Judicial Security Considerations

Presented by Sergeant Tammy L Johnson
WISCONSIN CAPITOL POLICE
Tammy.johnson1@wisconsin.gov

Behavioral Indicators

Be mindful of individuals demonstrating any of the following behaviors, which may indicate a mental health issue or pending security threat:

- Profuse sweating.
- Loitering without a reasonable explanation and/or for an extended length of time.
- Prolonged interest in an unusual manner.
- Avoiding security personnel or systems.
- Expressing or implying threats of violence.
- Unauthorized people trying to enter a restricted area or impersonating authorized personnel.
- Abandoning packages, boxes, suitcases, briefcases, etc.
- Inquiring about security protocols.
- Body language that is not appropriate for the situation (e.g., inappropriate responses when event speaker is speaking)

Away from the courthouse

Personal Security Considerations

- Create a personal or family emergency action plan and share it with Marshal or Sheriff as applicable.
- Vary daily routine.
- Tell a trusted person where you are going, particularly if outside of daily functions.
- Stay in well-lit public areas and avoid isolated streets.
- Identify scheduled local demonstrations to avoid large crowds.
- Hide personally identifiable information while in public areas.
- Carry simple-to-use protective tools such as pepper spray.
- Head to the nearest police station if being followed.
- Keep hands free as carrying items may result in further vulnerabilities.
- Avoid text messaging or lengthy cell phone use while walking alone.
- Be extra alert and know who and what are in the vicinity.
- Trust instincts and be assertive in decision-making; calling police, if necessary.
- Abstain from using judiciary authority or title on personal time.
- Change online passwords often. Use different passwords for each online account. Using a sentence as a password is recommended.
- Use two-factor authentication for logging into accounts when possible.
- Refrain from logging into bank accounts, e-mail, or social media accounts while on public Wi-Fi hotspots. When possible, use a reliable virtual private network service provider.
- Back up personal data and important records to a virtual, cloud environment or store hard copies of digital data at a physical location elsewhere. This will reduce vulnerability to ransomware.
- Protect computers by keeping firewalls turned on and keeping operating systems and antivirus software up to date.
- Avoid updating photographs on file with the news media or the government whenever possible.
- If appropriate, request media does not show photographs of your family or residence.

  Social Media:

  - Use caution when posting to social media, particularly when it comes to personally. identifiable information. Remember that once information has been posted to a social networking site, that information is no longer considered private.
  - Take advantage of privacy settings when using social media.

- Do not engage online or in social media with persons who have done business with the court.
- Beware of social media and email scams.
- Avoid posting names, ages, or schools of children.
- Never publicly announce that you are going out of town for work or vacation.

Safety Considerations in Public

- Make restaurant reservations and food orders using an alias.
- Avoid sitting near front windows in restaurants.
- Avoid using the title "Judge" on personal checks, credit cards, airline tickets, etc.
- Notify law enforcement when agreeing to speak in public or ride in parades. Be sure there are provisions made for security and crowd control.

Safety Considerations at Home

- Consider installing a peep hole on your door(s), and do not open the door to strangers.
- Consider installation of motion sensors.
- Consider installation of controllable security cameras.
- Consider installation of a Home Intrusion Detection System and utilize it.
- Consider installing 3M security film on all windows.
- Keep the residence's perimeter visible (e.g., well-lit with motion detection lighting and shrubs well-trimmed).
- Secure sheds and garages because tools such as ladders may be used to break into homes.
- Never leave a spare key under a mat or in a hiding place outside of the home.
- If utilizing a numeric keypad lock system, change the access number routinely.
- If utilizing a garage, make sure the door from the garage to your residence has a dead bolt.
- Take garage door openers out of cars when parked on the street or in driveways.
- Consider renting a Post Office Box to keep home addresses secure.
- Consider obtaining informed delivery with USPS.
- Only display addresses on mailboxes, not names.
- Avoid suspicious packages. Recognize potential indicators of a suspected explosive.
- Only open envelopes when you know the sender.
- Refrain from throwing away "hate mail." Instead, report it to court security and local law enforcement. Such mail may be helpful to investigators down the road. Refer to court policies on hate mail.
- Make sure that telephone and cell numbers are un-listed and non-published.
- Ensure home Wi-Fi is password-protected and uses a generic network identifier.

- Designate a “safe room” in the home that has a solid core door, a deadbolt lock, and a telephone or a cell phone with a charger when able.
- When traveling, make the house look lived in (e.g., set timers for lights and radios, redirect mail).
  - Practice *what-if* scenarios with family focusing on dangerous situations (e.g., intruders, fire).
- If neighbors are aware of your position, instruct them not to give strangers information about you or your family.
- Have personal and family information secured confidentially with the local law enforcement agency in your jurisdiction so that it can be used in an emergency situation.
- Refrain from announcing your name and phone number on voicemail greeting messages and from providing anonymous callers with any personally identifiable information.
- Return office telephone calls from only office phones unless the number is restricted.
- Have the ability to record telephone conversations in both the office and the home.
- For business, always give a work address or Post Office Box rather than a home address.
- Personally remove mailing labels containing names and addresses when bringing mail to the courthouse.
- Consider reinforcing windows with 3M coating to reduce unauthorized entry. Link: https://www.3m.com/3M/en_US/home-window-solutions-us/solutions/safety-security/
- Consider installing a voice-activated radio-dispatched alarm, or “VARDA” alarm. This is a burglar alarm that, when activated, broadcasts the type of alarm and the location of the transmitter over the local police radio frequency. Link: https://response-technologies.com/centurion- defender/

Safety Considerations While Commuting

- Take different routes to and from home and the office.
- Vary arrival and departure times at the courthouse every day.
- If you must leave the courthouse during the day, confidentially notify someone where you are going, what you will be doing, and when you should be expected to return to the building.
- Do not drive directly home if you perceive someone might be following you. Gas is cheaper than your life, so keep driving while deciding whether to go home.
- Request a court security officer escort when leaving the courthouse during late hours or when applicable.
- Consider concealing your judicial robes when transporting them in your vehicle.
- Travel with a fully charged cell phone.
- Maintain an emergency supply kit in your vehicle. Examples of suggested items include a spare tire and repair tools, jumper cables, a flashlight with extra batteries, and a first aid kit.
- Set up emergency contacts and medical information on your cell phone that can be accessed by first responders in the event of an emergency.

- Maintain at least a half tank of gas in your vehicle.
- Know where you are when traveling (be able to provide mile markers to dispatch or signage).

Ensuring the physical safety of visitors to courthouses around Wisconsin

High-profile cases require a collaborative team effort from the courthouse staff, attorneys, and local law enforcement. Prior to any high-profile case the recommendation is two meetings be conducted. The first meeting should be with staff such as JA, Clerk, sheriff, and facilities. The second meeting should include all involved attorneys.

Below is a plan to assist in maintaining decorum in the courtroom during high-profile trials.

Inside and Outside the Building

- **Determine expectations of involved Law Enforcement** ○ Where does the Judge Order end and law enforcement begin during the proceedings ○ Clear expectations.
    - Law Enforcement should share an Incident Action Plan
        - Determine expectations for evacuation in the event of an catastrophic event
- Evaluate the venue ○ Courtroom size – (large enough to accommodate media, staff, presenters, and visitors) ○ Ingress and egress (separate entrances are recommended) ○ Ample parking (judge, staff, visitors, and media)
    - Quantity and quality of security cameras (lighting inside and out)
    - Magnetometers (no one bypasses, including staff and attorneys; acquire one if courthouse does not have one)
    - Bollards to prevent vehicle attacks on all sides of the building (where appropriate) ○ Locked doors.
    - Visible barriers (stanchions, signs, restricted access areas)
    - Accessibility of internal hazards (HVAC, electrical, roof, basements, water supply) ○ Deliberation areas (secure and inaccessible to the public)
    - Seating in the courtroom (not recommended to seat victim and defendant's families together – clearly define the separation prior to entry)
    - Use of electronic devices (laptops, phones) and WIFI access (if password is provided it is recommended it be changed following proceedings)
    - Secure areas for the jury
    - Brush and trees (are trees climbable with visibility, climbable to allow access to roof or other parts of the building and is anything obstructing view from interior)
    - Resistive windows with minimal view from exterior
    - Duress alarms (functionality – test with dispatch for proper location information, adhered to desk, operation training and location identified correctly by the user)

- Visitors, Staff, Judges and Law Enforcement ○ Incident Action Plan (IAP) (updated for each event) ○ Evacuation plan (updated) – Update all staff training ○ Shelter in place plan (updated) – updated all staff training
    - Piggyback training (no holding doors)
    - Identifying staff (policy for wearing IDs visible in appropriate manner) o Internal law enforcement (hallways, courtroom, doors etc.- this may fluctuate) ○ External law enforcement (doors, visibly in the courtroom –large windows) ○ Access for law

enforcement (keys, fobs to ALL areas) ○ External squads (parking, high visibility, easy access) ○ K-9 presence (vapor wake or bomb sniffing daily)

- Expectation of securing visitors and removal of visitors (who determines when to remove – does law enforcement have carte-blanche authority to remove disorderly or disruptive individuals, i.e. loudly mumbling, body language aggressive such as hand gestors, sleeping)
- Communication for judge to law enforcement (duress alarms) ○ Identifying staff (policy for wearing IDs visible in appropriate manner) o Capabilities of the bailiff (armed, unarmed, response time, communication abilities) ○ Is there known medical knowledge/concerns for jurors, staff, judge, attorneys or likely visitors such as family members.
- Is there foresight of ADA accommodations (prepare for the unexpected)

- Evaluation of immediate surroundings ○ Surrounding buildings with clear line of sight **o** Commute for parties (judges, attorneys, witnesses, jurors) ○ Rescue (volunteer or staffed) ○ Fire (volunteer or staffed)
  - Trauma centers (notify local hospital security when needed)
  - Officers on the road (how many may be needed in the event of an emergency)
    - Trained officers inside the venue (courthouse or alternate) ○ Airspace (drones prohibited)
  - Protest location defined (plan for civil unrest in some situations and have a dedicated location prepared)

- Cyber Security – including monitoring all comments on listed recommendations on social media monitoring ○ Email monitoring ○ News monitoring.
  - Secure video feeds (Zoom, Microsoft Teams, and other abilities to communicate electronically)
  - Internal firewall monitoring (CCAP assistance)