Securing Justice

Report from the **COSCA Policy Committee**

December 5, 2025

COSCA
Conference of State Court Administrators

Contents

Introduction

It is incontrovertible that the security of court facilities and the safety of those who work in or use courts is a necessity. Literally dozens of books, hundreds of articles, countless training programs, and other resource materials exist explaining the need for courthouse safety and what the best practices are for enhancing the security of buildings and protecting judicial officers, court staff, litigants, jurors, and bystanders.[1] The topic has been a central focus of the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA) for over twenty years. In 2005, the National Center for State Courts (NCSC), in partnership with the National Sheriffs' Association and the Bureau of Justice, which is a division of the U.S. Department of Justice, hosted the National Summit on Court Safety and Security. Since 2005, CCJ and COSCA have issued seven separate resolutions in support of court security and emergency preparedness initiatives. Court leaders understand the importance of protecting judicial officers and court staff and the unique responsibility that arises from wielding the power to require ordinary citizens to respond to a court summons or subpoena. Although many protocols and procedures are in place, much remains to be done.

The focus of this paper is on the unique responsibilities of state supreme courts or state judicial councils, local government boards and agencies, and individual judicial officers and court staff to enhance the security of court facilities and the safety of those who work for and use the court system. Inherent in this discussion are the three fundamental elements of effective court security: communication and collaboration between stakeholders at all levels, the willingness of leadership to prioritize security issues, and active oversight and funding for improvements.

---

1 A very short list of court-specific security resources includes: *CCJ/COSCA Court Security Handbook: Ten Essentials Elements for Court Security and Emergency Preparedness*. Sept. 2012. **https://perma.cc/D7J5-35XH**; American Bar Association Judicial Security Committee. *Judicial Security Articles*. **https://www.americanbar.org/groups/judicial/committees/judicial-security/articles/**; National Association for Court Management. *Court Security Guide*. 2024; National Center for State Courts. *Personal Safety Inside, Outside the Courthouse: A Guide for Judges & Staff*. **https://www.ncsc.org/resources-courts/personal-safety-inside-outside-courthouse-guide-judges-staff**; National Center for State Courts. *Courthouse Planning and Security*. **https://www.ncsc.org/resources-courts/operations-governance/courthouse-planning-security**; National Center for State Courts. *High-Profile Case Management*. **https://www.ncsc.org/resources-courts/high-profile-case-management**; National Center for State Courts. *Creative Learning Services Portfolio: Arkansas Court Officer Training I and II webinars* (available upon request to National Center for State Courts). A more comprehensive list of resources on court security may be obtained through the Resource Library division of the National Center for State Courts.

Threat Landscape

The factors that make judicial officers, court staff, and court buildings high-profile targets are familiar to most court professionals. It is an unfortunate reality that public confidence in courts continues to drop.[2] Although the most recent NCSC State of the State Courts survey shows a slight increase in confidence in state courts, this must be read against a backdrop of years of dropping confidence in state courts and a Gallup poll released in the same time period showing a dramatic drop in trust in the judiciary.[3] In addition to court decisions that may be unpopular, the spread of disinformation fuels suspicion and stirs anger toward courts in general and specific judicial officers in particular.[4] It is perhaps due in part to this declining confidence in the judicial branch that judicial officers, court staff, and those that provide court-annexed services face frequent threats and harassing behavior.

A judicial officer who holds the fate of another's future in their hands can become a convenient target for those who feel they were disrespected or treated unfairly by either the legal process or by the other party to the action. In October 2023, Maryland Circuit Court Judicial Officer Andrew Wilkinson was murdered in his driveway by a litigant in a child custody case the judicial officer had ruled on earlier that day.[5] On June 3, 2022, John Roemer, a retired Wisconsin circuit court judge, was murdered in his home by a defendant he had sentenced to prison six years

---

2 Whitehurst, Lindsay. *Threats to Federal Judges Have More than Doubled in 'Alarming' Spike, US Marshals Director Says.* AP News. Feb. 14, 2024. **https://perma.cc/8XVX-F3HT**.

3 Karp, Jack. *Public Faith in State Courts Up as Trust in Fed. Courts Sinks.* Law 360 Pulse. Dec. 23, 2024. **https://www.law360.com/pulse/articles/2277007/public-faith-in-state-courts-up-as-trust-in-fed-courts-sinks** (citing Saad, Lydia & Benedict Vigers. *Americans Pass Judgment on Their Courts*. Gallup. Dec. 16, 2024. **https://news.gallup.com/poll/653897/americans-pass-judgment-courts.aspx**).

4 Conference of State Court Administrators. *Courting Public Trust and Confidence: Effective Communication in the Digital Age*. Dec. 2022. **https://cosca.ncsc.org/resources-courts/courting-public-trust-and-confidence-effective-communication-digital-age**.

5 Skene, Lea et al. *A Slain Maryland Judge Presided Over the Divorce Case of Man Identified as a Suspect in His Killing*. AP News. Oct. 20, 2023. **https://apnews.com/article/maryland-judge-shot-killed-394b2eaf2570813d1f2845c45f8a99fe**.

earlier.[6] In Texas, District Court Judge Julie Korucek was shot in her driveway on November 6, 2015, by a defendant facing a probation revocation hearing.[7]

Direct threats or harm towards judicial officers tend to be the highest profile of all judicial security concerns. Consequently, most courts collect some data on these types of direct threats or harm. Conversely, there is a dearth of information about incidents or threats directed toward court staff. Data available from North Dakota shows consistent annual trends of juvenile staff being involved in 16% of reported security incidents. Juvenile court probation officers are at an especially high risk for threats and actual injury due to both the nature and the location of their work. Because they are supervising youth in the community, frequent interactions with the youth and the youth's family members occur outside of secure facilities. North Dakota Clerks of Court and their staff are involved in an average of 10% of reported security incidents. Other reported incidents involved attorneys representing either the state or the other party to an action, jurors, and court reporters. Data collected by the Washington state courts shows that 21% of security incidents involved judicial officers and another 21% involved court employees, while 34% involved court users or the general public.[8]

When courts summon individuals involved in intensely emotional disputes to the courthouse, they have an obligation to ensure that prudent and effective safety measures are in place for both the litigants and bystanders. On visits to rural courthouses, Oregon Chief Justice Meagan Flynn and Oregon State Court Administrator Nancy Cozine heard firsthand accounts of domestic violence victims being stalked to courthouses and court staff having to shelter them until law

---

6 Winter, Tom, et al. *Former Wisconsin Judge Killed in 'Targeted' Attack; Suspect Had Hit List that Included Mitch McConnell, Gov. Whitmer*. NBC News. June 4, 2022. **https://www.nbcnews.com/news/us-news/former-wisconsin-judge-killed-targeted-attack-suspect-hit-list-include-rcna31995**.

7 United States Attorney's Office for the Western District of Texas. *Houston Man Sentenced to Life in Federal Prison for Racketeering Schemes that Involved the Attempted Capital Murder of State District Judge Julie Kocurek*. U.S. Department of Justice. Oct. 2, 2018. **https://www.justice.gov/usao-wdtx/pr/houston-man-sentenced-life-federal-prison-racketeering-schemes-involved-attempted**.

8 2024 data provided by Washington Courts Security Consultant.

enforcement could arrive.[9] Recent incidents occurring on courthouse property in Kentucky,[10] Pennsylvania,[11] Tennessee,[12] and Rhode Island[13] involved litigants, families of litigants, or enemies of litigants rather than judicial officers or staff. Additionally, incidents of jurors who report being harassed, stalked, and bullied appear to be increasingly common.[14]

While courthouses are generally considered safe places, there are enough high-profile incidents to remind everyone that there remains an urgent need to continue to implement safety measures.[15] Research has shown that mass shooters target certain sites if they are identified with or representative of a specific grievance, but mass shooters are also likely to choose to target an iconic or symbolic site to send a wider message to society.[16] The most prominent example of this is the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. The bomber in this incident was a Michigan man who was motivated by general antipathy toward several federal agencies and by anger over specific events that occurred in Idaho and Texas.[17]

---

9 Remarks of Nancy Cozine. COSCA Board Meeting. Nov. 20, 2024.

10 *Suspect In Shooting Outside a Kentucky Courthouse Has Died from a Self-Inflicted Gunshot Wound*. AP News. Aug. 20, 2024. **https://apnews.com/article/courthouse-shooting-kentucky-7fa3d4daa913398b53fdb248fa10d943.**

11 Muniz, Vivian. *Victim Identified in Northumberland County Courthouse Shooting*. 2822news.com. **Aug. 16, 2024. https://www.2822news.com/crime-court/pd-shooting-near-northumberland-county-courthouse/.**

12 *Judge Dismisses Lawsuit from Family of Man Who Was Stabbed at Courthouse*. Action News 5. Aug. 16, 2024. https://www.actionnews5.com/video/2024/08/17/judge-dismisses-lawsuit-family-man-who-was-stabbed-courthouse/.

13 *Man Shot Outside Providence Courthouse Reaches Settlement with City*. NBC 10 News. May 6, 2022. **https://turnto10.com/news/local/man-shot-outside-providence-courthouse-reaches-settlement-with-city.**

14 *See, e.g.*, Swygart, J. *Juror Harassment Alleged in Page Trial*. LimaOhio.com. May 15, 2025. **https://www.limaohio.com/top-stories/2025/05/15/juror-harassment-alleged-in-page-trial/**; *New Mexico Attorney General Raúl Torrez Condemns Harassment of Juror and Defends Integrity of Justice System After Judge Releases Defendant Following Manslaughter Conviction*. New Mexico Department of Justice. Mar. 21, 2025. **https://nmdoj.gov/press-release/new-mexico-attorney-general-raul-torrez-condemns-harassment-of-juror-and-defends-integrity-of-justice-system-after-judge-releases-defendant-following-manslaughter-conviction/**; Fieldman, Luis. *'Very Nasty': Juror from Karen Read Trial Says They Fear for Their Safety*. MassLive. Jul. 18, 2024. **https://www.masslive.com/news/2024/07/very-nasty-juror-from-karen-read-trial-says-they-fear-for-their-safety.html**.

15 Since 2013, the National Center for State Courts has published a Court Security Bulletin which includes a round-up of court security-related news headlines that will typically include 20 or more incidents. The bulletin is available as a free subscription at: **https://www.ncsc.org/newsletters?email=**.

16 Peterson, Jillian and James Densley. *The Violence Project: How to Stop a Mass Shooting Epidemic*. Abrams Press. 2021.

17 Jenkins, John Philip. *Oklahoma City Bombing*. Britannica. (Sept. 26, 2025). **https://perma.cc/ER7Z-TQQL**.

Targeting a location that is not tied to a site-specific grievance makes it more difficult to plan for and prevent incidents but also speaks to the need for comprehensive security measures. John Muffler, a faculty member of the National Judicial College and a former administrator of the National Center for Judicial Security, sums up the need for security awareness succinctly: "Violence is always situational. Premeditated violence is both predictable and preventable."[18]

Security is a Shared Responsibility

The provision of court services, including security, is multi-layered. Responsibility for court security may be spread between the highest court in the state or its state judicial council, the local government where each court is located, and the individual judicial officers and court staff who make up the court system. An understanding of assigned or assumed responsibility for each type of security consideration is key to making improvements.

COSCA understands that courts are structured differently. The discussion that follows should be construed to assign those responsibilities to the level that best fits the reader's situation and court structure. Because judicial officers exist at different levels within state court systems and have varying titles, this paper uses the term "judicial officer" unless the term "judge" is specifically used in a reference source.

I. Supreme Court and/or State Judicial Council Responsibility

The highest court within each state court system or a state's judicial council has the overall responsibility to advocate for legislation, secure funding, and ensure that courts have a voice in matters of security and emergency preparedness. The highest court or judicial council can also invoke its rulemaking and administrative authority to require or encourage courts at all levels to undertake security efforts.

18 Muffler, John F. *Adjudicating in an Unsecured Workplace: How to Assess and Stay Safe*. Court Manager. Vol. 33, no. 4, Nov. 2018.

Leadership at the highest levels should be familiar with the CCJ/COSCA Court Security Handbook.[19] The Handbook is designed as both an implementation guide and a means of measuring progress toward security and emergency preparedness goals. The 2016 report issued by the Arizona Court Security Standards Committee is another comprehensive guide to developing standards for courthouse and courtroom security.[20] Reference to these essential guides, as well as implementation of the following recommended measures, will ensure a security infrastructure capable of responding to the ever-changing landscape of threats faced by our state courts.

Recommendation #1: Create and Support Staff Positions with Responsibility to Monitor Safety and Respond to Safety Issues

States should establish a senior-level security or emergency management position and staff, to the extent practicable, within the office of the state court administrator. This position should be the main point of contact to identify security needs, receive incident reports, coordinate with law enforcement entities, direct training for judicial officers and court staff, and ensure that local security plans are in place. Examples of longstanding programs include:

- The Chief Justice of the Oregon Supreme Court has statutory authority to appoint a chief judicial marshal and others to implement court security, emergency preparedness, and business continuity operations, and to provide for the physical security of judicial officers or staff operating under the Judicial Department or the staff of the Office of the State Court Administrator.[21]

- The Illinois Supreme Court and its appellate courts are protected through a marshal service created by statute. This statute specifically creates a marshal service for the Supreme Court and imbues its officers with full police powers.[22]

---

19 **CCJ/COSCA Court Security Handbook: Ten Essentials Elements for Court Security and Emergency Preparedness**.

20 Arizona Supreme Court. *Ensuring Secure, Open, and Publicly Accessible Courts*. 2016. **https://perma.cc/K5JE-HEYP**; *see also* Arizona Administrative Order 2017-15 *Adoption of Court Security Standards and Implementation of Committee Recommendations*. Feb. 8, 2017. **https://perma.cc/YAV3-58T6**.

21 **ORS § 1.177**.

22 705 ILCS 5/11.

- The Texas Judicial Branch Division of Court Security was created under the Judge Julie Kocurek Judicial and Courthouse Security Act of 2017.[23]
- The Ohio Office of Court Security provides building and personnel security at the Moyer Judicial Center. The Office also performs security assessments for local courts, assists local courts with developing continuity of operations plans, and provides security education for new judges and their families.[24]
- Arkansas's Director of Security and Emergency Preparedness is a legislatively authorized position with the responsibility of assisting with the development of security and emergency preparedness plans for the judicial branch of government, including the supreme court, circuit courts, and district courts.[25]

The director of security may have a background in law enforcement, should receive training specific to physical and personal threat assessment and response, and should thoroughly understand the unique aspects of court operations. This position should be responsible for creating and updating emergency response plans by working with local courts to include relevant information and resources.

The director of security should be the primary point of contact to whom judicial officers and staff report threats or security incidents. This position should develop incident reporting forms and train all staff and judicial officers as to what, to whom, and when to report security issues. The director of security should coordinate with facilities managers and IT directors regarding selection, placement, and installation of courthouse security systems, including access controls, duress alarms, and video cameras. This position could also serve as a consultant on policies regarding courthouse and personal security, such as the availability of surveillance video recordings, ability to film or photograph in courthouses, prohibited items, law enforcement access to courthouses and whether they are allowed to be armed, and how to manage protests and public unrest.

---

23 Judge Julie Kocurek Judicial and Courthouse Security Act of 2017. SB 42 (Texas). **https://perma.cc/4X25-GNB4**; *See also, Court Security*. Texas Judicial Branch. **https://www.txcourts.gov/programs-services/court-security/**.

24 *Court Security Section*. The Supreme Court of Ohio & The Ohio Judicial System. **https://www.supremecourt.ohio.gov/courts/services-to-courts/court-security/**.

25 **A.C.A. § 16-10-1006**.

It is imperative that the director of security build relationships with local law enforcement and any contracted security screener services to ensure there is a clear understanding of the roles and responsibilities of the director regarding courthouse and personal security issues. The security director should be authorized with the appropriate clearance to share information with the state's fusion center. Fusion centers are state-operated entities that are part of a national network established following 9/11 for the purpose of gathering, analyzing, and sharing threat-related information among state, local, tribal, federal, and private partners. Finally, this state-level position should staff a statewide security committee and participate as requested in local court security committee meetings to ensure consistent application of statewide security policies and court rules.

Recommendation #2: Standardize Threat and Incident Reporting, Assessment and Management

State supreme courts or state judicial councils should require state-level reporting of threats and security incidents. A recent internal survey of state court administrators revealed that more than half of states mandate reporting of incidents for general jurisdiction courts (59%) and limited jurisdiction courts (61%), but only 50% of the states require the same reporting for appellate courts.

Reporting of Security Threat or Incident

Formal, written protocols that outline the process for reporting, evaluating, and responding to threats and incidents are imperative. Judicial officers and court staff at all levels should be encouraged to report security incidents, as well as threats and inappropriate communications. An incident reporting system should be sufficiently robust for data to be collected and analyzed but not so detailed that reporting becomes time-consuming or so structured that incidents that do not fit the allowable options cannot be reported accurately.

Key components of an incident reporting system include:

- Structured data fields with standard responses necessary for data analysis
- The ability to attach documents and photos

- An open text box to add narrative
- The ability to identify related incidents
- The ability to re-open an incident to add information about follow-up steps and ultimate disposition

Additionally, including data fields that identify the target's job title, race, gender, and other demographic information will allow courts to identify patterns in who is being targeted and whether that correlates to a wider animus toward certain groups of people. Courts have not generally collected demographic or personal information about the target of threats or inappropriate communications, but there is anecdotal evidence that the frequency and type of inappropriate communication increases for female judicial officers, judicial officers of color, and judicial officers who identify as LGBTQ+ or a non-conforming gender identity.[26] While a recent survey of judicial officers revealed that both genders were equally likely to receive communications that included an explicit or implicit threat of harm, more female (75%) than male (62%) judicial officers reported receiving inappropriate communications.[27] A survey of state court judges published in 2025 revealed that there is also a significant difference between male and female judges as to whether their most serious safety concerns were taken seriously by law enforcement.[28]

Threat Assessment

Consistency in reporting can be challenging because judicial officers have individual perceptions as to what constitutes a threat or concern. Courts must educate judicial officers, staff, and administrators as to the importance of reporting all concerning incidents and interactions, including communications, social media posts, or other publications no matter

---

26 Comments from Washington State Court Administrator Dawn Rubio. Apr. 17, 2025.

27 McDermott, Christine M., et al. *Perceptions and Experiences with Judicial Security Threats: A Survey of U.S. State Court Judges*. Court Review. The Journal of the American Judges Association. Vol. 60, no. 3, 2024, pp. 102–11. The authors define "inappropriate communication" as "any written, verbal or behavioral contact that conveys a threatening, harassing, or unsettling message." McDermott et al., p. 105.

28 McDermott et al., pp. 106–07.

how "trivial" they may appear. A security incident that rises to the level of criminal conduct will usually come to the attention of court administration; however, an off-color post about a judicial officer on a social media platform may not. While these two scenarios will not be handled in the same manner, appropriately tracking them will assist the court in evaluating the security landscape in their jurisdiction.

Developing standard definitions for reporting and providing security training for judicial officers and court staff would go a long way toward leveling out this uneven landscape. National standards that define differing levels of security incidents should be developed. Any standards should include levels and details, such as:

- Level One – Security Incident:
  - » An assault or physical act perpetrated upon a judicial officer, court staff member, attorney, juror, litigant, court user, or member of the public while on court property.
  - » Physical damage to a court facility.
  - » Activities undertaken to disrupt the administration of justice or threaten the safety of a courthouse and its occupants.
  - » Note: These activities do not have to rise to the level of criminal activity to be reported.
- Level Two – Direct Threat:
  - » Direct threats made regarding the perpetration of harm against a judicial officer or court staff member (including their family members) by virtue of their role in the administration of justice.
  - » These threats can be made via any form of written or spoken communication and need not be received by the judicial officer or court staff member directly to be reported.
  - » These types of incidents do not necessarily have to include specific language. For example, publishing a photograph of a judicial officer with their home address on a social media platform may be sufficiently threatening despite the lack of direct communication with the judicial officer.
- Level Three – Concerning Communications:
  - » While not directly threatening, these communications indicate that a member of the public has singled out a judicial officer, court staff member, or the court as a target for criticism, derision, or ridicule.

» Examples of these types of communications include nonsensical emails, social media posts, or other communications that deliberately identify a judicial officer in a non-threatening manner.[29]

A standard framework to identify security incidents and a national repository to store this data would help to inform court security policies for state courts. Aggregated, de-identified data on standard incident types could illuminate trends, highlight connections, and paint a much clearer picture of what judicial officers and court administrators believe to be true but cannot currently quantify on a national scale. Once standard security incident definitions are articulated, best practices for the collection of this data and recommended response protocols tailored to each threat level could follow.

Protocols Following Reporting of Security Threat or Incident

Courts should have a protocol in place that details who receives the initial report, how the information is shared, what follow-up actions are required, and which entities are responsible for each step. All incident reports should be submitted to the court security director, who is responsible for evaluating the nature and seriousness of the report. Additional analysis will provide valuable insight into types of threats, locations of incidents, number of individuals subjected to multiple incidents, commonalities among perpetrators, and frequency of law enforcement or prosecutor involvement in follow-up actions. For example, Pennsylvania uses software to assist in identifying incidents that carry an escalated level of risk and danger. This software is specifically developed for courts to analyze the reports it captures in its incident reporting system and to assess them within the context of a judicial setting.

While incident reporting is essential for courts to collect data on the types and frequency of threats or security incidents, it is equally important to ensure judges and court staff understand how these reports are used.

29 It should be noted that while there is nothing inherently concerning or wrong about this type of communication (indeed, this speech would likely be protected by the First Amendment), tracking these communications to monitor for potential escalation is a prudent component to judicial security protocol.

When a threat is assessed as potentially actionable, the security director should promptly share the information with appropriate law enforcement agencies and, depending on the nature of the threat, a state or regional fusion center. In situations where the threat is determined to be non-actionable — for example, vague or constitutionally protected speech without indicators of intent or capability — the court may still opt to monitor the individual's behavior, particularly their online activity, for any escalation or changes that could indicate increased risk.

Educating judges and court personnel as to what constitutes an actionable threat under legal and law enforcement thresholds is critical to setting realistic expectations. Law enforcement may not always intervene unless there is a clear articulation of intent, capability, and a specific target. Therefore, it is essential that the court's security director possess appropriate training and experience in behavioral threat assessment to make informed, credible evaluations.

Finally, follow-up communication with the judge or staff member who submitted the initial report is a vital part of the process. They should be informed of the status of the evaluation and any actions taken or limitations of the court's response and given the opportunity to express how much continued communication they desire. The discussion should also include recommendations to enhance personal security posture, often focusing on situational awareness and behavior-based safety measures. It is important to note that courts are not investigative bodies and should not attempt to conduct interviews with potential suspects or perform forensic analyses. Instead, any actionable information should be promptly referred to law enforcement for formal investigation.

After-Action Steps and Communication

An often-overlooked protocol following a serious incident or emergency event is the after-action review. This process collects the knowledge, thoughts, and actions taken by staff as soon after the incident as is reasonably possible. This review process can uncover such things as whether a previously identified vulnerability or a new vulnerability was exploited; the timeliness and methodology on how information was communicated before, during, and after the incident; and immediate reactions as to what should be done differently. While much of this work will need to be done at the local level, it is critical that protocols are established at the state level to improve security through consistent and effective incident and threat reporting systems.

Support the Countering Threats and Attacks on Our Judges Act

Courts should work with members of their congressional delegation to advocate for the passage of the Countering Threats and Attacks on Our Judges Act. Under this Act, the federal government would create a State Judicial Threat Intelligence Resource Center that would "provide technical assistance, training, and monitoring of threats for state and local judges and court personnel."[30]

Though incidents of violence against judges are widely publicized, what is often overlooked are the multitude of threats directed toward state judicial officers every day. The U.S. Marshals Service has documented that threats against federal judicial officers have more than doubled between 2020 and 2023.[31] Looking further, the data shows that between 2016 and 2021, threats against federal judges increased by almost 400%.[32] There is no national data on threats against state court judicial officers nor is there an aggregated set of state-level data available, either because individual states do not require it to be reported or it is not collected in a format that is easily analyzed or shared.

Despite this lack of data, there is a general perception that threats against state court judicial officers are increasing.[33] One state that has documented the increase is Illinois.[34] Another state is Texas, where the Texas Court Security Division has noted a 125% increase in threats between 2023 and 2024, and a 400% increase in threats since 2015.[35] Washington State documented a

---

30 *National Court Organization Backs Federal Legislation to Protect State Judges*. National Center for State Courts. July 23, 2025. **https://perma.cc/B3FW-BHP7**.

31 Whitehurst, Lindsay. *Threats to Federal Judges Have More than Doubled in 'Alarming' Spike, US Marshals Director Says.*

32 Whitaker, Bill. *Federal Judges Call for Increased Security After Threats Jump 400% and One Judge's Son is Killed*. 60 Minutes. May 30, 2021. **https://perma.cc/KQ3G-MEH2**.

33 *See generally* McDermott et al., 106–07.

34 Rogers, Phil. *Skyrocketing Threats Prompt Concern for Safety of Judges*. NBC 5 Chicago **https://www.nbcchicago.com/investigations/skyrocketing-threats-prompt-concern-for-safety-of-judges/2502149/**

35 Masumoto, Melia. *Threats to Judges Have Increased 125% this Past Year: How One Texas Lawmaker is Trying to Bring that Number Down*. KVUE. Sept. 5, 2024. **https://perma.cc/EMB3-P674**.

580% increase in threats between 2017 and 2024.[36] A national repository is needed to collect data on threats to state judicial officers. Even if a national framework is only aspirational at this juncture, courts should work toward this goal by collaborating to identify and define the types of incidents and information that should be reported and educating their constituencies as to the importance of doing so.

Recommendation #3: Promote Privacy Protection Laws

Courts should advocate for the passage of privacy protection laws for judicial officers, family members with whom they reside, and court staff. Thirty-five states have laws governing the protection of judicial officers' personal information. As of the writing of this paper, an additional four states have introduced bills to provide privacy protection for judicial officers. Courts are well aware that threats to judicial officers do not end when they resign or retire. Former judicial officers remain vulnerable after retirement. However, currently the privacy protection laws in only seventeen states explicitly include former judicial officers. Oklahoma is the only state to specifically cover active or retired tribal judges.[37] Whether a bill is pending or a statute has already been enacted, it should be reviewed to ensure that the protections extend beyond active judicial officers, it provides robust definitions of protected individuals and personal information, and it includes a remedy for violations.[38]

Judicial officers may own property outside of the state in which they reside. However, no state specifically extends privacy protections to non-resident judicial officers. Uniform privacy protections that cover any current or former judicial officer, without regard to where that service occurred, would ensure that the same protection judicial officers have in their state of residence follow them when they leave the state and after they leave the bench.

In addition to judicial officers, court staff also face threats to misuse their personal information. Often, litigants have far more interactions with court staff than they do with individual judges.

---

36 Data provided by Washington Courts Security Consultant.

37 **20 Okla. Stat. §§ 3011–19**.

38 The Rhode Island Judicial Security Act, enacted June 27, 2025, is a good example of these components. *See* Rhode Island Judicial Security Act. **H 5892**. (Rhode Island).

The staff become the de facto face of the court, and this makes them vulnerable to harassment and threats from litigants who may come to view individual court staff as covering up for corrupt judges, biased in favor of the other party, or personally invested in the outcome of a case.[39] Yet only a few states have provided for protection of personal data of court employees. Connecticut and Massachusetts are the only states whose privacy protection law includes all judicial branch employees.[40] Hawaii provides privacy protection for the administrative director and deputy administrative director of the courts.[41] Florida and Nevada provide coverage for the clerks of court and clerk of court staff.[42] North Dakota's law limits the same data privacy options afforded to judicial officers to juvenile court directors.[43]

Recommendation #4: Utilize Digital Monitoring and Information Removal Services

The digital world makes it easier than ever to find judicial officers outside of the physical world in which they work. As individuals move through the digital world, a digital picture of their activities, interests, and web searches is left behind. Data aggregator services collect this "digital exhaust" and combine it to create a comprehensive picture of where an individual lives and works, who their family members and close friends are, and how and where they are likely to spend their leisure time.[44] In creating the Judicial Security Task Force, the Louisiana Legislature recognized the growing concern with personal details about judicial officers being readily available online.[45]

---

39 For example, a March 2025 incident report from North Dakota includes a threat to "end" the court clerk because she "continues to file unlawful and untruthful documents," and states "watch out because no one is watching your back."

40 Conn. Gen. Stat. §1-217; Mass. Gen. L. 4 § 7; 66 § 10B.

41 **Act 187**. Relating to the Disclosure of Personal Information Associated with Certain Public Servants. 2024. (Hawaii.)

42 Fla. Stat. § 119.071; Nev. Rev. Stat. §§ 247.540, 250.140, 293.908, 481.091.

43 N.D.C.C. § 44-04-18.3.

44 The original FBI *Digital Exhaust Opt Out Guide*, published in 2019, is available in paperback through several booksellers or in electronic format online. *See*, *Digital Exhaust Opt Out Guide.* Federal Bureau of Investigation. 2019. **https://archive.org/details/fbi-digital-exhaust-guide**. Regional FBI offices may have more up-to-date and region-specific versions of this manual.

45 House Resolution No. 43. Louisiana. 2024. **https://perma.cc/FRT8-JKZE**.

Social media monitoring services scan publicly available postings on social media sites for mentions, tags, and keywords and alert the subscriber when they are found. The monitoring service may also serve as a negotiator between the poster and the subscriber. Social listening services scan sets of online data and analyze the information to understand the context of the posts and to identify patterns and trends. Commercial vendors may offer a mix of these services. Eleven states have contracts to provide online information removal for appellate judicial officers and ten states provide this same service to trial court judicial officers.

Scrubbing information from commercial sites tends to be relatively easy, although it needs to be done reiteratively.[46] A much more difficult task is to remove information from the public facing databases controlled by various governmental entities. Without the proper legal protections in place, it may prove impossible to remove or mask this data. Rhode Island's Judicial Security Act explicitly prohibits state, county, or municipal agencies from publicly posting or displaying protected personal information without the written permission of the protected individual, following receipt of appropriate notice that the information is protected.[47] Statutes in California, Maryland, Oklahoma, and Pennsylvania allow staff with the administrative office of the courts to request removal of information on behalf of individual judges. In Maryland, staff with the administrative office of the courts may initiate a civil action to enforce compliance.[48]

The quickest way to learn personal details about a judicial officer may still be the court's own website or social media accounts. Traditionally, courts have included information about spouses, children, and personal interests in judicial biographies. Editing these webpages to only include professional data will provide the public the information they need to know about a judicial officer's qualifications. For election or retention purposes, individual judicial officers may still choose to publish this information on a personal social media account or in an election guide but even if an individual judicial officer chooses to publish the information, it should not be readily

46 According to the Washington Courts Security Consultant, standard data removal services remove only 40% of online data. Human intervention, constant ongoing scans and addressing information on government sites is needed to adequately capture and remove data.

47 Rhode Island Judicial Security Act. **H 5892**. (Rhode Island).

48 Judge Andrew F. Wilkinson Judicial Security Act. SB 575. 2024. (Maryland.)

available through the court's official website or social media accounts.[49] If allowed, judicial officers should take care not to list their home addresses on contact information with the bar association to avoid making that being publicly available, and instead list their court address.

Recommendation #5: Conduct Home Security Assessments and Procure Funding for Monitoring

The need for judicial security does not end at the boundary of the court facility. Judicial officers must be made aware of the need for diligence in and around their homes. At a minimum, courts should include information about how to conduct a home security assessment in new judicial officer orientation classes. In 2008, the U.S. Marshals Service established the National Center for Judicial Security. Its services are primarily for federal courts, but they also provide consulting services to state and local courts, which may include training for court security officers and security assessments of court facilities and judicial officer residences.[50]

It is recommended that all judicial officers invest in home security monitoring equipment and services. Use of public funds to purchase equipment for judicial officers' private residences is likely not possible, but courts may be able to obtain funding to provide a stipend or reimbursement for monitoring services. Four states currently provide funding assistance for home security improvements for appellate judicial officers and two states provide assistance for trial court judicial officers. In addition to providing home security systems for judicial officers, one state also provides assistance to judicial branch employees whose homes have "an elevated risk of targeted violence."

Recommendation #6: Require Local Court Security Plans

A requirement for a local court security plan is often necessary to jumpstart discussions at the local level. When implementing this requirement, the court should consider establishing

---

49 For example, staff in the administrative office of the courts in Washington received a comment from a self-designated court watcher stating that they "looked for Justice ____'s information online, and gave up when it was not easily obtainable."

50 *National Center for Judicial Security*. U.S. Marshals Service. **https://www.usmarshals.gov/what-we-do/judicial-security/national-center-judicial-security**.

guidelines and standards, which can serve as the roadmap for local planning. The Arizona guide referenced in footnote 20 provides examples of the tools and resources that can be developed and provided to local court security committees.

States have used various mechanisms to establish this requirement:

- Indiana has a court rule requiring that all courts within a county work together to develop a single security plan that considers the needs of each facility and includes a continuity of operations plan.[51]
- South Dakota provides grants for security improvements but requires the county to show they have a court security plan in place and to obtain the approval of the presiding judge for the grant application.
- The Administrative Office of the Arkansas Courts administers a court security grant program that assists the circuit and district courts with implementation of local security and emergency preparedness plans.[52]
- The Judicial Council of California provides court security plan consultation, tools, and templates to assist trial courts in each of the state's fifty-eight counties in meeting rule of court requirements to have a court security plan in place.[53]
- The North Dakota Court System has adopted a security manual which includes a requirement that each court have a local court security committee and a local court security plan. A copy of the security plan, and, if available, drawings of the court facility, are kept on file with the office of the state court administrator so that there is remote access to them in case of a catastrophic event and outside aid or assistance is needed.
- Texas has a statute requiring all municipal and local administrative judges to establish a local court security committee and has established the Texas Judicial Branch Security Division to assist them.[54]

---

51 **Ind. Admin. R. 19**.

52 AR Code § 16-10-1006.

53 **Cal. R. of Court 10.172**.

54 *Court Security*. Texas Judicial Branch. **https://www.txcourts.gov/programs-services/court-security/**.

Recommendation #7: Ensure Confidentiality of Security and Emergency Plans

Courts should be diligent in ensuring that security plans, emergency preparedness and continuity of operations plans, and similar information collected or maintained by the court that could endanger public safety are not subject to open record requirements. Depending on the state, this may need to be done through statute or court rule.

- North Dakota has an exemption specified in Administrative Rule 41(c)(4)(A) that shields "all security plans, codes and other records that provide for the security of information, individuals, or property in the possession or custody of the courts against theft, tampering, improper use, illegal releases, trespass, or physical abuse or violence...."[55]
- The Indiana courts rely on a statutory exemption to shield "a record or part of a record, the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack." The statute includes an exemption for detailed drawings or specifications of structural elements; floor plans; and operating, utility, or security systems.[56]
- Oregon statute exempts court security plans, emergency preparedness plans, and business continuity operations plans from public disclosure.[57]
- Alaska's Administrative Rule 37.5(e)(2)(D) excludes from public access "documents or information that could compromise the safety of judges, court staff, jurors, or the public, or jeopardize the integrity of the court's facilities or property."[58]
- Washington's GR 31.1(c)(7) states, "A court or judicial agency may deny a records request if it determines that the request was made to harass or intimidate the court or

55 N.D. Sup. Ct. Admin. R. 41.

56 Ind. Code 5-14-3-4(b)(19).

57 ORS § 1.177(3).

58 Ak. R. of Admin. 37.5(e)(2)(D).

judicial agency or its employees; fulfilling the request would likely threaten the safety or security of judicial officers, staff, family members of judicial officers or staff, or any other person; or fulfilling the request may assist criminal activity."[59]

While all of the aforementioned security protocols are a piece of the puzzle, comprehensive and sustainable security improvements are unlikely to occur until the highest court in the state makes security improvement a priority and is willing to advocate for the necessary funding to support security initiatives which are essential in the ever-changing threat landscape.

II. Local Governance Responsibility

In many jurisdictions, local government is responsible for securing court facilities. While the executive branch of local government maintains the fiscal responsibility, the decisions on what level of court security to implement often fall to an independently elected sheriff. Security decisions within the purview of elected sheriffs may include controlling access to court buildings or certain areas of the building through screening or locks, the purchase and placement of interior and exterior cameras, monitoring or controlling parking areas, installing and testing duress alarms and interior warning systems, and hiring and training courtroom security officers. These security initiatives have ongoing costs associated with them and require close cooperation between the local government board or commission, local law enforcement, and local court to implement and successfully maintain. Limited jurisdiction courts funded through local government may be in a position to strongly influence the sheriff, the county or municipal board, and the county or city manager or auditor. On the other hand, providing for the security needs of a state court located within a building owned and maintained by local government may be viewed as an unfunded mandate and the court treated as a bad tenant rather than an equal partner. A best practice and the remedy for these potentially challenging dynamics is the maintenance of an active and knowledgeable local court security committee. Unfortunately, the lack of an effective court security committee that includes clear oversight and representation of key stakeholders is one of the most commonly missing components in

59 Wash. Gen. R. 31.1.

court security assessments conducted by the National Center for State Courts.[60] In addition to challenges around court security governance, there are three common factors that courts must recognize as major contributors to local inaction on security. Arizona has secured funding and staff to establish the Arizona Center for Judicial and Court Security and will begin training and certifying court security officers in 2026.

Lack of Funds – Reliable funding is imperative to maintain a robust security infrastructure. National events have spurred interest in and support of security initiatives over the years. For example, federal dollars flowed to state and local governments to harden security at court facilities following the 9/11 attacks. Likewise, many courts were able to obtain federal funds through the American Rescue Plan Act of 2021 (ARPA) to further enhance screening and similar security measures. These federal funding opportunities have been invaluable, but states and local governments must plan and provide for continuity of funding for security initiatives. The challenge on the local level is in the competing demands for services that frequently prevail over building improvements. Local government may operate under state laws that restrict the amount of revenue they can raise through taxation. Facilities may be located within a small tax base due to high concentrations of poverty or a sparsely populated area. Lack of funds can also include lack of personnel to screen entrances, patrol the facility, and provide courtroom security during proceedings.

A 2014 editorial in the *Des Moines Register* sums up the issues succinctly:

> *Iowa county officials are not necessarily opposed to better security in their courthouses, but like everything else, it comes down to money. It's easy to ban guns in public buildings, but it is not so easy to enforce a gun ban without the budget for security systems, metal detectors and guards on duty at courthouse entrances. County taxpayers bear the burden of these costs, yet county officials are reluctant to raise taxes.*
>
> *Security is not the only challenge Iowa counties face in providing for Iowa's courts. The state pays for the operation of the courts, including judicial officers' salaries and operating costs*

60 Comments from Nathan Hall, Principal Court Management Consultant with the National Center for State Courts. Apr. 17, 2025.

for clerk of court offices, but counties are responsible for court facilities.[61]

A thoughtful, deliberate and sustainable funding structure is imperative for providing the requisite security for state courts.

Architecture – Modern court facilities are constructed to separate the movement of judicial officers, the public, and in-custody criminal defendants. The architecture of the building may make this type of zoning impossible without extensive renovation or additions. Particularly with historic buildings, there may be public resistance to altering the architectural detail. If the building has been designated as an historic landmark, there may be restrictions on what can be done to improve security. Architecture is also an issue with smaller court facilities that were built before courthouse security was considered important. Many of these facilities simply lack the space to have screening and monitoring areas, restricted interior corridors, or secure stairwells and elevators. Although challenging, these architectural issues can be addressed through careful planning, building modifications, and the utilization of modern security tools.

Attitude – Perceptions and expectations around security can vary greatly, depending upon the community in which a court is located. In small communities, there may be a pervasive attitude that security is both unnecessary and pretentious based on a belief that everyone in the community is a known factor and therefore law enforcement will be able to anticipate and neutralize any pending threat. In areas where there has never been a serious security incident, deploying personnel or preventative measures on a routine basis may be seen as an unnecessary waste of money and resources. On the other hand, judicial officers and court staff may have become de-sensitized to potential danger due to the frequency of inappropriate communication and threats directed toward them. Communication and education around security issues is the best way to address these attitudinal challenges. With better understanding of best practices and the "why" behind security initiatives, attitudes towards security may improve.

Acknowledging the constraints imposed by funding, architecture, and attitudes will assist in opening discussions around security improvements. While improving security can be accomplished on an incremental basis, a full understanding of the challenges and clear

61 *The Register's Editorial: State Needs to Help Address Court Security*. Des Moines Register [Des Moines, Iowa], Apr. 21, 2014.

communication regarding all of these issues must be undertaken to formulate a multi-faceted security plan that will be understood and accepted by all stakeholders.

Recommendation #8: Conduct Interbranch Safety Planning

Court governance includes the delineation of security responsibilities in buildings jointly occupied by executive and judicial branches and is critical to maintaining the safety, operational integrity, and independence of both entities. Ambiguities in authority can lead to delays in decision-making, inconsistencies in security protocols, and potential risks to the public and employees. Establishing a comprehensive framework that respects the unique functions of each branch while fostering effective collaboration is vital for the security and functionality of these shared spaces.

The inclusion of the chief administrative judicial officer and court administrator as integral members of the building's emergency management team supports the judiciary's specific security needs and operational requirements. Judicial leadership's active participation facilitates planning and informed decision-making during emergencies, enabling mutually beneficial coordination with executive branch representatives and other relevant stakeholders.

It is equally essential to preserve the judiciary's authority to make decisions concerning security, operations, and personnel within judicial spaces. This autonomy supports the constitutional separation of powers and allows courts to address their unique operational priorities effectively. Judicial control over these decisions ensures that courtroom proceedings, judicial officer chambers, and other sensitive areas are maintained at the high-security standards required for the impartial administration of justice.

Interbranch collaboration can occur in courthouse security protocols without compromising the judiciary's independence. This includes joint planning for emergency protocols, regular communication to address potential security gaps, and tailored solutions for the judicial branch's distinct needs. By fostering a cooperative yet independent approach, shared facilities can operate securely while upholding the principles of governance.

Engaging in table top exercises is the quickest way to identify ambiguities in authority and gaps in communication. Twice a year, Hennepin County (Minnesota) engages presiding judges and county officials in table top exercises related to court-specific incidents and once a year, they engage county officials and senior court managers and supervisors in disaster recovery and

emergency preparedness.[62] Pennsylvania courts also engage in regular table top exercises to ensure communication channels remain open and all participants remain vigilant.[63]

Recommendation #9: Implement Court Security Training

While some courts hire and train courtroom security officers, in most courts, courtroom security is provided through local law enforcement. Regardless of the hiring authority, courts should ensure that security officers are well-trained. One widely used resource is the court-specific training available through the National Criminal Justice Training Center at Fox Valley Technical College in Wisconsin.[64] Training and certification for court security officers can also be obtained through the National Sheriffs' Association.[65] Arkansas requires all law enforcement to complete an eight-hour course on court security as part of the curriculum for the law enforcement academy.[66] Pennsylvania and Wisconsin periodically hold regional workshops and conferences specifically focused on judicial safety and courthouse security.

Understanding security risks and how to respond in an emergency is not just the responsibility of trained officers. A security incident is likely to occur outside the immediate presence of a security officer or after a security officer has been disabled. Yet, less than 50% of judicial officers who responded to a survey reported receiving more than one day of security training and more than 90% expressed support for a continuing education course on judicial security.[67] The importance of providing security training to all court staff should not be overlooked. This is particularly true for courts in rural locations or courts with very small caseloads that may not

---

62 Conversation with Fourth Judicial District Administrator Sara Gonsalves. Aug. 13, 2025.

63 Information provided by Andrea Tuominen, Pennsylvania State Court Administrator. Aug. 6, 2025.

64 *See* National Criminal Justice Training Center of Fox Valley Technical College. **https://ncjtc.fvtc.edu/**.

65 More information about products and services offered by the National Sheriffs' Association can be found on their website. *Court Security*. National Sheriffs' Association. **https://www.sheriffs.org/professional-development/court-security**.

66 *Commission on Law Enforcement Standards and Training*. Arkansas Department of Public Safety. **https://dps.arkansas.gov/law-enforcement/clest/arkansas-law-enforcement-standards-and-training-aleta/**.

67 McDermott et al., p. 109.

have any security personnel or screening stations in the courthouse. Clerk of court staff, juvenile court staff, and family court staff are on the front lines every day dealing with upset litigants and the family members of litigants and may be in the best position to identify concerning or escalating behaviors.

Training judicial officers and court staff on how to identify and respond to warning, concerning, or escalating behavior in individuals may make the difference between an averted threat and a tragic outcome. Maryland and South Dakota are two of the states that have provided Mental Health First Aid training to judicial officers, court staff and others. Arizona has built an online Mental Health Awareness training program for staff. South Carolina engages the state police to provide education and training for court staff.

Recommendation #10: Promulgate Security Policies

NCSC maintains a listserv available to current CCJ and COSCA members for queries related to state policies and protocols on safety and security issues. If they do not already exist, there are three primary policies that should form the foundation of a court's security framework. These are policies establishing the guidelines for use of force, use of restraints, and prohibited items.

Use of Force Policy

A Use of Force Policy sets expectations and guidelines for the acceptable use of physical contact or physical restraint that can be used to compel cooperation from an individual or restrain an individual from taking certain actions or attempting to flee. A robust policy will include definitions of the levels of force, guidelines for the levels of force that are acceptable under various circumstances, incident reporting requirements and after-action review procedures. A Use of Force Policy is essential if court security is directly employed by the judiciary. In all other arrangements, the court should work closely with the local sheriff or private vendor to craft a policy that reflects the court's expectations.

Use of Restraints Policy

The use of restraints on criminal defendants, juveniles, and respondents in mental health cases may implicate constitutional issues.[68] In crafting a Use of Restraints Policy, courts must consider the safety of the restrained individual, the risk of prejudice to the restrained individual if the restraints are visible to a jury, and the overall security of the court proceedings. A Use of Restraint Policy should set guidelines for each type of proceeding. Considerations for an exemption to the Policy should be listed and may include such things as whether the individual's past behavior in the courtroom includes disruptive or violent conduct, if the individual has a history of fleeing or attempting to flee, the nature of the charges and whether alternative security measures are sufficient to protect the safety of everyone in the courtroom. Courts are unlikely to have direct control over prisoner transport and custody. At the same time, courts have a responsibility to maintain order and safety during court proceedings. Close cooperation with law enforcement in crafting a Use of Restraints Policy provides an opportunity to explain when and why restraints cannot be used and ensure that the plan is acceptable to all entities responsible for security.

Prohibited Items Policy

Courts should have a policy identifying prohibited items in courthouses and specifying any exemptions.[69] It is a common policy to prohibit anyone from possessing a weapon on the premises of a court facility unless the weapon is used as evidence in a court case. The term "weapon" should be defined and may include firearms, knives, tools, and chemical agents such as pepper spray. It is helpful to look at the federal Transportation Security Agency (TSA) prohibited items list for guidance and possible alignment, which provides consistency for the public's expectations.[70] Typical carve outs to prohibited items policies include law enforcement officers, probation officers required to carry a firearm, private uniformed security guards

---

68 *See Deck v. Missouri*, 544 U.S. 622 (2005); *Youngblood v. Romero*, 457 U.S. 307, 324 (1982).

69 *See, e.g.*, **Ak. R. of Admin. 26.2**.

70 *See What Can I Bring?*, Transportation Security Administration, **https://www.tsa.gov/travel/security-screening/whatcanibring/all**.

who are under contract with the court and who are authorized to possess a weapon under the contract, and private security guards who are employed by a financial institution or security service who transport money or other valuables. It is important to specify these positions are authorized to carry a weapon when in the courthouse for their job but not when they are present on private business.

The policy should also address whether court employees may possess specific prohibited items. If the court allows judicial officers to carry firearms, there should be a policy outlining requirements. Some guidelines for consideration include requiring written authorization from the top administrator prior to bringing a firearm into the court, providing a certificate of successful completion of a specified handgun course and a concealed carry permit (if the state authorizes permits), specifying a handgun as opposed to a long arm and limiting to one handgun, and requiring the use of a court issued handgun safe if not wearing the firearm. The policy should specify who is to be informed of the judicial officer's approval to carry a firearm and require confidentiality of that authorization.

When local government controls court facilities, collaboration on drafting a Prohibited Items Policy is a key element in instituting a policy that will be supported and enforced. However, it is equally important to maintain the court's inherent right to control access to courts, particularly if a state law or local ordinance has authorized weapons in government buildings. South Dakota provides two examples of how the supreme court responded to such laws in order to maintain a secure environment for supreme court justices, trial court judges, and court users.[71,72]

III. Individual Responsibility

The foregoing sections address important initiatives that courts need to consider to improve system-wide security. Implementing all of the recommendations provided herein would

---

71 *SD Supreme Court Says Judges No Longer Have to Physically Preside in County Courthouse That Allows Guns*. Fargo Forum [Fargo, South Dakota], Jan. 14, 2021. **https://www.inforum.com/business/sd-supreme-court-says-judges-no-longer-have-to-physically-preside-in-county-courthouse-that-allows-guns#:~:text=The%20South%20Dakota%20Supreme%20court,courthouse%2C%20though%20not%20the%20courtroom**.

72 **S.D. Codified L. 22-14-24**; *See also* Mercer, Bob. *South Dakota's New Law on Concealed Pistols Doesn't Protect State Court Administrator's Office*. Keloland.com. Aug. 26, 2019. **https://perma.cc/TCA3-B8F7**.

create the ideal security environment, but the ideal is rarely possible. Individual responsibility for security and safety increases in proportion to the lack of formal security protocols and protections available in a given jurisdiction.

Recommendation #11: Educate and Advocate for Personal Responsibility

Individual judicial officers and court staff have a responsibility to advocate for courthouse security, to report threats, and to cooperate with security measures. They also have a responsibility to participate in security training and drills and to be proactive in protecting themselves and their family members by following best practices for judicial safety. In his Ph.D. dissertation, former Nevada Judge Charles Weller noted that, "as courthouses become more secure, individuals are more likely to attack judges outside of the courthouse in their community or at their homes."[73] Individual responsibility starts with adoption of the following frame of mind and best practices.

Recognize that Security is Neither a Luxury Nor a Pretension

National discussions around security may seem far-removed from local reality. Rural America constitutes 97% of the land area of the United States.[74] Many court facilities in the United States are located in small towns where there are limited routes to reach the facility and non-secure parking areas upon arrival.

In some communities with small populations, there is likely to be a single school system and a limited number of places of worship, restaurants, or adult activity leagues. Everyone in the area may know where the judicial officer lives, where their children go to school, where they worship, and what they do for recreation in their off-hours. The judicial officer, law enforcement, court staff, and the attorneys who appear before the court may have known each other long

73 Weller, Charles E. *Statutory Response to Court Security Concerns*. 2013. University of Nevada, Reno.

74 *Courts Need to Enhance Access to Justice in Rural America*. Conference of State Court Administrators. 2018. **https://perma.cc/2W29-BMHF**.

before their assigned roles brought them together in the courthouse. In these situations, it is not uncommon for judicial officers and administrators to shy away from pushing for security improvements. There is often an unspoken sense that asking for security implies that the request is ego-driven and that the judicial officer or court consider themselves to be "above" the others who work in the facility.[75] In addition, there may be a sense of fatality that says, "If it is going to happen, it will happen, so I am not going to worry about it." This attitude hinders attempts to engage with other county officials in creating safety and emergency plans and running practice drills.

Complacency is not the answer. Individuals who choose to use violence as a means of demonstrating anger or grievance with authority in general, or the judicial system in particular, look for soft targets and opportunity.[76] While a local court may not possess the means or the methods to introduce comprehensive security measures, there is no excuse to make an attack as easy as possible either.

Advocate For and Comply With Security Measures

It cannot be stressed enough that even the best security measures can be defeated by careless attitudes. Acts by a judicial officer, such as propping open secure doors, disabling duress alarms, refusing to allow court security officers to be present during proceedings, allowing attorneys and court staff to bypass security screening, or prohibiting safety drills during regular court hours, sends a strong message to local government officials that security is not valued. These attitudes also increase the likelihood of negative outcomes in the event of an actual security incident.

---

75 A North Dakota judge shared an experience she had when a sheriff's deputy with whom she had gone to high school was tasked with escorting her to her vehicle due to a credible threat against her. Using her first name, he asked, "_____, do I really need to walk you to your car?" To which she responded, "Yes, and you actually have to defend me if _____ tries to kill me."

76 *See* National Threat Assessment Center. *Mass Attacks in Public Spaces: 2016-2020*. U.S. Secret Service, Department of Homeland Security. 2023. **https://www.secretservice.gov/newsroom/reports/threat-assessments/mass-attacks-public-spaces/details-1**.

Report All Threats and Security Incidents

For long-term judicial officers and court staff, threats can become routine. After years of being threatened and having nothing happen, they start to believe that all threats are harmless. One consequence of complacency is that people stop reporting incidents. It is important to report all threats to law enforcement and to use an incident reporting system if it is available. This logs the incident; helps to identify if the threat is specific to a single judicial officer, staff member or location; and provides law enforcement the initial information necessary to assess the threat.

Protect Personal Information

Judicial officers and court staff should be proactive in protecting their personal information. This includes understanding privacy settings and configuring them properly, setting preferences to prevent websites from storing cookies, opting out of behavioral advertising services, and generally practicing good cyber hygiene. Individuals should also consider using a digital scrubbing service. These services monitor which companies are buying and selling consumer data, alert the user when their data has been collected or transferred, and facilitate the process to file a request to stop the company from using your data.

Ensure Proper Training

Promoting personal responsibility is a key component to enhancing security. Training judicial officers and staff in a variety of areas will help to mitigate risks and improve their personal security posture. The following listing identifies a number of trainings that can be made available to judicial officers and court staff, or which individuals may pursue independently.

- **Pathway to Violence**

  The Pathway to Violence framework was developed by Frederick Calhoun and Steven Weston in 2003[77] to explain the triggers and behaviors that lead to violence. The model moves from grievance through attack. An overview of the model is available through the

77 Calhoun, Frederick S. and Steven Weston. *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent*. Specialized Training Services. 2003.

Cybersecurity and Infrastructure Security Agency (CISA),[78] and more detailed training is available through the Violence Prevention Training organization.[79] Calhoun and Webster themselves offer suggestions for using the Pathway to Violence for managing threats.[80]

- **Situational Awareness – Courthouse and Adjacent Areas**

  Paying close attention to the details of your surroundings, or situational awareness as an all-the-time practice, should focus on courthouse interior spaces, including courtrooms, chambers, secure hallways, and public hallways. Extra attention should be paid when traversing through workspaces, customer service areas, public spaces, and shared stairways and elevators.

  Focus should continue when in courthouse exterior spaces, including the adjacent property and grounds. Transitional spaces between two secure areas are a common place for attacks to occur. Good habits include observing details when entering and exiting the parking garage or lot, approaching and exiting the courthouse, quickly entering or exiting vehicles and observing who is in the area. Judicial officers should pay special attention to the routes they drive or travel to work or home and vary those routes if possible.

- **Situational Awareness – Beyond the Courthouse**

  Situational awareness for judicial officers should extend beyond the courthouse. Assessing what is going on and paying close attention to details should be an everyday skill used outside of work – around home; when grocery shopping or dining out; and when attending public events such as concerts, fairs, sporting events, and judicial outreach events in the community.

---

78 *Pathway to Violence*. Cybersecurity & Infrastructure Security Agency. Feb. 24, 2023. **https://www.cisa.gov/resources-tools/resources/pathway-violence**.

79 *The Pathway to Violence*. Violence Prevention Training. **https://perma.cc/YZ5T-CA2A**.

80 Calhoun, Frederick S. and Stephen W. Weston. *Perspectives on Threat Management*. Journal of Threat Assessment and Management. Vol. 2, no. 3-4, 2015, pp. 258-267. https://www.apa.org/pubs/journals/features/tam-tam0000056.pdf.

- **Social Media Security**

  A judicial officer's personal social media accounts should only be shared with known and trusted contacts. Training on how to avoid compromising security when using social media should include discussions about whether settings are private. Sharing current location information of the judicial officer and family members and future travel plans, as well as photos of homes, should be avoided. Judicial officers and court staff should receive training on how to respond to inappropriate communications and how to report them.

- **Personal Vehicle and Public Transportation Security**

  The judicial officer's personal vehicle is vulnerable to being targeted if it has a personalized license plate or bumper stickers that announce the car belongs to a judicial officer. Training should instill practices like locking doors immediately after entering a vehicle and avoiding common habits like sitting in the car before leaving or after arriving or looking at a smartphone without being aware of who may be approaching the vehicle.

  Judicial officers who use public transportation are more likely to encounter litigants in an unexpected and casual setting. When using public transportation, remain alert to your surroundings and the other individuals who share the space. Basic security measures include avoiding overly crowded platforms and trains or buses and varying the time or routes used. Before entering any ride-share vehicle, use the driver photo and vehicle license number function of the ride-share application to confirm the correct vehicle and driver are present. If possible, use a nearby location rather than a home address as the pick-up or drop-off location.

- **Home Security**

  Judicial officers should develop a home security audit practice, which includes checking all exterior door locks and window locks when exiting or even when home. All judicial officers should consider installing security systems and evaluate their personal comfort level with the range of available options, such as hiring a security company to install and monitor the system or buying a readily available app-based system that is low cost that they can install themselves. Decisions will need to be made regarding the number and location of cameras and whether they have interactive audio components. Other options

may include installing window alarms or glass-break sensors or keeping dogs as an additional deterrent. Training should also help the judicial officer evaluate the exterior of the home in terms of landscaping, installing exterior lighting to deter someone from approaching the residence, avoiding rocks that can be used to break windows, and avoiding overgrown trees or shrubs that can provide a place for someone to conceal themselves.

Training for family members is also recommended, as is developing a family plan to respond to a security breach or credible threat.

- **Vacation Security**

  Training should extend to planning for when a judicial officer leaves home for a vacation or other travel. Preparation should include making sure the home is secured, that someone is checking on the property during the absence, and there is a plan to keep any pets safe. Finally, the security of the destination should be considered in advance. Judicial officers should be mindful of sharing their vacation plans publicly, on social media, in the courtroom, and at any public event or forum.

- **Training on Working with High-Conflict Individuals**

  Judicial officers and court staff who interface with the public should receive periodic training on how to interact effectively with high-conflict individuals. Due to the nature of judicial work, which involves people navigating serious disputes, such as family law, domestic violence, or criminal matters, it is expected that some members of the public and even some attorneys may exhibit challenging behaviors. This may include yelling, arguing, speaking disrespectfully, interrupting, or moving into someone's personal space. Also, some people visit courthouses because they are First Amendment auditors who assert it is their First Amendment right to film various areas and people, including staff. In addition, sovereign citizens can be disruptive because they claim they are not subject to the court's jurisdiction and may refuse to follow required procedures. These various situations can be frightening and intimidating, so it is important to train judicial officers and staff on how to specifically diffuse behaviors in each of these situations and keep it from escalating.

- **Disaster Response**

  Training on how to respond to emergency situations is important. Such trainings should include background science on how people behave physically and emotionally in high-stress events so judicial officers and staff know what to expect. Also, information should be provided about the three stages of disaster response (denial, deliberation, and decisive moment). Attention should be paid to what to do: avoid, deny, and defend. Trainings should discuss the difference between the need to shelter-in-place and when lockdown is appropriate. Finally, the training should explore the role of the judicial officer, with the primary objective of removing the judicial officer from the situation if possible, instead of seeking involvement.

  It is important to understand that many people misunderstand the role of active shooter training in a courthouse environment. Some judicial officers and court staff want to participate in an in-person training simulation as if there was an active shooter attempting to shoot one or more people, using firearms shooting blanks and a chaotic environment with people running around with some severely injured needing medical attention. Such simulations are only appropriate for trainings specifically for a law enforcement response to an active shooter situation, not for civilian trainings for court staff and judicial officers. This is not appropriate and not advised for court staff and judicial officers because the training can cause trauma, overemphasize the actual danger in the workplace, and cannot be practiced with enough frequency to develop an automatic response to such a situation. Instead of an in-person simulated active shooter drill, court staff and judicial officers should receive video-based training on how to react to a shooter based on run, hide, fight responses mentioned above.

From architecture to incident reporting to appropriate training and everything in between, it is clear that court security is a complex issue that cannot be solved by fiat or unilateral actions at any level. Understanding where the responsibility for each piece lies is the first step in initiating productive discussions and lasting changes.

Checklist

The security of judicial officers and court personnel is a matter that deserves continuous attention. Because every court will be at a different stage, COSCA recommends the following checklist for courts to assess and monitor their progress:

- ☐ Create and support staff positions with responsibility to monitor and respond to safety issues.
- ☐ Standardize threat and incident reporting, assessment, and management.
- ☐ Promote privacy protection laws.
- ☐ Utilize digital monitoring and information removal services.
- ☐ Conduct home security assessments and procure funding for monitoring.
- ☐ Require local court security plans.
- ☐ Ensure confidentiality of security and emergency plans.
- ☐ Conduct interbranch safety planning.
- ☐ Provide court security training on a regular basis.
- ☐ Promulgate security policies.
- ☐ Educate and advocate for personal responsibility and provide appropriate trainings to facilitate proficiency and comfort in addressing various situations.


COSCA
Conference of State Court Administrators