

National Association of Women Judges Annual Conference – **BOSTON 2025: *Balancing the Scales: Judicial Security in an*** ***Evolving Landscape***

Links and Resources:

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>

U.S. Federal Courts | *Project 365 Videos and Training: Security Tips and Guidance* | <https://rise.articulate.com/share/GxbqHeCov1mkTqKLr37h5fyNdDyN5W21#/>

New York Times Opinion Guest Essay | *A Federal Judge Says: Knock Off the Threats* | Feb 27, 2025 | <https://www.nytimes.com/2025/02/27/opinion/judges-threats.html>

Court Review Vol. 60 | *Perceptions and Experiences with Judicial Security Threats: A Survey of U.S. State Court Judges* | PDF file found on pg. 2

State of New Hampshire Judicial Branch | *Request for Proposals RFP NHJB-2024-02 for Security Risk and Vulnerability Assessment of NH Judicial Branch Facilities* | Oct 8, 2024 | PDF file found on pg. 12

National Center for State Courts | *Home Security Audit and Recommendations* | PDF file found on pg. 35

CounterBalance | *The Dire State of Judicial Security* | PDF file found on pg. 44

The Edward Davis Company | *Presentation on Judicial Security* | PDF file found on pg. 48

Perceptions and Experiences with Judicial Security Threats:

A Survey of U.S. State Court Judges

Christine M. McDermott, Evan Murphy, Patrick Grimes & John Muffler

Although there are many recent examples of violence toward judges and their families, such as the highly publicized 2024 attack on Clark County District Court Judge Mary Kay Holthus,¹ the 2020 murder of the son of New Jersey District Court Judge Esther Salas at her home² reinvigorated a focus on judicial security. In response to this tragedy, a bipartisan bill named after Judge Salas's son, the Daniel Anderl Judicial Security and Privacy Act, was passed to protect federal judges and their families' personally identifiable information (PII) from being published, displayed, or sold.³ Despite lawmakers' efforts, many state judges' personal identifying information is still easily accessible online today.⁴

Judicial security differs for federal and state judges. Federal judges are protected uniformly by the U.S. Marshals Service (USMS), and all reported threats go through the USMS Judicial Security Division.⁵ This centralized repository shows that inappropriate communications, threats, and physical attacks on federal judges increased 344% over six years, with 926 incidents in 2015⁶ and 4,511 in 2021.⁷ On the other hand, state judges are protected on a fragmented basis, including court security and local law enforcement, and the reporting procedures vary by state. For example, roughly half of state judges are not required to report threats to a central repository.⁸ Additional challenges for state judges stem from the lack of a universal vocabulary; for example, some judges might interpret "court security threats" to mean only threats or incidents in the courtroom.⁹

Protections for state judges, when they exist, vary significantly. Several states criminalized assaults on judicial officers (e.g., Ari-

zona¹⁰) or judges (e.g., New York¹¹). Others increased the severity of such an act; for example, Virginia raised assault on a judicial officer from a Class 1 misdemeanor to a Class 6 felony,¹² and Washington made an assault "in a courtroom, jury room, judge's chamber, or any waiting area or corridor immediately adjacent to a courtroom, jury room, or judge's chamber" a third-degree assault.¹³ Other states focused on different aspects of judicial privacy (e.g., New Jersey,¹⁴ Hawaii,¹⁵ Illinois,¹⁶ Nevada,¹⁷ and Texas¹⁸) by allowing judges to seek relief when personal information is maliciously posted or to make certain identifying information (e.g., home address, phone number) private. Surprisingly, the mechanism for making identifying information private also differs between states.¹⁹ For example, in New Jersey, a judge simply needs to register on a website,²⁰ whereas Nevada judges need a court order.²¹

As there is no national repository for state court judges of inappropriate communications, threats, and physical attacks,²² and very little research on state judge judicial security exists,²³ self-report research from a national sample of judges can potentially provide the best opportunity to understand the scope of state judicial security concerns and determine if state judges mirror the pattern of increased threats found among federal judges. A better understanding of state judges' perceived and real security threats may result in allocating resources and education to help judges protect themselves and their families and encourage states to enact legislation consistent with federal statutes for judicial security.

Footnotes

1. Ken Riller & Rio Yamat, *Defendant Faces New Charges After Attacking a Nevada Judge in Court, Which Was Caught on Video*, ASSOCIATED PRESS, Jan. 4, 2024, <https://apnews.com/article/judge-attacked-las-vegas-court-video-8f1c9a98ae128fe80506351d17f6c01>.
2. Esther Salas, *My Son Was Killed Because I'm a Federal Judge*, N.Y. TIMES, Dec. 8, 2020, <https://www.nytimes.com/2020/12/08/opinion/esther-salas-murder-federal-judges.html>.
3. Press Release, Congress Passes the Daniel Anderl Judicial Security and Privacy Act, UNITED STATES COURTS (Dec. 16, 2022), <https://www.uscourts.gov/news/2022/12/16/congress-passes-daniel-anderl-judicial-security-and-privacy-act>.
4. FACILITIES AND SECURITY—ANNUAL REPORT 2021, UNITED STATES COURTS, <https://www.uscourts.gov/statistics-reports/facilities-and-security-annual-report-2021>.
5. *Id.*
6. *Id.*
7. FACILITIES AND SECURITY—ANNUAL REPORT 2022, UNITED STATES COURTS, <https://www.uscourts.gov/statistics-reports/facilities-and-security-annual-report-2022>.
8. William E. Raftery, *Want to Know the Number of Court Security Inci-*

dents? We Do, Too, Trending Topics series, NATIONAL CENTER FOR STATE COURTS, Sept. 29, 2021, <https://cdm16501.contentdm.oclc.org/digital/collection/facilities/id/269>

9. *Id.*
10. A.R.S. § 13-1204, 2015.
11. Assembly Bill A409D (2011).
12. Va. Code § 18.2-57(A), (C)(2006).
13. SB 5484—2013-14, 2013.
14. P.L. 2021, c. 371.
15. H.B. 1539, 2022.
16. 705 ILCS 90, 2012.
17. NRS 247.540, 250.140, 293.908, 481.091.
18. S.B. 42 2017.
19. Ron Zayas, *Securing the Integrity of Our Judicial System*, 59 CT. REV. 16-22 (2023).
20. P.L. 2021, c. 371.
21. NRS 247.540, 250.140, 293.908, 481.091.
22. *Id.*
23. Raftery, *supra* note 8; JUDICIAL SECURITY REPORT: 2014, NATIONAL JUDICIAL COLLEGE, www.judges.org/wp-content/uploads/2019/12/USMS_survey_report.pdf; Zayas, *supra* note 19.

THE PRESENT STUDY

The present study surveyed state court judges from across the United States to understand their security concerns, planning and preparation, past experiences with security threats, and judicial security needs. This study also measured potential differences in judicial perceptions due to actual security concerns they have experienced (i.e., having received an inappropriate communication, threat, or attack), security behaviors enacted (e.g., locking doors, carrying a gun for protection, limiting online information), and their gender. The results of this study provide a foundational understanding of judges' past experiences with judicial security concerns and discuss judges' desires for further judicial security training and resources.

RESEARCH QUESTIONS

To what extent are judges worried about security concerns toward themselves and their families?

To what extent are judges educated, trained, and prepared to handle judicial security concerns?

To what extent have judges experienced security concerns?

To what extent do judges perceive the need for a judicial security center dedicated to state court judges?

Do any of the above vary by the judge's gender, past security concerns, and number of safety precautions taken?

MATERIALS AND METHODS

PARTICIPANTS

Participants were recruited using the National Judicial College's (NJC) course enrollment database. The NJC is a premier judicial education organization that educates thousands of judges annually from all 50 U.S. states. Judges who attended a continuing education course or webinar at the NJC between 2017-2021 were eligible for selection. To better understand the experiences of female-identifying judges, who are underrepresented in the judiciary,²⁴ we stratified the sample by gender so half of the sample was male and half was female. With these considerations, a stratified random sample of 2,000 judges was selected and invited to take our survey.

Participants were 398 judges (20% response rate) from 48 U.S. states. Further details about participants' demographic and career characteristics are listed in Table 1.

PROCEDURE

Participants selected for our survey were notified through email one week before receiving it. After a week, participants received a survey link to our online Qualtrics survey. Participants who still needed to complete the survey were given three weekly reminders. Data collection was completed after four weeks.

SURVEY

Survey participants completed a four-part survey reporting (1) their perceptions of security concerns, (2) their security planning and preparation, (3) their experiences with security concerns, and (4) their judicial security needs. Section one of the survey asked

judges about their safety concerns for themselves and their family, their perceptions of specific security risks, and where they feel most vulnerable to security threats. Section two of the survey asked judges about their previous training on issues of judicial security, their use of common security measures, and whether they have ever carried a gun for their protection since becoming a judge. Section three of the survey asked judges about inappropriate communications (defined as any contact, whether written, verbal, or behavioral, that conveys a threatening, harassing, or unsettling message), threats (defined as inappropriate communications that express, explicitly or implicitly, the intent or desire to cause harm, or the belief that harm will be done), and physical attacks that they have experienced since becoming a judge. We also asked judges whether they reported these threatening experiences and to what extent they felt their concerns were taken seriously. Section four asked judges about the need for a national judicial security center and the benefits of continuing judicial education. Judges also suggested ideas for additional resources that would be helpful for judges to address their security concerns.

TABLE 1
JUDGES' DEMOGRAPHIC AND CAREER CHARACTERISTICS

CHARACTERISTIC	FULL SAMPLE (N = 399)	
	n	%
Gender		
Female	206	54.2
Male	174	45.8
Race		
American Indian/Alaskan Native	17	4.5
Asian/Asian American	15	3.9
Black/African American	34	8.9
Hispanic/Latinx	28	7.4
White	290	76.3
Other	15	3.9
Judicial Selection		
Appointed	213	55.2
Elected	173	44.8
Type of Judge		
Administrative Law Judge	43	11.1
Appellate Judge	15	3.9
Family Law Judge	32	8.3
Federal Judge	3	0.8
General Jurisdiction Judge	199	51.4
Military Judge	2	0.5
Special (Limited) Jurisdiction Judge	55	14.2
Tribal Court Judge	17	4.4
Other	21	5.4
Note: Judges were an average of 57 years old ($SD = 8.47$) and had an average of 10.5 ($SD = 7.34$) years on the bench.		

24. 2022 US State Court Women Judges, National Association of Women Judges <https://www.nawj.org/statistics/2022-us-state-court-women-judges>.

RESULTS

PERCEPTIONS OF SECURITY THREATS

Judges largely agreed that they worry about their safety, their families' safety, and internet safety (see Table 2).²⁵ Responses were measured on a scale of 1 (Strongly Disagree) to 7 (Strongly Agree). These worries were related to behaviors such as increased worry about personal safety, a belief that the profession was becoming more dangerous, increased worry about family safety, a feeling of being threatened because of a legal decision,

TABLE 2 JUDGES' AGREEMENT WITH SAFETY CONCERNS			
STATEMENT	% ALL JUDGES IN AGREEMENT ^a	% FEMALE JUDGES IN AGREEMENT	% MALE JUDGES IN AGREEMENT
I worry about my safety because of my position as a judge.	82.7	84.4+	80.5+
It is becoming more dangerous to be a judge.	78.6	82.0+	75.1+
I worry about the safety of my family because of my position as a judge.	74.1	71.9	76.9
I have felt threatened because of a decision I made in a case.	78.7	70.9+	60.4+
I worry about the availability of personally identifiable information (e.g., home address) about myself and my family online.	90.2	90.7	90.2
I feel that my courthouse building is safe.	68.1	64.6	71.3
I would have security concerns if I had to oversee an election law case. ^b	40.4	40.5	40.8
Note: * = male and female judges significantly different from one another, + = male and female judges marginally different from one another. ^a This includes judges who did not disclose gender or identified outside the male/female binary, and therefore this column will not be a perfect mean of male and female judges. ^b Please note that these data were collected before the recent spate of security concerns surrounding highly publicized election law concerns; we anticipate research conducted today would yield different results.			

25. This article discusses our main findings, for all comparisons see Appendix A.

26. Regression analysis demonstrated all statements in Table 2 were associated with judges taking extra precautions (e.g., locking doors and windows, installing/using security systems, varying routes to work; $ps < .05$) except for "I feel my courthouse building is safe."

27. $M_{\text{Carried Gun}} = 4.50$, $SD = 1.90$ vs. $M_{\text{No Gun}} = 4.97$, $SD = 1.77$,

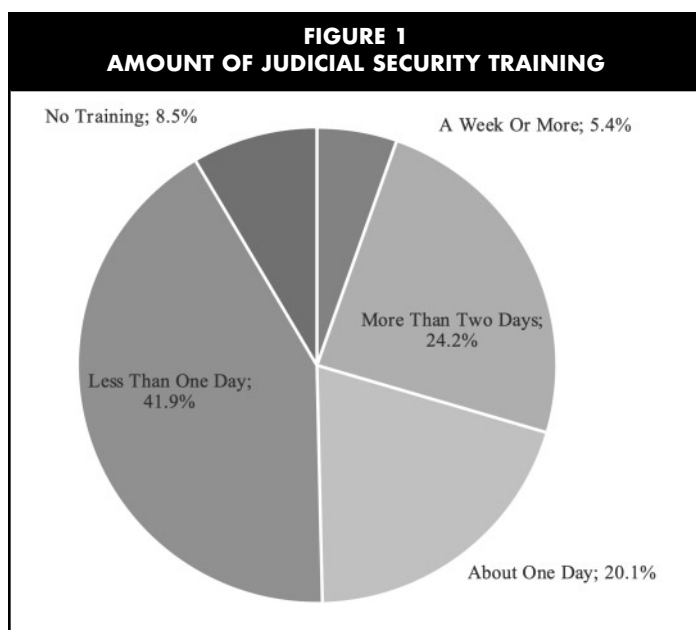
increased worry about online PII, and increased worry about security concerns in election law cases. All these behaviors were associated with enacting more routine safety measures (see Table 2),²⁶ Although perceptions of courthouse safety were unrelated to the number of safety measures used, judges who had carried a gun for protection felt significantly less safe in their courthouses than judges who had not.²⁷

Gender appears to be associated with some of the judges' perceptions. Female judges were significantly more likely to have felt threatened than male judges (see Table 2).²⁸ Additionally, although the difference was not statistically significant, female judges appear to be somewhat more concerned than male judges about their safety²⁹ and perceive that it is becoming more dangerous to be a judge.³⁰ Gender did not affect concern for family safety, concern about the availability of personally identifying information online, perceived courthouse safety, or perceived election law safety.³¹

SECURITY TRAINING AND PLANNING

The next section of the survey asked judges to report their judicial security training, planning, and preparation. We first asked judges how much training they have received on judicial security. Judges reported a wide range of security training, with just over half of all judges surveyed (50.4%) reported having less than one day of training on judicial security (see Figure 1). Experiencing security training as a judge was related to safety behaviors.³² Judges with a week or more of security training enacted an average of 1.22-1.60 more safety behaviors (out of 11 possible behaviors) than judges with less security training (see Figure 2).

Judges were asked to select which judicial security measures



$t(226.20) = 2.37$, $p = .009$.

28. $F(1, 379) = 4.25$, $p = .04$.

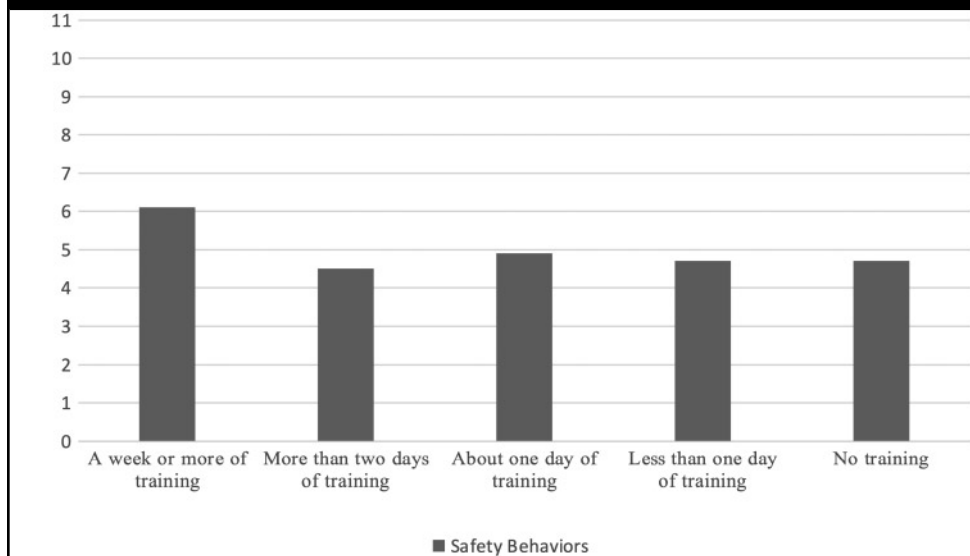
29. $F(1, 378) = 2.68$, $p = .10$.

30. $F(1, 378) = 2.79$, $p = .096$.

31. All MANOVA results with p values greater than .10.

32. $F(4, 381) = 2.78$, $p = .027$, $\eta^2 = .029$.

FIGURE 2
NUMBER OF SAFETY BEHAVIORS ENACTED BY
AMOUNT OF JUDICIAL SECURITY TRAINING



they employ from a list of common security measures suggested by judicial security experts³³. Safety behaviors taken were added to create a safety-measures score ranging from 0 (no safety behaviors reported) to 11 (all safety behaviors reported); judges averaged five safety behaviors. Most judges reported locking their doors and windows at home (90.8%), limiting their personal info online (77.6%), and using a home security system (57.5%). Less common security measures were removing identifying information from cars (42.2%), illuminating sight lines around the home (41.2%), varying travel routes to work (38.2%), using home surveillance (34.9%), carrying a gun for protection (31.6%), receiving personal mail at the courthouse (16.5%), using a safe room (4.8%), and “other” (22.1%). Of judges who selected “other,” approximately one-quarter mentioned dogs.

We asked judges if they had ever carried a gun for protection since they became a judge. Nearly one-third of judges (31.6%) reported carrying a gun for their protection. Judges who had received an inappropriate communication were more likely than those who had not to report carrying a gun for protection at some point while serving as a judge (see Figure 4).³⁴ Judges who reported they had received a threat as a judge were also more likely than those who had not to report carrying a gun for protection at some point while serving as a judge.³⁵ Additionally, male judges were more likely than female judges to report

carrying a gun for protection at some point while being a judge.³⁶

EXPERIENCED SECURITY CONCERNS

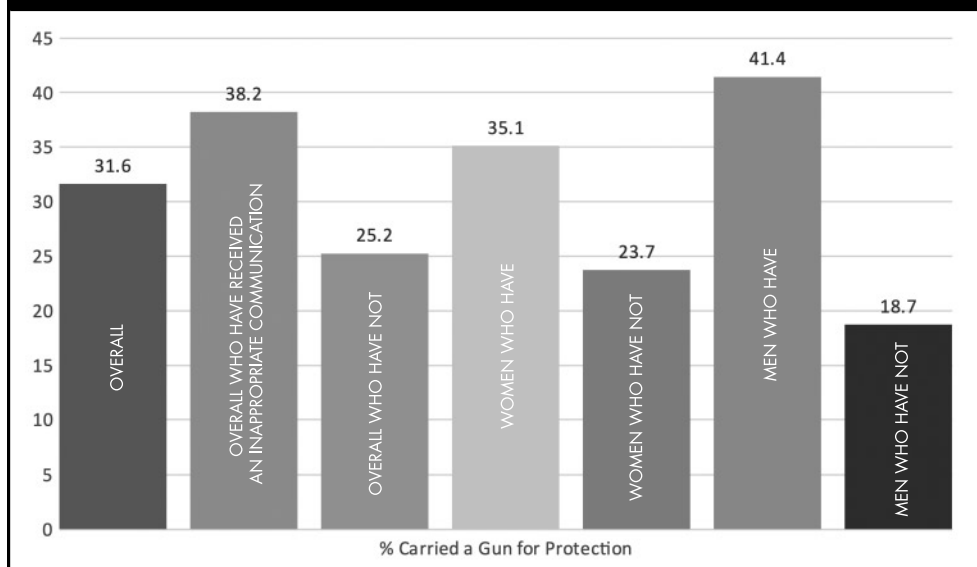
The third section of the survey measured judges’ experiences with security concerns. More specifically, we wanted to know to what extent judges had experienced inappropriate communications, threats, and physical attacks because of their position as a judge. We asked about judges’ experiences reporting their judicial security concerns and to what extent they felt their concerns were taken seriously. We also asked judges to describe a significant judicial security concern they have experienced through an open-ended question.

We first asked judges if they had ever received an inappropriate communication.

An inappropriate communication is any written, verbal, or behavioral contact that conveys a threatening, harassing, or unsettling message. Over two-thirds of judges reported that they have received an inappropriate communication while being a judge, with female judges experiencing a greater chance of receiving an inappropriate communication than their male peers (see Figure 4).³⁷ Female judges (75%) were significantly more likely than male judges (62%) to experience an inappropriate communication. Receiving an inappropriate communication was associated with taking more safety measures.³⁸

We next asked judges about their experiences with judicial

FIGURE 3
EFFECTS OF GENDER AND RECEIVING AN INAPPROPRIATE COMMUNICATION OR
THREAT ON CARRYING A GUN FOR PROTECTION



33. Henry E. Hudson & John Muffler, *A Few Tips for a More Security-Conscious Lifestyle*, JUDGES’ J., Summer 2014, at 24-27.

34. $X^2(1, N = 394) = 4.97, p = .026$.

35. $X^2(1, N = 391) = 22.89, p < 0.01$.

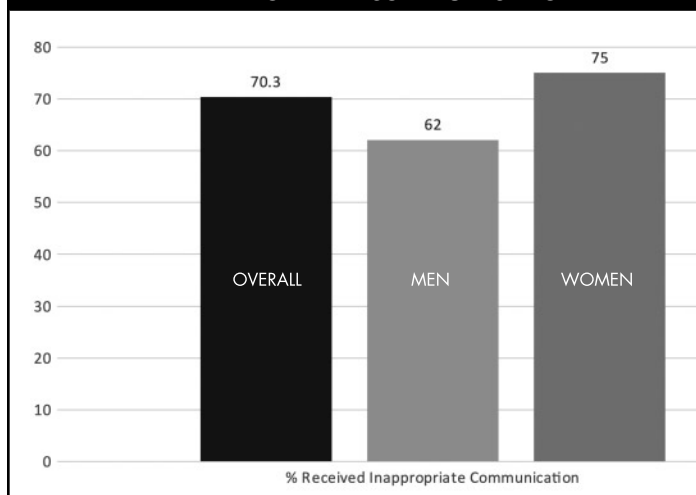
36. $X^2(1, N = 379) = 7.31, p = .007$.

37. $X^2(1, N = 379) = 7.27, p < .01$.

38. $R^2 = .03, F(1, 368) = 13.37, p < .001$.

39. $R^2 = .01, F(1, 368) = 14.40, p < .001$.

FIGURE 4
EFFECTS OF GENDER AND RECEIVING
AN INAPPROPRIATE COMMUNICATION

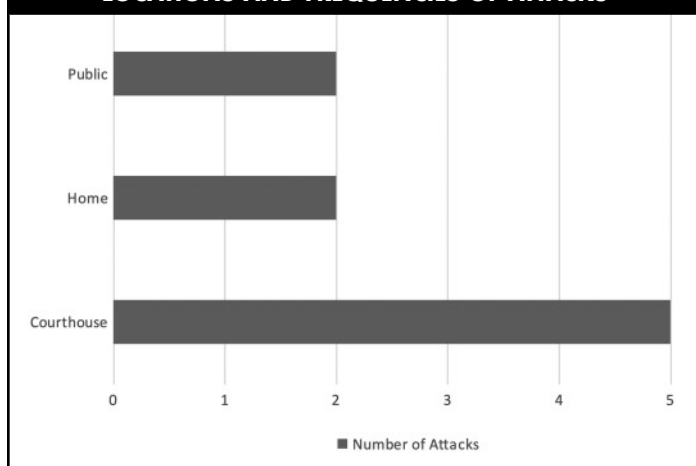


security threats. A *threat* is defined as inappropriate communications that express, explicitly or implicitly, the intent or desire to cause harm, or the belief that harm will be done. Most judges reported that they had been threatened while being a judge (56.1%). Male and female judges were equally likely to receive threats. Receiving a threat was associated with taking more safety measures.³⁹

In addition to inappropriate communications and threats, we asked judges whether they have ever been physically attacked because of their position as a judge. Eight judges (2%) reported a previous physical attack, one judge was attacked twice. One judge reported being attacked in two different locations (see Figure 5).

Judges who had reported a previous concerning security experience—when compared to judges without those experiences—were significantly more worried about their safety as a judge, agreed more that it is becoming more dangerous to be a judge, were more worried about their family's safety because of their job as a judge, were more likely to have felt threatened, and were

FIGURE 5
LOCATIONS AND FREQUENCIES OF ATTACKS



40. All MANOVAs were significant, $ps < .001$.

TABLE 3
LEVEL OF CONCERN BY PREVIOUS CONCERNING
SECURITY EXPERIENCE

STATEMENT	JUDGES WITH PREVIOUS CONCERNING SECURITY EXPERIENCES	JUDGES WITHOUT PREVIOUS CONCERNING SECURITY EXPERIENCES
	% AGREED	% AGREED
I worry about my safety because of my position as a judge.***	86.6	73.1
It is becoming more dangerous to be a judge.***	83.3	65.5
I worry about the safety of my family because of my position as a judge.***	79.3	61.7
I have felt threatened because of a decision I made in a case.***	77.6	33.5
I worry about the availability of personally identifiable information (e.g., home address) about myself and my family online.***	94.3	81.3
I feel that my courthouse building is safe.	67	70.1
I would have security concerns if I had to oversee an election law case.	42.3	37.3

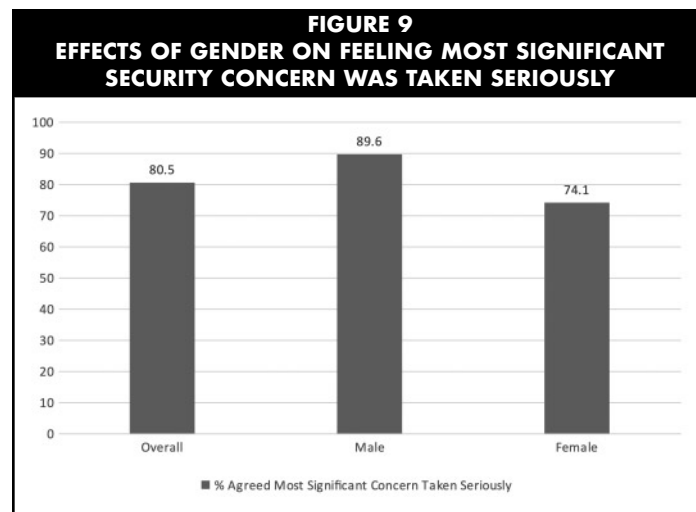
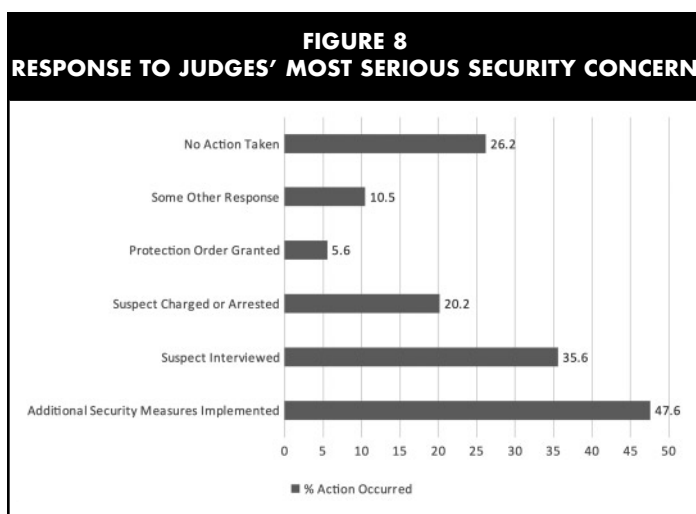
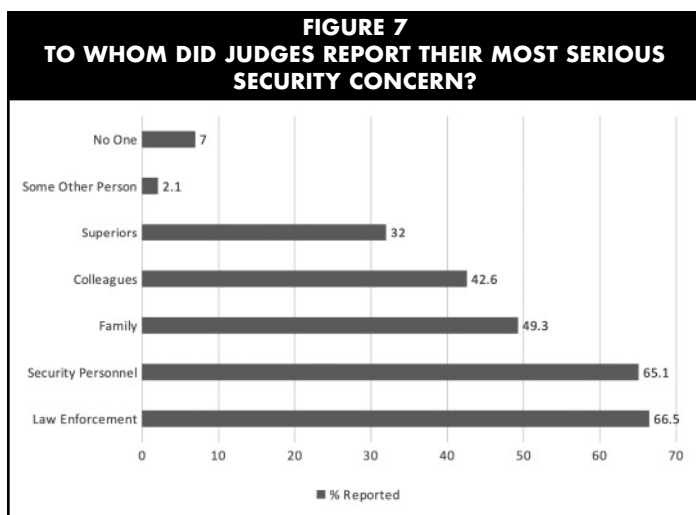
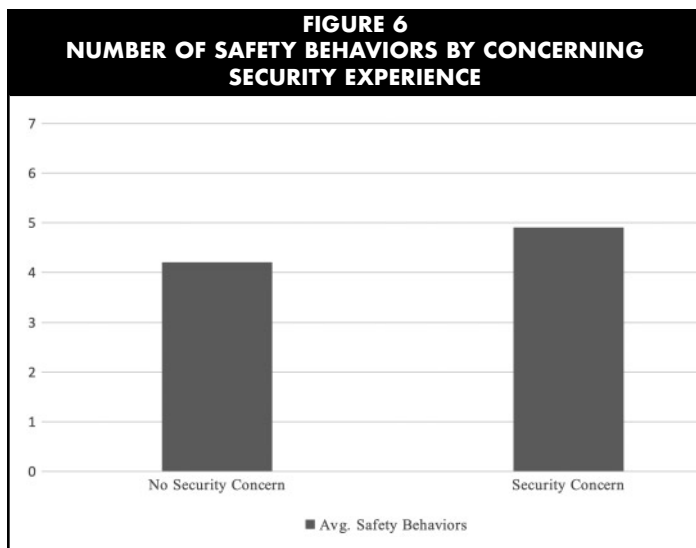
Note: Statements marked with *** are significant at the $p < .001$ level.

more worried about identifying information online.⁴⁰ Judges who had a previous concerning security experience felt as unsafe in their courthouses and overseeing an election law case as judges who had not (see Table 3).⁴¹ Additionally, judges with a previous concerning security experience engaged in more safety behaviors than those without the experience (see Figure 6).

Among judges who reported a concerning security experience, we asked to whom they reported their security concerns (see Figure 7), what the response was, and to what extent they felt their security concerns were taken seriously. For those who reported their most serious security concern, we asked judges what the response was after reporting their most serious security concern (see Figure 8).

In addition to asking whom judges reported their security concerns to, we also asked judges to indicate the extent to which

41. MANOVAs were not statistically significant, $ps > .10$.



they agree, on a 7-point Likert scale where 1 equaled *strongly disagree* and 7 equaled *strongly agree*, that their concerns for their most significant security concern were taken seriously. Most judges agreed to some extent that their concerns were taken seriously. However, this perception differed by judges' gender, with male judges significantly more likely than female judges to feel that their security concerns were taken seriously when reporting their most significant security threat (see Figure 9).⁴²

Finally, we asked judges to describe a significant judicial security concern they have experienced. We received 227 open-ended responses describing various concerning judicial security experiences ranging from inappropriate communications to physical attacks. A coding scheme was developed based on themes present through the judges' responses. Three primary themes of inappropriate communications, threats, and physical attacks emerged (see Table 4). Judges provided over 100 examples of explicit threats toward them and their families. In these examples, judges described people approaching them at their homes and in public, as well as posting about them online on social media. Most threats described intentions to commit violence at the courthouse or judges' homes. Finally, several judges described their experiences of being physically attacked. Most of these attacks happened in the courtroom, where defendants scaled the bench or threw objects at the judge (e.g., a chair). However, some judges described violent attacks in their homes (see Table 4 for an example). Other judges described damage to their property, such as having tires slashed, their car's gas tank filled with a foreign substance, and bombs delivered to the courthouse. Sadly, many judges reported an inadequate response to their concerning security experiences.

JUDICIAL SECURITY NEEDS

The fourth and final section of the survey measured judicial security needs. More specifically, we asked judges a series of questions about the need for a national judicial security center for state judges, the benefits of continuing judicial education, and ideas for additional resources that would be helpful for judges to address their security concerns.

Judges were asked three questions about the need for a

42. $t(251) = 3.46, p < .001$.

43. $F(1, 385) = 18.02, p < .001$.

TABLE 4
JUDGES' EXPERIENCED SECURITY THREATS

THEME	EXAMPLE QUOTES
Inappropriate Communications	"A litigant came to my home and attempted to discuss his case. I contacted the police and recused from his case. Police did nothing or if they did the litigant was not arrested and the police never followed up with me." "An inappropriate communication was made via social media from a litigant about me, which included my children. I reported it to law enforcement. They took the report very seriously and investigated the matter thoroughly."
Threats	"I was threatened by a defendant that I had previously sentenced. He called my clerk more than once and said he was coming to kill me and blow up the courthouse. When they finally found who it was and picked him up, he tried to convince law enforcement to help him kill me. It went to trial, he was convicted, and the sentencing judge basically gave him time served. I was very disappointed in the sentence. This case is a major reason I am retiring from the bench." "I received a letter at work threatening to rape and kill my family and me. I gave the letter to law enforcement. I received no follow up." "A confidential informant told law enforcement that a neighbor was going to enter my house with night vision goggles and shoot me and my family. He was eventually arrested and charged with firearms violations and sent to prison. I spent about 2 weeks sleeping with a shotgun watching the entrance before arrest occurred."
Physical Attacks	"A person attacked self and family at our home. Tried to slit my wife's throat, daughter-tried to stab her in chest. I was struck over head, with object causing substantial head injury." "I had a defendant (half-shackled to a wheelchair sitting directly next to me in court) throw feces at me. He was removed, the trial went forward in his absence, and I did not initiate contempt proceedings because he was mentally ill—he was found competent by another judge subsequently. The security personnel—no subsequent action. The department of corrections officer wrestled him down, or else he would have reached me physically. He was within 3 feet of me."

national judicial security center serving state court judges. Judges indicated the extent to which they agreed that it would be beneficial to have a security center that provides educational programs on judicial security; to hold symposiums on major, recent security incidents; and to create and maintain a judicial threat database (see Figure 10). Judges who reported a previously concerning security experience were significantly more supportive of all aspects of the national judicial security center for state court judges than those who had not.⁴³ Support for the judicial security center in all three dimensions was also associated with

increased numbers of security measures taken.⁴⁴

Finally, we asked judges, "Would continuing judicial education on judicial security be beneficial for judges?" Judges responded affirmatively to the benefits of continuing judicial education on judicial security, with those who reported a previously concerning security experience significantly more likely than those who had not to endorse continuing judicial education on judicial security.⁴⁵ Increased belief that continuing judicial education on judicial security would be beneficial was associated with increased numbers of security measures taken.⁴⁶

DISCUSSION

Recent and high-profile cases of judicial attacks, such as the murder of U.S. District Judge Esther Salas's son and the attempted murder of her husband by a disgruntled lawyer,⁴⁷ highlight some of the dangers judges can face. Records of security threats to federal judges indicate that security incidents and threats are an increasing problem.⁴⁸ As there are no reporting standards for state judges, the extent of security problems faced by state judges is currently unknown. This study examined if judges perceive security concerns, if they experience security threats, what steps they take to protect themselves, and what security resources they desire. Individual factors, such as gender, experienced security concerns, and number of security behaviors enacted were also examined for their impact on judicial perceptions of security. The data supports both the notion that state judges are threatened and the need for legislative and funding-related improvements for judicial security.

PERCEPTIONS OF SECURITY CONCERNS

Judges in our survey largely indicated that they had security concerns, with most judges worrying about their safety (82.7%) and the safety of their families (74.1%). Judges who had previously received an inappropriate communication or threat, those who reported engaging in more security behaviors, and women were more concerned about safety than their counterparts. More than 90% of judges surveyed also indicated that PII poses a security threat. As high-profile cases such as the attack on Judge Esther Salas's family have been facilitated by being able to find judges' home addresses online, and judges in our sample reported many concerning security experiences, this nearly unanimous concern seems well-founded. This concern was particularly high among judges with a previous concerning security experience and those who reported engaging in more safety behaviors.

When asked about safety in their courtrooms, more than three in ten judges (31.9%) indicated they did not feel safe in their courthouses or office buildings. Judges who had never received an inappropriate communication or threat felt safer than those who had. Taken together, judges reported substantial concern for their safety and the safety of those around them, though factors can serve to heighten this concern.

44. $R^2 = .03$, $F(1, 379) = 12.68$, $p < .001$.

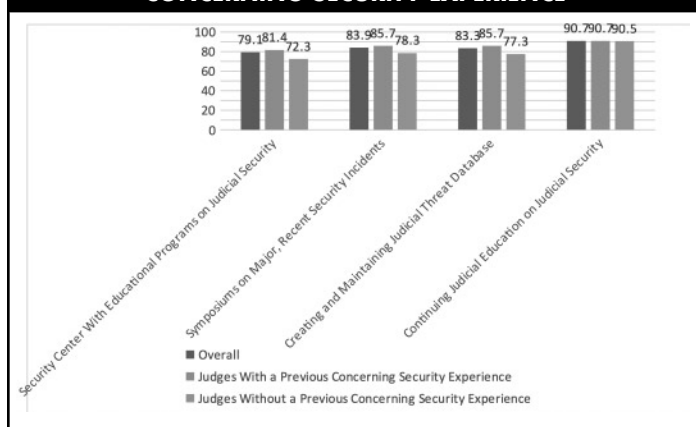
45. $F(1, 384) = 5.40$, $p = .021$.

46. $R^2 = .05$, $F(1, 379) = 21.51$, $p < .001$.

47. Salas, *supra* note 2.

48. FACILITIES AND SECURITY, *supra* note 7.

FIGURE 10
AGREEMENT WITH SECURITY REMEDIES BY PREVIOUS CONCERNING SECURITY EXPERIENCE



SECURITY TRAINING AND PLANNING

When asked about any security training offered, more than half of judges reported receiving less than one day since becoming a judge, with most getting security training as a continuing education credit. A week of security training increased the number of safety behaviors judges reported enacting compared to less or no training. Regardless of training, the most common security measures included locking doors and windows, limiting personal information online, and using a home security system. Nearly one-third of judges (31%) reported carrying a gun for protection, with male judges and those with a previous security concern having an increased likelihood of carrying a gun. This statistic indicates an increase from a previous internal survey, which found that 26% of judges carry a gun.⁴⁹ Additionally, a study using a representative sample of U.S. adults suggests that approximately 17% of U.S. adults have carried a gun for protection at least some of the time.⁵⁰ This finding suggests heightened security concerns for judges compared to both the general public and a previous cohort of judges that should be explored further in future research.

EXPERIENCED SECURITY THREATS

Most judges (70.3%) reported receiving an inappropriate communication, conveyed through letters, verbal, or technological means (e.g., social media, email, text). These inappropriate communications were mainly received at the courthouse, though a substantial percentage were received online, in public, and at home. Being female was associated with a higher risk of receiving an inappropriate communication.

More than half of judges (56.1%) reported receiving a threat. Threats were largely verbal, but were also in written form (e.g., letters, social media, email, and text). Most threats were received at the courthouse, but some were online, in public, at home, in transit, or in some other place. A small subset of judges reported being physically attacked (and one judge indicated multiple physical attacks). Attacks mainly occurred in the courthouse, but attacks at home and in public were also reported.

The overwhelming majority (though not all) of judges reported their most significant security concern largely to law enforcement, or security personnel, or both but often also to family, colleagues, and supervisors. In cases in which judges' most serious security concerns were reported, about half involved additional security measures adopted, more than a third involved the suspect interviewed, one in five judges involved the subject being arrested, and on rare occasions, a protective order was put in place. Judges also reported that no subsequent actions were taken in more than a quarter of the cases. Judges largely felt that their most serious security concern was taken seriously, but this was more common for male judges than female judges. Future research should further investigate judges' experiences reporting threats and explore why female judges' concerns are taken less seriously (or perceived as being taken less seriously).

JUDICIAL SECURITY NEEDS

Judges were very supportive of enhanced training and security measures. Over 90% of judges felt a continuing education course on judicial security would be helpful. Nearly 80% of judges support a judicial security center that would provide programming and educational materials for state court judges. More than 80% of judges support the same security center providing a centralized database of security threats and incidents to replicate what federal judges already have. Judges were similarly enthusiastic about an annual symposium on judicial security, including case studies of incidents arising each year. Judges with concerning security experiences were most supportive of the proposed symposium. When asked which measures they would like to enact, judges mentioned education and training for themselves and their staff (including court security), money to improve security equipment in courts (e.g., metal detectors, panic buttons, increased security personnel), and legislation and training to remove personally identifying information from the internet.

Overall, our study indicates that security is a concern for all judges but is felt most keenly by judges who have had prior concerning incidents. Female judges appear somewhat more concerned about their safety and feel that their security concerns are taken somewhat less seriously than male judges.

LIMITATIONS AND FUTURE DIRECTIONS

This research is a first step in studying judicial security issues at the state court level. As with all studies, there are limitations. First, although a stratified random sample of judges was taken from the National Judicial College's database of more than 20,000 judges, this database does not represent all U.S. judges. Additionally, with a response rate of roughly 20%, it is possible that judges who were more concerned about security were more motivated to complete the survey. Future research should try to increase response rates and sample sizes, perhaps by partnering with judicial organizations at the state level. Furthermore, states might consider their own research to learn about judicial security considerations specific to their own state.

The current sample was also predominantly White and served

49. *Our Survey: 1 in 4 Judges Carries a Gun*, National Judicial College, Sept. 21, 2017, <https://www.judges.org/news-and-info/1-in-4/>.

50. Kim Parker, *America's Complex Relationship with Guns*, Pew Research

Center, June 22, 2017, <https://www.pewresearch.org/social-trends/2017/06/22/americas-complex-relationship-with-guns/>.

as a general jurisdiction judge. Future research should perhaps stratify by identity backgrounds (i.e., race, ethnicity) and different types of dockets (e.g., family-court judges) who may disproportionately be impacted by security threats, as these subpopulations were too limited in the present sample to draw any meaningful conclusions.

A final limitation stems from the inherent self-report nature of a survey. Self-reporting requires the respondent to remember and report behaviors accurately; incidents that were embarrassing, minor, or that occurred in the distant past are less memorable or desirable to report. Establishing a judicial security center or other centralized repository for data on threats and other incidents involving state judges would allow for a greater understanding of the dangers for state court judges, including the relative frequency of threats.

CONCLUSION

The present study is among the first to examine perceptions of security and experiences of security threats among state court judges. Most judges indicated they were concerned about their safety and the safety of their family and were especially concerned about the availability of personally identifying information online. These sentiments likely stem, at least in part, from experience, as most judges indicated that they had experienced at least one inappropriate communication or threat.

Judges who reported carrying a gun for protection were more worried about their safety and the safety of others than judges who did not. Nearly one in three judges reported ever carrying a gun for protection while serving, indicating serious security concerns. Judges with a previous security concern perceived greater danger than those without this experience. Furthermore, gender effects indicate that female judges perceive somewhat greater danger than male judges, which could be rooted in reality—female judges were more likely to receive an inappropriate communication than male judges (though both genders were equally likely to receive a threat). Additionally, when reporting a serious security concern, judges generally felt their concern was taken seriously, but female judges felt less heard than male judges.

Judges want to improve judicial security. Judges indicated they would appreciate security training for themselves and their staff; a judicial security center that would provide both security education and a centralized repository of threats and incidents to equalize that which is available to federal judges; funds to upgrade security measures in their courthouses; legislation passed that would allow them to remove their personally identifying information from the internet; and assistance removing their and their family's personally identifying information from the internet once it is possible for them to do so. The data suggest that judges who experienced a security concern were more likely to increase their security measures. One of the patterns that seems to exist from the data is that judges are more likely to take security precautions seriously as the threats against them occur. This pattern of not prioritizing judicial security until it is already a problem appears to exist among state legislatures as well. While it was not a specific topic we explored, the authors note that existing laws and regulations are often created in reaction to horrific crimes against judges. By shifting to a proactive rather than reactive approach to legislating judicial security, perhaps future tragedies can be prevented.

Judges are entrusted with upholding the rule of law. They are meant to do their duties divorced from their views, beliefs, or potential consequences—a task made much more difficult if their safety and their family's safety are legitimately compromised because of their position. As U.S. Circuit Judge Richard J. Sullivan stated, “The safety of judges and their families is essential—not just to the individuals involved, but to our democracy. Our system of justice depends on judges who are free to carry out their Constitutional duties without fear of reprisal or violence.”



Christine McDermott, Ph.D., is a graduate of the University of Nevada, Reno's Interdisciplinary Social Psychology Ph.D. Program. She is a researcher at the National Judicial College. Her work explores legal and judicial decision-making across a wide spectrum of topics.



Evan Murphy, Ph.D., is a graduate of the University of Nevada, Reno's Interdisciplinary Social Psychology Ph.D. Program and a former researcher at the National Judicial College. He now oversees research and evaluation efforts of reentry, and other workforce development programs, as a Senior Evaluation Specialist in the U.S. Department of Labor's Chief Evaluation Office.



Patrick Grimes is the Chief Financial Officer at the National Judicial College. He is involved in research related to judicial education. His personal interests relate to understanding and measuring outcomes related to specific training programs.



John F. Muffler, MS, CTM, Principal of Aequitas Global Security, LLC, is a strategic consultant for judicial officers, public figures, and victims of domestic violence on anti-assassination strategies and the assessment and management of situations that might pose a hazard to their safety or well-being. He serves as adjunct faculty for the National Judicial College, the National Council of Juvenile and Family Court Judges, Florida Judiciary's College of Advanced Judicial Studies, committee member for the American Bar Association's Judicial Division, faculty/consultant for the National Center for State Courts, and is a Strategic Advisor for Gavin de Becker & Associates. He is a retired United States Marshals Service Chief Inspector that led the National Center for Judicial Security.

APPENDIX A: PATERN OF RESULTS BETWEEN GROUPS

		RECEIVED INAPPROPRIATE COMMUNICATION	RECEIVED THREAT	# SECURITY PRECAUTIONS TAKEN	APPOINTED VS. ELECTED	GENDER	RACE	AREA OF PRACTICE
PERCEPTIONS OF SAFETY THREATS	Worry About Own Safety	Significant	Significant	Significant	Non-Significant	Marginal	Non-Significant	Non-Significant
	Feel Being a Judge is Becoming More Dangerous	Significant	Significant	Significant	Non-Significant	Significant	Non-Significant	Non-Significant
	Worry About Family Safety	Significant	Significant	Significant	Non-Significant	Non-Significant	Non-Significant	Significant
	Worry about PII online	Significant	Significant	Significant	Significant	Non-Significant	Non-Significant	Non-Significant
	Feel Their Court Is Safe	Non-Significant	Significant	Non-Significant	Significant	Marginal	Non-Significant	Non-Significant
	Threatened by Decision	Non-Significant	Significant	Significant	Non-Significant	Significant	Non-Significant	Non-Significant
SAFETY BEHAVIORS	Reported Carrying a Gun for Protection	Significant	Significant	N/A	Significant	Significant	Non-Significant	Significant
	Experiencing Security Training	Non-Significant	Non-Significant	Significant	Non-Significant	Non-Significant	Non-Significant	Non-Significant
SECURITY THREATS	Received Inappropriate Communication	N/A	Non-Significant	Significant	Non-Significant	Significant	Non-Significant	Significant
	Received Threat	Non-Significant	N/A	Significant	Non-Significant	Non-Significant	Non-Significant	Significant
	Felt Their Most Serious Safety Concern Was Taken Seriously	Non-Significant	Non-Significant	N/A	Non-Significant	Significant	Non-Significant	Non-Significant
SECURITY NEEDS	Support a Judicial Security Center with Educational Programming	Significant	Significant	Significant	Non-Significant	Non-Significant	Non-Significant	Significant
	Support a Security Symposium	Significant	Significant	Significant	Non-Significant	Non-Significant	Non-Significant	Non-Significant
	Support a Judicial Security with a Database of Threats	Significant	Significant	Significant	Non-Significant	Non-Significant	Significant	Non-Significant
	Support Continuing Judicial Education on Security	Significant	Significant	Significant	Non-Significant	Marginal	Significant	Non-Significant

Note: Appointed vs. elected compares appointed and elected judges. Gender compares male and female judges. Race compares White to Non-White judges. Received inappropriate communication and received threat compares judges who have received such communication to those who had not. Area of practice compared administrative law judges to all other types of judges.



State of New Hampshire Judicial Branch

REQUEST FOR PROPOSALS RFP NHJB-2024-02

FOR

**SECURITY RISK AND VULNERABILITY ASSESSMENT OF NH
JUDICIAL BRANCH FACILITIES**

October 8, 2024

TABLE OF CONTENT

SECTION I. OVERVIEW AND SCHEDULE.....	4
A. Introduction	4
C. Purpose and Background	4
D. Contract Term	5
SECTION II. SCOPE OF SERVICES TO BE PROVIDED	6
A. Scope of Work.....	6
SECTION III. RFP PROCESS.....	10
A. Agency Point of Contact/Restriction of Contact with Agency Employees.....	10
B. Vendor Inquiries.....	10
C. RFP Addendum	10
D. Property of the NHJB.....	11
E. Confidentiality of a Proposal.....	11
F. Public Disclosure.....	11
G. Ethical Requirements	12
H. Non-Commitment	12
I. Compliance	12
J. Proposal Cost	12
SECTION IV. PROPOSAL SUBMISSION REQUIREMENTS	13
A. Proposal Submission, Deadline, and Location Instructions	13
B. Validity of Proposal	13
C. Proposal Format	13
SECTION V. EVALUATION OF PROPOSALS	15
A. Criteria for Evaluation and Scoring	15
B. Oral Interviews and Product Demonstrations.....	15
C. Cost Proposal Scoring.....	15
D. Negotiations and Selection.....	16

NEW HAMPSHIRE JUDICIAL BRANCH

RFP NHJB-2024-02

Security Risk and Vulnerability Assessment of NH Judicial Branch Facilities

SECTION VI. CONTRACT DOCUMENT	17
--	-----------

SECTION I. OVERVIEW AND SCHEDULE

A. Introduction

This request for proposals (RFP) is issued by the New Hampshire Judicial Branch (NHJB) through the Administrative Office of the Courts (hereinafter jointly referred to as AOC) to solicit proposals for a contractor-supplied physical security risk and vulnerability assessment of NH Judicial Branch facilities.

B. Schedule

The following table provides a Schedule of Events for this RFP through contract finalization and Notice to Proceed. NHJB reserves the right to amend this Schedule at its sole discretion and at any time through a published Addendum.

EVENT	DATE	LOCAL TIME
RFP Released to Vendors (Advertisement)	October 8, 2024	
Vendor Inquiry Period Ends	October 21, 2024	11:59 PM
Final NHJB Responses to Vendor Inquiries	October 24, 2024	11:59 PM
Vendors Submit Proposals	November 12, 2024	11:59 PM
Estimated Notification of Selection and Begin Contract Development	November 29, 2024	

C. Purpose and Background

The New Hampshire Judicial Branch (NHJB) is a constitutionally separate but co-equal branch of government within the State of New Hampshire. NHJB's mission is:

[t]o preserve the rule of law and protect the rights and liberties guaranteed by the United States and New Hampshire Constitutions, the courts will provide accessible, prompt, and efficient forums for the fair and independent administration of justice, with respect for the dignity of all we serve.

NHJB consists of the Supreme Court, Superior Court, Circuit Court, and the Administrative Office of the Courts. Within the Administrative Office of the Courts is the Court Security Department. The Department is responsible for providing safety and security for judges and non-judicial employees throughout court facilities. The Bureau of Court Facilities, a bureau in the Executive Branch Department of Administrative Services, is responsible for providing the court facilities.

For this project, the Administrative Office of the Courts is seeking a vendor to conduct both a physical security risk assessment and a broader vulnerabilities assessment at each of the court facilities located in 39 different locations throughout the State of New Hampshire. The full list of locations is in Appendix E.

Information regarding the NHJB can be found on the NHJB website at <https://www.courts.nh.gov/>.

D. Contract Term

The resulting contract shall be a Firm Fixed Price/Not To Exceed contract. The contract term shall commence on the effective date of the contract as defined herein and run through December 31, 2025 subject to continued availability of funding. Following the initial term of the contract, the AOC may opt to renew the contract for the additional 6-month period, through June 30, 2026, at the sole option of the AOC, subject to continued availability of funding and satisfactory performance.

The AOC anticipates awarding one contract resulting from this RFP process.

SECTION II. SCOPE OF SERVICES TO BE PROVIDED

A. Scope of Work

The successful vendor will deliver the following objectives and tasks:

1. Project Objectives

- a. Identify and assess the overall security risks and vulnerabilities to include determining Facility Security Level (FSL) associated with each facility listed in Appendix E attached to this RFP;
- b. Recommend options to mitigate and remediate each of the identified risks and vulnerabilities;
- c. Produce a Security Risk Assessment and Vulnerability Assessment Report;
- d. Produce schematic design(s) for recommended physical improvements to building and surrounding site area facility; and
- e. Provide a security plan and an emergency operation plan for each facility.

2. Task 1 – Facility Security Level (FSL) Assessment

- a. The contractor shall conduct a FSL Assessment on each of the 39 facilities listed in Appendix E. The FSL Assessment will correspond to a level of risk that relates directly to a Level of Protection (LOP) and associated set of baseline security measures. The integration of the Physical Security Criteria (PSC) is predicted on an FSL designation.
- b. The FSL is based on the analysis of security-related facility factors listed below, which then serve as the basis for the implementation of certain protective measures specified in the Facility Security Management Process.
 - i. Mission Criticality
 - ii. Symbolism
 - iii. Facility Population
 - iv. Facility Size
 - v. Threats to Facilities

3. Task 2 – Security Risk and Vulnerability Assessments and Recommendations

- a. The contractor shall:
 - i. Provide a thorough review and evaluation of all aspects of the physical security features of the listed facilities to identify risks.
 - ii. Provide FSL assessments in accordance with the Facility Security Management Process, which shall (1) identify security related threats from internal and external sources during and after operating hours, (2) identify critical assets, (3) identify security scenarios on which to base the security program, (4)

- analyze vulnerabilities, (5) assess impacts of threat scenarios, (6) identify actions that mitigate risk, and (7) provide an analysis of mitigation actions using a risk matrix scoring approach with risk scores that consider likelihood and severity of impacts.
- iii. Review listed facilities security systems, as well as court and security operational policies and procedures that impact safety and security and provide recommendations. Recommendations shall include, any physical changes, equipment recommendations, upgrades, associated estimates, and any recommended changes to policies and procedures. Recommendations shall be aligned with all building and fire codes and security best practices.
 - iv. Cyber-terrorism threats are not included in the scope of this RFP. IT, computer, and communication systems will only be reviewed to the extent as they interconnect with physical access: cyber-physical convergence vulnerabilities.
 - v. Produce and deliver written Security Risk Assessment and Security Vulnerability Assessment Reports for each of the 39 facilities identified in Appendix E. The reports shall detail findings and present a summary of recommended solutions to address identified risks and vulnerabilities. The reports shall include:
 - A. Identification of multiple solutions for identified risks and/or vulnerabilities.
 - B. A cost estimate for implementation of all recommended solutions.
 - C. A prioritized implementation plan and timeline for all recommendations.
 - D. Identification and documentation of any federal funding opportunities that may be available to assist with implementation of recommendations.
 - vi. The Physical Security Risk Assessment Report shall be presented in the following format:
 - A. Site Information
 - B. Site Description
 - C. Methodology
 - D. Approach
 - E. Facility Security Level Determination
 - F. Risk and Vulnerability Assessment Information and findings.
 - vii. The Security and Vulnerability Assessment Report shall include:
 - A. Site Vulnerabilities and the Corresponding Options for Consideration grouped in the following categories:
 - a. Security, Safety and Resilience Management

- b. Security Force, including but not limited operational risks
 - c. Risks associated with court operations and procedures
 - d. Alerting and Notification
 - e. Perimeter Security
 - f. Parking, Barriers, and Standoff
 - g. Access Control/ Entry control
 - h. Building Envelope
 - i. Electronic Security Systems
 - j. Illumination.
- viii. Draft Security Risk Assessment and Vulnerability Assessment Reports shall be submitted electronically to the AOC project manager identified in the contract in both Word and PDF formats.
- ix. Security Risk Assessment and Vulnerability Assessment Reports shall be submitted withing (10) business days after each site assessment is complete. The final version of the reports shall be submitted no later than (5) business days after the New Hampshire Judicial Branch completes its internal review and editing process and the contractor has answered all questions.
- x. Security Risk Assessment and Vulnerability Assessment Reports and any work product shall be considered property of the New Hampshire Judicial Branch, and the contractor shall maintain a non-disclosure agreement.
- xi. The contractor shall provide in-person presentations regarding the assessment and reports for seven (7) of the thirty-nine (39) facilities identified by the New Hampshire Judicial Branch, including the supreme court, two superior courts (selected by the Chief Justice of the Superior Court in consultation with the Assistant Director – Safety and Security), three circuit courts (selected by the Administrative Judge of the Circuit Court in consultation with the Assistant Director – Safety and Security) and the Administrative Office of the Courts. The presentations will be held at the Administrative Office of the Courts, One Granite Place in Concord, NH.

4. Task 3 – Project Management, Meeting, and Quality Assurance/Quality Control (QA/QC)

- a. Contract shall keep the AOC fully apprised of the project by providing timely meetings and other forms of communication including, but not limited, to:
 - i. Maintaining a designated Project Manager who will be the point of contact for the AOC. This individual shall attend all meetings and be responsible for the overall coordination of all project communication, activities, and deliverables.
 - ii. Scheduling and leading kickoff meetings and/or workshops shall be scheduled within (30) days of a final contract being awarded.

- iii. Within seven (7) business days of receiving the site list, the contractor shall provide to the state a master schedule detailing when each building assessment will be completed.
- iv. The AOC reserves the right to prioritize facilities in scheduling.
- v. The AOC will coordinate a vendor assessment team access to facilities prior to each assessment. The Assistant Director – Safety and Security will be the AOC lead and point of contact for the selected vendor throughout the contract term.

B. Vendor Qualification Requirements

1. Minimum vendor qualification requirement (a vendor who fails to meet all the minimum vendor qualification requirements will be deemed non-compliant and will be disqualified from further consideration).

- a. Vendor must have a minimum of ten (10) years' experience providing physical security assessments. Please provide references with name and contact information.
- b. Vendor must have no conflict of interest regarding any work performed by the firm or by the State of New Hampshire.
- c. Vendor shall be independent and non-product affiliated security consulting firms. Project leads shall be credentialed through the American Society for Industrial Security International (ASIS) as Physical Security Professionals (PSP) or similar levels of professional certifications to perform a security risk assessment.
- d. Vendor shall have successfully fulfilled contracts of similar scope, scale, terms, and costs. Please provide a summary of such contracts.

2. Preferred Experience and Qualifications for Vendor.

- a. Experience providing physical security assessments in court facilities. Please provide a summary.

3. Registration with the Secretary of State. For an out of state vendor, they must have a valid Certificate of Authority to transact business, as required by New Hampshire law RSA 293-A. The form for applying for a Certificate of Good Standin can be acquired through the New Hampshire Secretary of State's website at: <https://sos.nh.gov/corporation-ucc-securities/corporation/forms-and-fees/>

This requirement *must* be satisfied by applying for a Certificate of Authority before the effective date of the contract resulting from this RFP.

SECTION III. RFP PROCESS

A. Agency Point of Contact/Restriction of Contact with Agency Employees

The sole point of contact for this RFP, from the RFP issue date until the resulting contract is effective:

Assistant Director Takhmina Rakhmatova
procurement@courts.state.nh.us

From the date of release of this RFP until the award is made and announced regarding the selection of a vendor, all communication with personnel employed by or under contract with the NHJB regarding this RFP is prohibited unless first approved by the RFP Sole Point of Contact. NHJB employees have been directed not to hold conferences and/or discussions concerning this RFP with any potential contractor during the selection process, unless otherwise authorized by the RFP Sole Point of Contact. Vendors may be disqualified for violating this restriction on communications.

B. Vendor Inquiries

All contact concerning this RFP, including but not limited to, requests for clarifications, questions, any changes to the RFP, must be submitted via email and received by the Point of Contact by the end of vendor inquiry period (see Schedule of Events herein).

The email subject must be as follows: **INQUIRIES TO RFP NHJB-2024-02**

The vendor must identify the RFP name, page number and relevant paragraph and include the vendor's name, telephone number, and e-mail address.

The AOC's responses to properly submitted inquiries will be posted on the following website on or before the date specified in the Schedule of Events: <https://www.courts.nh.gov/our-courts/supreme-court/about/administrative-office-courts/rfps-and-rfis>

The AOC may consolidate and/or paraphrase questions for sufficiency and clarity. Oral statements, representations, clarifications, or modifications concerning the RFP shall not be binding upon the AOC. Official responses by the AOC will be made only in writing by the process described above. It is the responsibility of vendors to review the most updated information related to this RFP before submitting a proposal.

C. RFP Addendum

The AOC reserves the right to amend this RFP at its discretion, prior to the Proposal submission deadline. In the event of an addendum to this RFP, the AOC, at its sole discretion, may extend the Proposal submission deadline, as it deems appropriate.

D. Property of the NHJB

All material received in response to this RFP shall become the property of the NHJB and will not be returned to the vendor. Upon Contract award, the NHJB reserves the right to use any information presented in any Proposal.

E. Confidentiality of a Proposal

Unless necessary for the approval of a contract, the substance of a proposal must remain confidential until the Effective Date of any contract resulting from this RFP. A vendor's disclosure or distribution of Proposals other than to the AOC will be grounds for disqualification.

F. Public Disclosure

The content of each vendor's Proposal shall become public information upon the award of any resulting Contract. Any information submitted as part of a response to this RFP may be subject to public disclosure under applicable law.

Confidential, commercial or financial information may be exempt from public disclosure under applicable law. If you believe any information being submitted in response to this request for proposal, bid or information should be kept confidential as financial or proprietary information, you must specifically identify that information in a letter to the AOC and must mark/stamp each page of the materials that you claim must be exempt from disclosure as "CONFIDENTIAL". A designation by the vendor of information it believes exempt does not have the effect of making such information exempt. The AOC will determine the information it believes is properly exempted from disclosure. Marking of the entire Proposal or entire sections of the Proposal as confidential will neither be accepted nor honored. Notwithstanding any provision of this RFP to the contrary, vendor pricing will be subject to disclosure upon approval of the contract. If a request is made to the AOC to view portions of a Proposal that the vendor has properly and clearly marked confidential, the AOC will notify the vendor of the request and of the date the AOC plans to release the records. To halt the release of information by the AOC, a vendor must initiate and provide to the AOC, prior to the date specified in the notice, a court action in the Superior Court of the State of New Hampshire, at its sole expense, seeking to enjoin the release of the requested information.

By submitting a proposal, vendors acknowledge and agree that:

- The AOC may disclose any and all portions of the proposal or related materials which are not marked as confidential and/or which have not been specifically explained in the letter to the person identified as the point of contact for this RFP;
- The AOC is not obligated to comply with a vendor's designations regarding confidentiality and must conduct an independent analysis to assess the confidentiality of the information submitted in your proposal; and
- The AOC may, unless otherwise prohibited by court order, release the information on the date specified in the notice described above without any liability to a vendor.

G. Ethical Requirements

From the time this RFP is published until a contract is awarded, no vendor shall offer or give, directly or indirectly, any gift, expense reimbursement, or honorarium, as defined by RSA 15-B, to judicial or non-judicial employee of the AOC, any elected official, public official, public employee, constitutional official, or family member of any such official or employee who will or has selected, evaluated, or awarded an RFP. Any vendor who has been convicted of an offense based on conduct in violation of this section, which has not been annulled, or who is subject to a pending criminal charge for such an offense, shall be disqualified from bidding on the RFP. A vendor that was disqualified under this section because of a pending criminal charge which is subsequently dismissed, results in an acquittal, or is annulled, may notify the AOC.

H. Non-Commitment

Notwithstanding any other provision of this RFP, this RFP does not commit the AOC to award a Contract. The AOC reserves the right, at its sole discretion, to reject any and all Proposals, or any portions thereof, at any time; to cancel this RFP; and to solicit new Proposals under a new acquisition process.

I. Compliance

Vendors must be in compliance with applicable federal and state laws, rules and regulations, and applicable policies and procedures adopted by the AOC currently in effect, and as they may be adopted or amended during the contract period. It is vendor's responsibility to determine the applicability and requirements of any such laws, rules and regulations.

J. Proposal Cost

By submitting a Proposal, a vendor agrees that in no event shall the AOC be either responsible for or held liable for any costs incurred by a vendor in the preparation of, or in connection with the Proposal, or for oral presentation or product demonstration if any.

SECTION IV. PROPOSAL SUBMISSION REQUIREMENTS

A. Proposal Submission, Deadline, and Location Instructions

Proposals must be submitted via E-mail to procurement@courts.state.nh.us.

Proposals must be clearly marked as follows:

**NEW HAMPSHIRE JUDICIAL BRANCH
RESPONSE TO RFP NHJB-2024-02
SECURITY RISK AND VULNERABILITY ASSESSMENT OF NH JUDICIAL BRANCH
FACILITIES**

The email subject must be as follows: **RESPONSE TO RFP NHJB-2024-02**

Proposals must be received no later than the time and date specified in the Schedule of Events section. Late submissions may not be considered for contract award. Delivery of the Proposals shall be at the Bidder's expense. NHJB accepts no responsibility for mislabeled email or email that is not delivered or undeliverable for whatever reason.

B. Validity of Proposal

The proposal shall be signed by a person authorized to legally bind the Bidder and shall contain a statement that the proposal and the pricing contained therein will remain valid for hundred and eighty (180) days following the deadline for submission of Proposals in Schedule of Events, or until the effective date of any resulting Contract, whichever is later.

C. Proposal Format

- a. For clarity, the proposal should be typed or printed. Proposals should be single-spaced with 1" margins on white 8 1/2" x 11" paper using a font no smaller than 12-point Times New Roman or similar. The proposal must be in the searchable PDF format.
- b. Bidders must respond to each question and instructions listed in Appendix C of this RFP. Number each response in the proposal to correspond to the relevant question or instructions of the RFP.
- c. All pages of the proposal should be numbered consecutively beginning with number 1 on the first page (not including the cover page or table of contents pages) through to the end, including all forms and attachments. Bidder's name should appear on every page, including attachments.
- d. All electronic documents should be formatted for printing as formatting will not be adjusted prior to printing and review of these documents.
- e. It is the responsibility of the Bidder to provide all information requested in the RFP package at the time of submission. Failure to provide information requested in this RFP may, at the discretion of the AOC, result in a lower rating for the incomplete sections and may result in the proposal being disqualified for consideration.
- f. The Bidder shall complete and submit the "Proposal Cover Page" provided in Appendix A of this RFP and provide it with the Bidder's proposal. The cover page must show the specific

- information requested, including Bidder address(es) and other details listed. The proposal cover page shall be dated and signed by a person authorized to enter into contracts on behalf of the Bidder.
- g. The Bidder should complete and submit the “Debarment and Non-collusion Certification Form” provided in Appendix B of this RFP. Failure to provide this certification may result in the disqualification of the Bidder’s proposal, at the discretion of the AOC.

SECTION V. EVALUATION OF PROPOSALS

A. Criteria for Evaluation and Scoring

The AOC will evaluate each responsive proposal using a scoring scale of 100 points which will be distributed as set forth in the table below:

CATEGORIES	POINTS
Technical Proposal	
Proposed specifications for work to be performed	25
Vendor Experience and Qualifications (including but not limited to vendor and vendor staff qualifications, experience with similar scope and scale, references from contracts for services with a similar scope and scale)	45
Cost Proposal	30
TOTAL MAXIMUM POINTS	100

The review team will use a consensus approach to evaluate the proposals. The Vendor receiving the highest number of evaluation points will be recommended for contract negotiations.

B. Oral Interviews and Product Demonstrations

The AOC reserves the right to invite vendors to oral interviews and/or product demonstrations. The NHJB retains the sole discretion to determine whether to conduct oral interviews, with which vendors, and the number of interviews. Vendors are advised that the AOC may decide to conduct interviews with less than all responsive vendors.

The purpose of oral interviews and product demonstrations is to clarify and expound upon information provided in the written proposals. Information gained from oral interviews and product demonstrations will be used to refine technical review scores assigned from the initial review of the proposals. Vendors are prohibited from altering their proposals during the oral interviews and product demonstrations. Therefore, Vendors should submit proposals that present their rates and other information as clearly and completely as possible.

The AOC may ask the vendor to provide written clarifications of elements in their proposal regardless of whether it intends to conduct oral interviews.

C. Cost Proposal Scoring

Cost proposals will be reviewed upon completion of the final technical scoring of proposals. Vendors are advised that this is not a low bid award and that the scoring of the cost proposal will be combined with the scoring of the technical proposal to determine the overall highest scoring vendor.

Best and Final Offers: The AOC may seek a best and final offer (BAFO) from any Bidder in this procurement process. All Bidders are expected to provide their best value pricing with the submission of their proposal.

D. Negotiations and Selection

1. The AOC reserves the right to waive minor or immaterial deviations from the RFP requirement if determined in the best interest of the NHJB.
2. The final decision regarding the award of the contract is subject to approval by the Director of AOC and the Administrative Council (if applicable).
3. If the AOC determines to make an award, it will issue an “intent to negotiate” notice to a vendor based on these evaluations. The AOC reserves the right to negotiate with the successful Bidder to finalize a contract at the same rate or cost of service as presented in the selected proposal. Such negotiations may not significantly vary the content, nature or requirements of the proposal or the AOC’s Request for Proposals to an extent that may affect the price of goods or services requested. The AOC reserves the right to terminate contract negotiations with a selected Bidder who submits a proposed contract significantly different from the proposal they submitted in response to the advertised RFP. In the event that an acceptable contract cannot be negotiated with the highest ranked Bidder, the AOC may withdraw its award and negotiate with the next-highest ranked Bidder, and so on, until an acceptable contract has been finalized. Alternatively, the AOC may cancel this RFP, and solicit new proposals under a new acquisition process.
4. The AOC reserves the right to reject any and all Proposals or to make multiple awards.

SECTION VI. CONTRACT DOCUMENT

- A. The Selected Bidder will be required to execute a contract in the form of the NHJB Standard Terms and Conditions which is attached as Appendix D.
- B. To the extent that a vendor believes that exceptions to the standard form contract will be necessary for the vendor to enter into the Agreement, the vendor should note those issues during the vendor inquiry period. The AOC will review requested exceptions and accept, reject or note that it is open to negotiation of the proposed exception at its sole discretion. If the AOC accepts a vendor's exception the AOC will, at the conclusion of the inquiry period, provide notice to all potential bidders of the exceptions which have been accepted and indicate that exception is available to all potential bidders. Any exceptions to the standard form contract that are not raised during the Vendor inquiry period are waived. In no event is a vendor to submit its own standard contract terms and conditions as a replacement for the NHJB's terms in response to this solicitation.
- C. Allocation of funds is final upon successful negotiations and execution of the contract, subject to the review and approval of the Director of the Administrative Office of the Courts, and NHJB Administrative Council (if applicable). Contracts are not considered fully executed and valid until approved by the Director and the Council and funds are encumbered. No contract is effective unless signed by the Director.

APPENDIX A

PROPOSAL COVER PAGE

RFP NHJB-2024-02

**PHYSICAL SECURITY RISK AND VULNERABILITY ASSESSMENT OF NH JUDICIAL
BRANCH FACILITIES**

Bidder's Organization Name:			
Chief Executive - Name/Title:			
Tel:		E-mail:	
Headquarters Street Address:			
Headquarters City/State/Zip:			
<i>(Provide information requested below if different from above)</i>			
Lead Point of Contact for Proposal - Name/Title:			
Tel:		E-mail:	
Local Office Street Address:			
Local Office City/State/Zip:			

- This proposal and the pricing contained therein will remain valid for hundred and eighty (180) days following the deadline for submission of Proposals in Schedule of Events contained in the RFP, or until the effective date of any resulting Contract, whichever is later.
- No personnel currently employed by the NHJB or any NH State agency participated, either directly or indirectly, in any activities relating to the preparation of the Bidder's proposal.
- No attempt has been made, or will be made, by the Bidder to induce any other person or firm to submit or not to submit a proposal.
- The above-named organization is the legal entity entering into the resulting agreement with the NHJB should they be awarded the contract.
- The undersigned is authorized to enter contractual obligations on behalf of the above-named organization.

To the best of my knowledge, all information provided in the enclosed proposal, both programmatic and financial, is complete and accurate at the time of submission.

Name (Print):	Title:
Authorized Signature:	Date:

APPENDIX B
DEBARMENT AND NON-COLLUSION CERTIFICATION
RFP NHJB-2024-02
SECURITY RISK AND VULNERABILITY ASSESSMENT OF NH JUDICIAL BRANCH
FACILITIES

By signing this document, I certify to the best of my knowledge and belief that the aforementioned organization, its principals and any subcontractors named in this proposal:

- a. Have not, within the past 2 years, been convicted of, or pleaded guilty to, a violation of RSA 356:2, RSA 356:4, or any state or federal law or county or municipal ordinance prohibiting specified bidding practices, or involving antitrust violations, which has not been annulled;*
- b. Have not been prohibited, either permanently or temporarily, from participating in any public works project pursuant to RSA 638:20;*
- c. Have not previously provided false, deceptive, or fraudulent information on a vendor code number application form, or any other document submitted to the state of New Hampshire, which information was not corrected as of the time of the filing of a bid, proposal, or quotation;*
- d. Are not currently debarred from performing work on any project of the federal government or the government of any state;*
- e. Have not, within the past 2 years, failed to cure a default on any contract with the federal government or the government of any state;*
- f. Are not presently subject to any order of the department of labor, the department of employment security, or any other state department, agency, board, or commission, finding that the bidder is not in compliance with the requirements of the laws or rules that the department, agency, board, or commission is charged with implementing;*
- g. Are not presently subject to any sanction or penalty finally issued by the department of labor, the department of employment security, or any other state department, agency, board, or commission, which sanction or penalty has not been fully discharged or fulfilled;*
- h. Are not currently serving a sentence or is subject to a continuing or unfulfilled penalty for any crime or violation noted in this section;*
- i. Have not failed or neglected to advise the division of any conviction, plea of guilty, or finding relative to any crime or violation noted in this section, or of any debarment, within 30 days of such conviction, plea, finding, or debarment;*
- j. Have not been placed on the debarred parties list by the NH Department of Administrative Services pursuant to RSA 21-I:11-c within the past year;*
- k. Have not been convicted of wage theft of its employees within the past 2 years;*
- l. Have not been convicted of a felony level offense involving worker safety practices within the past 2 years; or*
- m. Have not been found guilty, within the last 2 years, of misclassification of workers as independent contractors, in violation of department of labor standards and the definition of employee in RSA 281-A:2.*

I further certify that: the Proposal submitted in response to this RFP, the prices, terms and conditions, and Work quoted have been established without collusion with other vendors and without effort to preclude the NHJB from obtaining the best possible competitive Proposal. The above-mentioned entities understand and agree that collusive bidding is a violation of state and federal law and can result in fines, prison sentences, and civil damage awards.

Failure to provide this certification may result in the disqualification of the Bidder’s proposal, at the discretion of the NHJB.

Name (Print):	Title:
Authorized Signature:	Date:

APPENDIX C

BIDDER RESPONSE TEMPLATE

RFP NHJB-2024-02

SECURITY RISK AND VULNERABILITY ASSESSMENT OF NH JUDICIAL BRANCH FACILITIES

Bidders must submit proposals in accordance with “Appendix C– Bidder Response Template”. The Bidder’s proposal should sequentially follow each section found in Appendix C and Bidder must answer each question that is asked in each section, as well as respond to all information sought. The AOC reserves the right to reject any and all proposals that do not follow this required formatting. All proposals must address the following:

Section 1. Executive Summary

- The executive summary, which must not exceed five (5) pages, must identify how the Vendor satisfies the minimum standards for consideration, to include company size, availability of local personnel, geographic location of area offices, and an identified point of contact. Vendors are encouraged to highlight those factors that they believe distinguish their proposal. As such, a Vendor Profile/Background which demonstrates adequate security and corporate knowledge regarding court security is important.

Section 2. Vendor Entity Overview and Qualification

a. Vendor Overview (5 Page Limit)

Identify the proposed role of the Vendor on the Project. Describe the major business areas of the firm. Provide a high-level description of the firm’s organization and staff size. Discuss the firm’s commitment to the public sector, experience with this type of Project Implementation, and any experience in New Hampshire and/or in court systems. Demonstrate that the Vendor has correctly estimated the magnitude of effort and resources necessary to implement the Vendor’s Bid Proposal, and that the Vendor has the capabilities to perform the full Scope of Work.

b. Prior Project Descriptions

Provide descriptions of no more than three (3) most recent similar projects completed. Each project description should include:

- An overview of the project covering type of client, objective, project scope, role of the firm and outcome.
- Project measures including proposed cost, actual project cost, proposed project schedule and actual project schedule.
- Names and contact information (name, title, address and current telephone number) for one or two references from the client; and
- Names and project roles of individuals on the proposal team for the New Hampshire Project that participated in the project described.

c. Financial Strength

Provide at least one of the following:

- The current Dunn & Bradstreet Report on the firm; or
- The firm's two most recent audited financial statements; and the firm's most recent un-audited, quarterly financial statement; or
- The firm's most recent income tax return. For example, either a copy of the IRS Form 1065, U.S. Return of Partnership Income or Schedule E (IRS Form 1040) Supplemental Income and Loss (for partnerships and S corporations); or IRS form 1120, U.S. Corporation Income Return. These forms are typically submitted when a Vendor does not have audited financial statements.

d. Litigation

Identify and describe litigation in which the Vendor was a party in the last ten (10) years. Discuss merits, current status and, if available, outcome of each matter.

Section 3. Qualifications of proposed staff

Provide a resume not to exceed two (2) pages for each Vendor staff positions proposed to work on this project. Each resume should address the requirements in Services, Requirements and Deliverables including, but not limited to:

- The individual's educational background.
- An overview of the individual's work history.
- The individual's prior experience in security assessment, including assignment type (e.g. court, retail, military, etc.), role and duration of the assignment.
- Any significant certifications held by, or honors awarded to the Candidate.
- Copies of completed training.
- A history of the individual's applicable experience

Section 4. Subcontractor

Vendors must provide information on any Subcontractor(s) proposed to work on this Project. Required information shall include but not be limited to:

- Identification of the proposed Subcontractor and a description of the major business areas of the firm and their proposed role on the Project.
- A high-level description of the Subcontractor's organization and staff size.
- Discussion of the subcontractor's experience with this type of Project.
- Discussion of how the Vendor will verify a subcontractor's qualifications, background checks, and performance as they relate to the Vendor's specifications.
- Any other evaluations, assessments, course completions used for employment.
- Resumes of key subcontractor personnel proposed to work on the Project.
- Two (2) references from companies or organizations where they performed similar services (if requested by the State).

Section 5. Detailed Explanation of Plan of Operation:

Vendor must describe in detail how Section II of this RFP will be performed and include a project plan and timeline with a comprehensive and clear description of the plan for deliverables with the estimated timeframes for each and the role of each staff.

Section 6. COST PROPOSAL

Cost Proposal must be submitted separately from the Technical Proposal

The cost proposal must include a proposed deliverable payment structure, including the cost for each location specified in Appendix E, and any information necessary to ensure understanding of the cost proposal provided.

HOME SECURITY AUDIT AND RECOMMENDATIONS

Even though reports indicate that judges and other judicial branch personnel are more likely to be injured in a fall at home or in an automobile accident than in a work-related assault, increased violence in recent years has resulted in three judges being murdered at home. These deaths were directly connected to cases over which they presided. The home security audit that follows is designed to identify security risks and provide judges and other judicial branch personnel with basic personal security recommendations that can be used to protect them and their homes.

PERIMETERS/EXTERIOR OF THE HOME

1. Does the home have perimeter lighting? Yes ☐ No ☐

Recommendation: It is important that the entire yard is illuminated at night, without shadows.

Recommendation: Install motion detector lights for interior and exterior protection. Outside motion detector lights can be installed to automatically turn on interior lights, giving the impression someone has entered a room, at the same time the outside lights turn on.

2. Does the home have trees and shrubs that are overgrown to the point where they block easy view from within? Yes ☐ No ☐

Recommendation: Trim or remove thick shrubbery from window areas and replace them with shrubs that have thorns, like roses, near windows.

Recommendation: Trim or remove trees that may provide access to upper floor windows or balconies, and make sure trees or shrubs do not block a clear view of entries and windows from the street.

3. Does the home have outbuildings (detached garage, pool house, storage buildings) located on the property? Yes ☐ No ☐

Recommendation: Include all outbuildings into the main security system. Install quality residential locks on the buildings.

4. Do all perimeter doors provide protection from intruders? Yes ☐ No ☐

Recommendation: All perimeter doors should be solid core wood or steel with a deadbolt lock, in addition to any other locking device.

The door should have a peep hole installed to view any visitors prior to granting access to the home. No glass should be on the door that can be broken to gain entry. It is important that a three-inch strike plate for screws be installed in all entry doors.

Recommendation: Secure sliding glass doors with pins to prevent both horizontal and vertical movement, especially when the home is left vacant for an extended period of time. Sliding glass doors should be hung so that the sliding door is mounted on the inside. The door should be reinforced with a “jimmy-proof” bar to prevent forced entry.

Recommendation: Re-key or replace locks if keys are lost or stolen or if you move into a previously occupied residence. Make sure that you follow strict key control with keys used to access the home.

Recommendation: Be sure to restrict the number of keys to your residence. Keep keys in your possession; **DO NOT** hide keys outside under the mat, over doors, in mail slots, or in potted plants.

5. Are basement windows to the home secured? Yes ☐ No ☐

Recommendation: All basement windows should be secured from inside the home. Glass basement windows should be replaced by polycarbonate material or reinforced with decorative security bars. All ground shrubs in proximity to the basement windows should be trimmed or removed so that they do not provide potential intruders with cover from observation.

6. Does the home have an attached garage? Yes ☐ No ☐

Recommendation: Whenever possible, park vehicles in the garage. Always enter the vehicle from inside the garage. Always keep the garage doors closed and locked when not in use. In order to limit your exposure outside the vehicle during the hours of darkness, install an automatic garage door opener and make sure all family members know how to operate the garage door manually in the event of an emergency. Ensure that the door from the garage into the main house itself is a solid core door with a deadbolt locking device.

Recommendation: If there is a vehicle parked outside, make sure the area is well-lighted. If at all possible, have a remote starter installed in all vehicles, especially if they are parked outside. This device will allow you to start your vehicle from a safe distance.

7. Does the mail box or the entry of the home personally identify the occupants? Yes ☐ No ☐

Recommendation: So judges and their family members cannot be easily identified and then targeted, names of residents should not be displayed on mailboxes

INTERIOR OF THE HOME

1. Does the home have an anti-intrusion alarm system? Yes ☐ No ☐

Recommendation: Consider installing an anti-intrusion alarm system in the home that is tied into the local police department or a certified central alarm monitoring organization. Instruct family members on the operation of the system. Consider installing a local enunciation system or siren. The advantage of a siren is to alert neighbors to notify authorities, should the direct-connect alarm lines be compromised.

Recommendation: As an added security measure, alarm systems can be customized to provide monitoring for fire, medical alert, and closed circuit television (CCTV) surveillance of home exterior. The presence of cameras on the outside of the home is a definite deterrent to would-be intruders.

Recommendation: If you have a monitored intrusion detection system, display the monitoring company's decal or sign prominently on doors, windows, and in the yard to announce the presence of a security alarm system in the home.

2. Do you have smoke/heat detectors installed throughout the home? Yes ☐ No ☐

Recommendation: Smoke alarms and heat detectors should be installed throughout the home. They should be hard-wired into the home's electrical system with a battery backup in the event of a power failure. In addition, install and maintain all-purpose fire extinguishers throughout the home, especially in the kitchen.

Recommendation: Establish and periodically test fire evacuation procedures for all family members.

3. Is the exterior door leading from the basement to the upper floor made of solid core and equipped with a deadbolt lock? Yes ☐ No ☐

Recommendation: As with other exterior doors in the home, it is important that the basement door be of solid core wood or steel construction and equipped with a quality deadbolt lock to prevent entry by intruders.

4. Can the interior of the home be accessed through windows or other openings from the second floor or roof? Yes ☐ No ☐

Recommendation: All second floor windows and roof skylights must be secured to prevent access by intruders who could use drainpipes and other means to access the roof or upper floors.

5. Does the home have louver-type windows? Yes ☐ No ☐

Recommendation: Louvre windows should be replaced with solid windows made with tempered or shatterproof material.

6. Do all windows have adequate window coverings? Yes ☐ No ☐

Recommendation: Windows should be equipped with internal blinds, curtains, drapes, or shutters to prevent someone from seeing inside.

CONDOMINIUM AND APARTMENT SECURITY

Security in condominium and apartment complexes must be a cooperative effort between residents, management, maintenance workers, and police. All must work together to provide the best possible security for the building. Most of the recommendations for single-family dwellings apply to condominiums and apartment complexes. The following is an audit that is particular to those type buildings.

1. Do all doors and windows have locks that will secure the condominium/apartment while it is vacant? Yes ☐ No ☐

Recommendation: Examine all locks on doors and windows to ensure they are working properly. Before leaving the condominium/apartment, make sure all doors and windows are locked. Always double-check locked access windows that are at ground level.

2. Does your complex have a separate “Laundromat” area? Yes ☐ No ☐

Recommendation: If at all possible, avoid using the Laundromat in your complex by yourself. Always team up with a neighbor who you know and trust.

3. Does your complex have a building association or a way to alert residents of an emergency? Yes ☐ No ☐

Recommendation: Develop an apartment alert system with neighbors in the complex to help protect each other’s property. A well-organized and active tenant association will assist in deterring intruders.

Recommendation: Get to know the tenants in the complex. After you meet them, make a personal contact list for future use.

4. Does the complex have an electronic access system to control entry into the building? Yes ☐ No ☐

Recommendation: Do not allow access to strangers by “buzzing” them into the building. If someone enters the building by following you in, and that person is unknown to you, do not ride the elevator with them. If needed, exit the building and then re-enter later.

Recommendation: Report suspicious strangers, sounds, or actions to police, then notify the complex manager.

MAIL SECURITY

If you receive mail at your home, be wary of suspicious letters or packages. Do not open a letter that appears to be unusual in any way, particularly if it has a perceptible bump, which might be an explosive device. Notify law enforcement immediately of any unexplained package in or near your home. You should notify law enforcement when mail items have any suspicious features, such as:

- Excessive weight, size, or postage
- Springiness in the top, bottom, or sides of the envelope
- Wires or strings protruding from or attached to the envelope
- Envelope has uneven balance or a peculiar odor
- Stiffening of an envelope with cards or other material (such stiffening could be a spring-loaded explosive striker)
- No return address or the place of origin is unusual or unknown
- Name is misspelled

All such items should be isolated. Only trained law enforcement professionals should be allowed to open suspicious mail.

FAMILY SECURITY RECOMMENDATIONS

Recommendation: If at all possible, your home telephone number should be unlisted.

Recommendation: Family members, including care givers, should never tell anyone you are out of the house. They should be instructed to take messages from callers only.

Recommendation: Emergency police and fire numbers should be programmed into the telephone using the “In Case of Emergency” (ICE) concept. If you do not have a programmable phone, you should post emergency numbers near the main telephone in the home.

Recommendation: Do not discuss family plans with outsiders. Even your friends should not be informed. In general, do not discuss your family’s comings and goings.

Recommendation: Family members should not stop at the same supermarket at the same time on the same day each week. Vary your daily activities.

Recommendation: Children should be instructed not to open doors to strangers. All visitors should be viewed through a peephole with the door locked. Intercom systems should be used to aid in the identification of strangers.

Recommendation: If it is necessary to leave children at home, keep the house well-lighted and notify the neighbors.

Recommendation: Advise your children to:

- Never leave home without advising parents where they will be and who will accompany them.
- Travel in pairs or groups.
- Walk along busy streets and avoid isolated areas.
- Use play areas where recreational activities are supervised by responsible adults and where police protection is readily available.
- Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot—even if the strangers say mom or dad sent them or said it was okay.
- Report immediately to the nearest person of authority (teacher or police) anyone who attempts to molest or annoy a child.

Recommendation: Be wary of strangers. Be watchful of strange cars that seem to cruise the neighborhood or strange persons who suddenly start to frequent the neighborhood streets. Record information that may be helpful to police.

Recommendation: Observe cars parked in the neighborhood with one or more persons inside or persons who seem to be doing nothing in particular.

Recommendation: Never reveal to any stranger that you are home alone.

Recommendation: Know where your children are at all times. Maintain a daily itinerary and stress the importance of notifying other family members of changes in the schedule.

Recommendation: As mentioned above, have unlisted telephone numbers for ALL family members.

Recommendation: Always request salesmen, repairmen, meter readers, delivery personnel, and even policemen (in civilian clothes) to show their identification prior to admitting them into your home. If in doubt about their identity, place a call to their business to confirm employment. Never accept a phone number that they offer; always use the telephone directory or call the information operator.

Recommendation: Do not put your home telephone number on stationary or on any name and address stickers in order to preclude undesirable telephone calls.

Recommendation: When harassing or obscene telephone calls are received, take action to change your phone number immediately. Family members should never engage in a telephone conversation with unknown or unidentified persons.

Recommendation: Children must follow a school schedule, but if they are driven to school, varied routes should be followed. Children should be escorted to and from bus stops. Neither hiking nor walking to school is recommended.

Recommendation: Inform school authorities that children should not be released from school, athletic events, and club meetings on the strength of a telephone call. Advise the school authorities to confirm the call with your home or office.

Recommendation: Instruct the school administration that if an authorized person does not explain a child's absence from school shortly after school starts, they are to call the child's home or your office to determine the child's status.

Recommendation: Do not open doors to strangers or accept delivery of packages unless the sender is known. Instruct children and in-home help on this procedure. Install a chain lock on the main entry door so that you may accept small packages or letters by partially opening the door. Do not rely heavily on this type of lock, as an intruder can break them away by forcing the door.

Recommendation: Check references of service personnel, domestics and childcare providers, and any other employees who have routine access to your residence or property.

Recommendation: When receiving a wrong number telephone call, never give your name or number. Just state that the caller has the wrong number.

Recommendation: When a stranger requests to use your telephone for an emergency, never allow entry into the home. Offer to summon assistance, and use the phone yourself.

Recommendation: Never answer your telephone with your name; a simple hello is acceptable.

Recommendation: Report all suspicious activity to the local police.

TRAVEL RECOMMENDATIONS

Whether you are going to the store or Europe, the fact that you have left your home or office changes your security status **SIGNIFICANTLY**. Travel decreases your security because you are not adhering to your routine, but instead, you are exposed to unfamiliar surroundings. If you plan to travel outside your home area or overseas, you should check with your director of security for additional security measures that can be taken to protect you and your family.

VEHICULAR TRAVEL RECOMMENDATIONS

Recommendation: Do not pick up strangers or give a ride to a stranger or volunteer your car to a group of strangers even though you may have a friend with you in the car.

Recommendation: If you should have car trouble on the road, drive to the side of the road and place a handkerchief or white cloth on the radio antenna or door facing traffic. Either place a cell phone call or wait for help to come.

Recommendation: If you are driving and an attempt is made to force you off the road, move toward the center of the roadway and quickly proceed to a busy street and seek assistance. As you proceed, blow your horn to attract attention to your plight.

Recommendation: Do not stop to aid other motorists or pedestrians, regardless of the circumstances. If you believe the emergency is genuine, use a cell phone or proceed to a public phone and report the matter to authorities, then let them handle the emergency.

Recommendation: If you suspect you are being followed:

- Circle the block to confirm the surveillance.
- Do not stop or take other actions that could lead to a confrontation.
- Do not drive home.
- Do not try to evade or elude the follower.
- Obtain a description of the vehicle and its occupants.
- Go to the nearest police or fire station and report the incident.
- Have an alternative safe place to go in the event you cannot get to the police station.
- Report the incident to police once you are safe.

Recommendation: Avoid using magnetic key boxes hidden in the wheel well of your car.

Recommendation: Park your car in a secured garage; do not park your car on a public street.

GENERAL SECURITY RECOMMENDATIONS

Recommendation: Place the police emergency telephone number (911), and the police non-emergency number next to the phone in your home for immediate use; program it into your telephone system if possible. Do not answer the telephone with your name or official title.

Recommendation: Ladders and scaffolding should be kept in locked outbuildings or garages.

Recommendation: Advise the local police department of your occupation and address. Complete and submit a judicial profile for you and your family (attached), to the chief security officer for use in emergencies. Judicial profiles should be protected as “confidential-restricted access” documents.

Recommendation: Consider moving all fuse and switch boxes into the home if possible. Place locks on those that remain outside or in outbuildings/garages.

Recommendation: Consider a trained watchdog for the family residence. In addition to being a natural deterrent, it is another means of alarming the home.

Recommendation: Be constantly aware of surveillance. Usually a potential victim is watched for several days before an act of violence is carried out.

Recommendation: Prepare an inventory of household and personal possessions, describing the articles and listing the serial numbers for reference.

Recommendation: In order that personal items (jewelry, appliances, TV sets, radios, etc.) can be identified if lost or stolen, a code number should be engraved on each item with an etching machine.

Recommendation: A small safe or security box, which can be bolted down to a closet floor,

should be used to secure personal jewelry, cash, and personal documents that are frequently used. Consider a safety deposit box for items used less frequently.

Recommendation: When the home is left vacant, install timers on televisions, radios, and lights in order to give the impression that the home is occupied.

Recommendation: Have “Caller ID” for incoming telephone calls to your home. Use “Caller ID” blocking to prevent your telephone number from being displayed on outgoing calls.

Recommendation: Become familiar with the streets and roads surrounding your home. Have a planned escape route from your home to a designated safe place in case of fire or intrusion.

Recommendation: Plan and practice driving to area emergency services, such as hospitals, police stations, and safe places.

Recommendation: Make sure your trash is kept in a secure place, such as a locked outbuilding.

Recommendation: Keep the names, addresses, and telephone numbers for all staff members handy in the event of an emergency.

Recommendation: If you have household employees, make sure they have been screened with background checks.

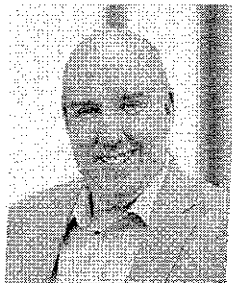
For further information contact:
National Center for State Courts
Court Consulting Services
707 17th Street – Suite 2900
Denver, CO 80202
(303) 305-4315



This document was prepared by Jim O’Neil, NCSC Security Consultant
Revised: June 2013

DIRE The State of

Threats against judges have multiplied; threats against women judges have increased even more rapidly.



By David Hofstede,
Freelance writer and the Director of
Legislative Outreach for Ironwall by Incogni

Threats against judges have multiplied; threats against women judges have increased even more rapidly. One can only imagine how Judge Charlotte Sweeney felt when the request landed on her docket. The American Civil Liberties Union petitioned to temporarily bar the Trump administration from removing undocumented aliens under the Alien Enemies Act.

On one side a prominent national organization with the resources to publicize one version of the facts to sway a national jury to their point of view. On the other, the United States Executive Branch, with equal if not greater resources, and a spokesperson in the Commander and Chief who will not only argue that the case is unfair, but that he is once again being persecuted by activist judges.

As with any other case, Judge Sweeney would listen to the testimony of both sides, review the facts, and then issue a verdict – knowing that, whichever way she rules, she is about to anger about half of the country.

It's never been an easy job. But it's also never been this difficult – or dangerous.

f Judicial Security

"We've seen an increased willingness from public officials and public figures to criticize judges in ways that go beyond the type of informed criticism that Chief Justice John Roberts identified in his 2024 report on the judiciary," said Judge Paul Grimm, who served 25 years on the federal bench, and is currently the Director of the Bolch Judicial Institute at Duke University.

It seems worse now because it is. The ACLU alone has filed nearly 400 cases against the Trump administration that are likely to be unpopular with his supporters. But growing hostility against the judiciary predates the current officeholder. "What is happening now is not unique to any one political party or political ideology. There have been examples of Democratic leaders

threats, harassment, vandalism, and even violence.

For more than a decade we've been living in a hyper-politicized and polarized nation. The inability of Congress to pass legislation on major issues has left a void that Chief Executives going back decades have attempted to fill with executive

orders that are inevitably challenged in court, putting judges at the center of contentious national debates. And when the media covers these cases, it invariably specifies which president appointed the ruling judge, reinforcing the perception that judges act

politically rather than independently.

Discussion of controversial cases is amplified by social media, where the tone of such conversations is typically aggressive and threatening. "If I make a threatening comment to an audience of five, it has less impact than if I make it to an audience of five million," Grimm said. "Somewhere in that five million there is a greater likelihood that someone is going to act rather

Several disparate factors have all contributed to a heightened hostility against judges, and an increased number of individuals and organizations willing to express their grievances through threats, harassment, vandalism, and even violence.

"What Chief Justice Roberts said was, of course the public has a right to criticize judges, and informed criticism about a decision is within the realm of what is appropriate. But he identified four categories of conduct that cross the line, and that includes criticism or action that's intended to intimidate, personal threats, claims that courts are not legitimate, and refusals to comply with court orders."

criticizing judges by name and with very strong threatening terms. Both sides have done it," Grimm said.

How Did We Get Here?

Several disparate factors have all contributed to a heightened hostility against judges, and an increased number of individuals and organizations willing to express their grievances through

than merely voice their anger, and we have seen examples of that in both state courts and federal courts.”

Women Judges Targeted More Frequently

While the reality of the rising threat level is widely acknowledged, what has not been addressed is the disparity between the volume of threats received by women judges. “It is hugely disproportional toward women,” said Ron Zayas, CEO of Ironwall by Incogni, a company that provides online privacy protection to US courts.

“Our numbers also reveal that the situation is even worse for women of color, who are threatened at a rate about 40% higher than a white male judge,” Zayas said. “It’s also clear that the type of threats they receive are more vicious, more compromising, and oftentimes they threaten sexual violence. When courts invest in protection, they don’t seem to acknowledge that, or that women judges are especially in danger”.

The nature and intent of threats directed at judges has also evolved. Direct threats – those sent to a specific judge at the courthouse or at the judge’s home (easy to do given the online accessibility of anyone’s home address) are up as much as 400% according to the US Marshals Service. Someone is angry at a judge over a loved one being sentenced, or being denied child visitation, and expresses that grievance by threatening the judge or his or her family. You hurt me – now I’m going to hurt you.

“Those types of threats still happen every day. But there’s another kind of threat – I liken it to a mafia threat, that is

also increasing,” Zayas said. “These are threats issued not to punish a judge for what they have done, but to stop them from doing something in the future and to change their behavior.”

A recent illustration happened in April, when hundreds of federal judges received pizzas at their home, with those orders attributed to the murdered son of a federal judge. “The mob doesn’t necessarily want to kill you. That’s their last resort. What they want to do is influence your decision-making. So, they send you a message that is designed to let you know that they can get to you,” Zayas said.

When a judge receives an active threat, Ironwall places that judge into its emergency support program. The company now has three times as many judges in receiving this protection than it did last year. “Judges and courts are taking these threats more seriously. There’s a greater sensitivity and a greater acknowledgment that threats turn into violence more than they have before,” Zayas said. “Courts are more aware of it, which is why more courts are paying for protection.”

What Can Be Done?

“I think the first line of defense is increasingly going to fall upon the individual judges themselves, becoming more informed, aware of the threat factors, getting a security assessment and how they can harden their environment,” Judge Grimm believes. “It’s incumbent upon judges to be aware of their personal behaviors as far as information they are sharing online and seek input from security professionals who can teach them the proper ways to protect

themselves and their families.”

As with online protection, alarms and home security systems provide an extra layer of safety that could discourage or repel a potential attacker. However, also as with online protection, don’t just choose a provider and assume the problem is solved. Get more than one estimate and program description and test the response time. If someone is trying to break into your home, and help doesn’t arrive for 30 minutes or more, that will likely not be effective.

Explore federal and state options that cover part or all the cost of home security systems. Inquire with your court, local law enforcement and the US Marshals for direction in how to select and use the system best for you.

Judicial Protection Laws

Twenty states have passed consumer data protection laws that give residents more control over their personally identifiable information, and more are now passing similar laws specific to judges, granting them authority to have their home addresses and other private data removed from anywhere it may be accessed online. At the federal level, the Daniel Aderl Judicial Security and Privacy Act (“Daniel’s Law”) generally prohibits federal agencies and private businesses from publicly posting certain personal information (e.g., home addresses) of federal judges and their immediate family members.

If judicial protection legislation is pending in your state, contact your legislators and let them know of your advocacy. If not, contact them to raise awareness over the number of threats

and attacks judges now face, and request that a bill providing protection be introduced in the next session.

But laws are just words on paper unless they are enforced, and that takes resources that must be allocated to do so. "Given the configuration of the House and the Senate as it is at the present and the degree of hostility being directed at judges, I think it would be a welcome surprise if in that environment the appropriations for the state and federal judiciary included sufficient funds and resources to heighten security for judges," said Grimm.

Statutes do help, even when resources are lacking. They provide guard rails and raise awareness that certain actions are illegal and dangerous. But when awareness that enforcement is lacking becomes prevalent, they are more easily ignored. Let's face it – everyone in a town knows the roads where it's safe to drive 50mph when the speed limit is 35, because the police are focused elsewhere.

The passage of the Americans with Disabilities Act (ADA) offers a prime example of beneficial legislation that was initially ineffective because state attorneys general were swamped with violation reports and could only prosecute one out of every 10,000 cases. "To address the glut, they opened up private enforcement," Ron Zayas explained, "which allowed people to sue individually and enforcement to be turned over to attorneys and activists being able to move these cases forward. After that the number of lawsuits went up significantly."

Such private enforcement is now available to courts as well. "That allows

companies like ours to act on their behalf, and we can be much more aggressive in doing so," Zayas said.

"When properly implemented, online protection removes personal information online, and that has been proven to neutralize threats like the weaponization of pizza delivery. And like most preventative measures, it is cheaper than the cost of hiring armed details for judges, or the cost of a cowered judiciary."

Judges are People Too

In these contentious times, Judge Paul Grimm believes judges and lawyers must engage more actively with the public, to help them understand that judges are doing their jobs as a necessity, in a Constitutional checks and balance structure that was intended to allow each of the government branches to exercise authority over the others, so that no one branch becomes too powerful.

"We are in a hyperpolarized environment of congressional gridlock, bold action by executives by both parties, willingness on the part of political actors and public figures to personally criticize and attack the motives, the integrity, the impartiality, the legitimacy and patriotism of individual judges. And where is the counter-narrative?"

"It tends to be a letter to the editor that few people see, or a statement by a bar association. And that has a limited audience that is already more familiar with the situation. We have an American public that is largely, civically illiterate about the judiciary, which is the only branch of government that is designed to protect their rights, privileges, and benefits," Grimm said. "Courts and

judges are not telling their own stories; their stories are being told by other individuals, many of whom may not care whether they get it right."

Because of this, Ron Zayas believes the situation is likely to get worse.

"Courts have a historically low level of public confidence, and that situation is being exploited for a purpose. When the President says they're corrupt and that judges are bad people, he is giving his supporters tangible reasons to not just dislike the courts, but to believe that the courts are making their lives worse.

"We're already at the point where judges are asking for permission from their ethics committees to talk out about this stuff because they're not allowed to do it. But will it get to the point where we still have time to fix it? I don't know. But it is incumbent upon judges to protect themselves," Zayas stressed. "They should have the court do it. They should have the government do it. But at the end of the day, they must take responsibility and say, 'This is not going to happen to my family.'"

Through his work with the Bolch Institute, Judge Grimm is already speaking out in defense of judicial security and independence through civics and education programs. "We have to engage with the public because we didn't get in this position overnight. We must help them understand how our system works, and why the courts are vital to protecting the rule of law, which is essential to protecting their freedoms. And we must figure out a way to get that message out beyond the legal community so we're not just talking to ourselves. If we can do these things, then we have some hope."



THE EDWARD DAVIS

COMPANY



Prepared By :

The Edward Davis Company

32 Atlantic Ave 5th Floor

Boston MA 02110

eddavisllc.com

mail@eddavisllc.com

Prepared For :

**National Association of Women
Judges (NAWJ)**

NAWJ CONFERENCE BOSTON

October 23-25, 2025

ABOUT ME

Edward F. Davis is the President and CEO of The Edward Davis Company, a strategy and security services firm that advises government agencies, courts, and Fortune 500 companies on crisis response, risk management, and security planning. He served as Boston Police Commissioner from 2006 to 2013, leading the nationally recognized response to the Marathon bombing.

With more than 35 years in law enforcement, Commissioner Davis has extensive experience in judicial and courthouse security, high-profile trial protection, and strategies to safeguard judges and court staff from threats and intimidation. He has testified before Congress and the Senate on terrorism and public safety, and has served as an expert witness in cases that directly impacted judicial outcomes. Internationally, he has advised on policing and justice issues in Europe, the Middle East, and Asia.

He holds a master's degree from Anna Maria College, honorary doctorates from Northeastern, Suffolk, and UMass Lowell, and was a Fellow at Harvard's Institute of Politics.





Paul McLaughlin

In September 1995, Boston prosecutor Paul McLaughlin was shot and killed by gang leader Jeffrey Bly, who had McLaughlin tracked before the murder. Bly was set to be prosecuted by McLaughlin on carjacking charges the next day.

Details of the case:

- **Paul McLaughlin:** An assistant attorney general, McLaughlin was assigned to the Suffolk County District Attorney's office to prosecute gang-related cases.
- **Jeffrey Bly:** A leader of the Theodore Street Posse gang in Boston's Mattapan neighborhood, Bly feared going to prison for the carjacking and decided to kill McLaughlin to stop the trial.
- **Motive:** Bly, the leader of a gang in the city's Mattapan neighborhood, had developed a vendetta against McLaughlin after the prosecutor had previously tried Bly twice on other charges. Fearing a long prison sentence, Bly plotted the murder to prevent the carjacking case from moving forward.
- **Tracking:** Bly instructed a fellow gang member to follow McLaughlin from his courthouse office to his car at a commuter rail station in West Roxbury, recording his movements.
- **The murder:** Bly waited for McLaughlin at the train station. When McLaughlin got into his car, Bly shot him once in the head and fled.
- **Aftermath:** Bly was convicted of first-degree murder in 1999 and sentenced to life in prison without parole.



*Photo of Mr. Paul McLaughlin
Source: The Boston Globe*



Edward T. Bigham III

On October 2, 1980, Middlesex County prosecutor Assistant District Attorney Bigham, 28, was shot and killed along Memorial Drive in Cambridge after his car broke down. Three Boston men were later charged in the attack.

Details of the case:

- **Assistant District Attorney Bigham:** A Middlesex prosecutor since 1979, he began in the District Court system and had been promoted to the Superior Courts only a month before the shooting.
- **The attack:** Around 1:40 a.m., Bigham’s Volkswagen developed mechanical problems and was parked roadside when a large white car pulled up behind him. Three men approached. Bigham was shot in the chest.
- **Aftermath at the scene:** Bigham staggered from the vehicle before collapsing a few steps away. An MIT security guard administered emergency aid, but he was pronounced dead at Cambridge Hospital at 2:03 a.m.
- **Suspects:** Henry McLendon, Aldin Carter, and Arnold Evans, all Boston residents in their early 20s, were charged with murder, two counts of armed assault with intent to rob, and assault with a dangerous weapon.



UPI. (1980, October 2). An assistant district attorney was shot and killed early... – UPI archives. UPI. <https://www.upi.com/Archives/1980/10/02/An-assistant-district-attorney-was-shot-and-killed-early/9722339307200/>

Drive Murder. News: The Harvard Crimson. News | The Harvard Crimson. (1981, February 3). <https://www.thecrimson.com/article/1981/2/3/mem-drive-murder-pttwo-boston-men/>



DANIEL ANDERL JUDICIAL SECURITY & PRIVACY ACT

BACKGROUND & ORIGIN

- > Named in memory of Daniel Anderl, the 20-year-old son of U.S. District Judge Esther Salas, tragically murdered in a home attack in July 2020.
- > The assailant impersonated a delivery driver and had obtained Judge Salas’s personal info online.

KEY PROVISIONS

- > Bans data brokers from posting, selling, sharing information
- > Protects judges’ & families’ Personally Identifiable Information
- > Judges: request removal → 72-hour takedown
Exceptions: voluntary disclosures, news, gov’t records
- > Administrative Office of the U.S. Courts. may seek removal/injunctions; grants for redaction

IMPLEMENTATION

- > Administrative Office of the U.S. Courts Threat Management Branch offers Information removal services & threat monitoring services.
- > Home Intrusion Detection System program reimburses home security enhancements. . Up to \$2,500 for equipment plus increased monitoring support (\$800 annually).

Feature	Federal (Daniel Anderl Act 2022)	New Jersey (Daniel’s Law 2020)
Who is protected?	Federal judges & their families	State judges, prosecutors, law enforcement & families
What info is protected?	Addresses, phones, vehicle info, SSNs, schools, property	Primarily addresses and phone numbers
Scope	Nationwide	State of New Jersey only
Obligations for Public Entities	Must redact PII from publicly available records/websites upon request	Must remove/redact PII from online public records within specific timelines
Criminal Penalties	Civil penalties; potential injunctions and fines for noncompliance	Criminal penalties (disorderly persons offense); fines and potential jail time
Online Platform Liability	Platforms may be required to remove info or face fines	Platforms must comply or face civil/criminal penalties under NJ law



PERSONAL SECURITY

Home Security

- Layered defenses: alarms, cameras, reinforced doors, trimmed landscaping
- Use P.O. Box for mail; scrub home address from public records
- Establish and regularly practice family safety protocols (safe words, emergency plans, lockdown drills)

Digital & Daily Life Protection

- Layered defenses: alarms, cameras, reinforced doors, trimmed landscaping
- Use P.O. Box for mail; scrub home address from public records
- Family Preparedness: Coordinate with family to coordinate safety protocols
- Community familiarity increases digital risk: neighbors or local acquaintances may share personal info online.

Public & Community Presence

- Anticipate that litigants may see you in the community afterward.
- Deflect case-related conversations politely
- Avoid apparel, license plates, or vanity markers that identify you as a judge.
- Vary where you shop, dine, and attend services to avoid predictable patterns.

In the Courtroom & Commuting

- Park in well-lit, populated areas; avoid signs marking reserved “Judge” parking.
- Never preside without a security officer present.
- Keep proceedings orderly — remove disruptive individuals immediately to prevent spillover intimidation outside court.
- For virtual hearings from home, always use an official virtual background to hide personal surroundings.

Special Emphasis for Female Judges

- Recognize that gendered harassment may target your role as both judge and woman — often spilling into family or community life.
- Family-centered protections (school safety, digital monitoring, awareness training).
- Work closely with local police to extend security beyond the courthouse — including home patrols, faster response times, and ongoing communication.

THREAT MANAGEMENT

How to Assess Threats

Evaluate credibility and capability:

- Determine whether the threat is specific (who/what/when/where), feasible (does the person have the ability to act), and persistent or escalating in intensity. Distinguish between impulsive outbursts and credible, planned actions.

Analyze context and risk level:

- Consider whether the threat violates law or protective orders, appears in public forums (e.g., online), or targets family members, all of which elevate risk. Use a structured threat assessment scale (low/moderate/high).

Leverage documentation to reveal patterns:

- Record every incident (date, time, subject, evidence, witnesses, response) in a centralized, secure log. Repeated vague threats or unusual contacts can signal escalation when viewed collectively.

Threat Response



- Always document: every threat including date/time, subject details and nature of the incident, maintain originals of every concerning contact.
- Adhere to organizational or institutional protocols designed for handling threats.
- Involve authorities promptly, especially when there is a credible or immediate risk.

Muted Threat Response



Respond quietly when threats are:

- Vague, impulsive, or non-specific.
- Isolated outbursts with no evidence of capability.
- Risk of prosecution would escalate the threat actor's behavior.
- Insufficient evidence for charges

When do Threats Lose Relevance?



- Threats lose relevance only with **continued oversight, not silence.**
- Reduced frequency, intensity, and proximity could indicate that the threat environment is becoming less severe.
- Judges may hesitate to report repeated or low-level threats or harassment.
- Institutional encouragement and a clear reporting culture are essential to ensure proper evaluation and ongoing protection over time.



EDC COURT ASSESSMENTS

WHAT WE LEARNED

What Prompted Security Assessments in the Court System?

- Increase in emotionally charged family/domestic cases
- Rising harassment, intimidation, and doxxing of judges
- Courthouse facilities uneven, security systems untested
- Growing concern about workplace violence and active shooter threats

What We Learned (System-Wide)

- Post orders are inconsistent across courthouses
- Duress/panic switches are often untested or unknown
- Judges report threats, follow them beyond courtrooms
- Awareness and culture are as critical as physical security
- Fobs are being used instead of keys; fobs can be easily duplicated

What We Learned (Courtroom)

- Zoning opposing parties reduces flash points
- Pre-court '5-minute huddle improves readiness
- Bailiff placement critical in family/domestic dockets
- Judges' parking spaces are identified by their names

What We Learned (Travel/Commute)

- Parking lots and transitions are consistent risks
- Vary routes/times when possible
- Escorts are effective but underutilized
- Safe-haven routes (police/fire stations) are not widely known

WHATS CHANGING

What's Changing (Judges' Personal Safety)

- Issue safety packets with home/travel checklists
- Train families on household and social media safety
- Routine late-day escorts for high-risk sessions
- Follow threats across a judge's career, not just cases

What's Changing (System Level)

- Standardized post orders across courthouses
- Quarterly duress alarm tests with tracked response times
- Risk-rating of dockets, especially family/domestic cases
- Unified threat intake and triage process
- Replace fobs with something more secure
- Change names from parking spots to "reserved"

What's Changing (Daily Habits)

- Reverse-in parking, well-lit/staffed areas
- Delayed posting on social media, don't post location
- Lighting, locks, and cameras at home
- Household plan for unexpected visitors

What Can Be Done Now

- Issue judge safety packets
- Repair chokepoints, re-key doors (if needed)
- Adopt pre-court huddles and docket risk-ratings
- Offer quick home security consults

"QUICK WINS" (0-90 DAYS)



THANK YOU

CONTACT US :



Call

+888-550-3120



Mail

mail@eddavisllc.com



Address

32 Atlantic Ave Boston MA 02110



Web Adress

www.eddavisllc.com