends.
- Put all outgoing mail in a secure U.S. Postal Service collection box.
- Keep all personal information and important documents in a secure location.
- Make sure you include information on all your accounts, including customer service numbers.
- Be alert to signs your identity may have been stolen, such as bills that do not arrive, unexpected account statements or credit cards, denial of credit for no apparent reason, and calls or letters about purchases you did not make.
- Monitor your credit report for suspicious activity. To obtain a free copy of your report go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228.
- Carefully review all financial and account statements for suspicious or unauthorized activity.
- For more information on what to do if your identity is stolen, go to [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**Campaigning Precautions:**

- Arrange for security at parades, dinners, and events.
- Take someone along when going door to door.
- Do not use your home address on campaign materials.

## **COURTROOM SECURITY CHECKLIST**

- Set rendezvous point for courtroom personnel in the event of a building evacuation.
- Create a safety plan for jurors in the event of an emergency or building evacuation.
- Establish emergency communications plan for courtroom staff, including contact information.
- Provide list with contact information for building security, courtroom staff and emergency personnel near telephones.
- Find a secure place to lock sensitive information.
- Regularly test duress alarms in the courtroom.
- Scan for and remove all potential weapons.
- Regularly check performance of court security cameras.
- Review visibility of courtroom and chambers at day and at night from the outside.
- Account for all keys to the courtroom and court office.