Judicial Security

RECOMMENDATIONS FOR IMPLEMENTING SOUND PROTECTIVE INTELLIGENCE METHODOLOGIES

By John F. Muffler and Judge James R. Brandlin

Most states' Canons of Judicial Ethics largely mirror the ABA Model Code of Judicial Conduct. Judges are required to decide all matters assigned to them unless disqualified. Judges are required to uphold and apply the law fairly and provide all affected parties with the opportunity to be heard. They are to remain patient, dignified, and courteous. These fundamental principles are sometimes difficult to follow when judges are confronted with increasing caseloads and disproportionate numbers of difficult self-represented litigants, particularly in family law and criminal cases. A judge's ability to master the skill sets needed to balance these competing interests can also directly impact that judge's safety and well-being. A judge's ability to be fair is predicated upon his or her ability to preside over cases without fear or favor. When judges and other public safety officials are faced with increasingly inappropriate communications and threats, their impartiality can suffer.

What then are the ingredients of a threat and an inappropriate communication, and what can judges and other public safety officials do to mitigate these problems? What are the best practices? Why do some people, specifically litigants, make these inappropriate communications? What happens when litigants feel they have not had their day in court or feel that they have not been heard?

We have both asked these questions of our colleagues. Judges universally highlight the inherent difficulties associated with litigants suffering from mental illness as well as the ever-present danger associated with any emotional court proceeding involving a loved one. Moreover, whenever a litigant feels that counsel or the judge was unsympathetic or handled his or her grievance inappropriately, anything from a disruption in court to a direct threat can occur.

By definition, all threats are inappropriate communications, but not all inappropriate communications are threats. An inappropriate communication can be defined as something that does not respect the boundaries or procedures established in that forum or it may reflect an unusual interest in the recipient of the communication. A threat can be an indication of danger or an attempt to control another through expression of an intention to inflict pain, injury, evil, or punishment. The difference is a defining line for law enforcement. For threat assessment professionals, these inappropriate communications are markers along the continuum of risk and are indicators for the application of different threat management techniques.

In the past year alone, U.S. Marshals have investigated 1,390 inappropriate communications to federal judges, assistant U.S. attorneys, justices of the U.S. Supreme Court, and other government officials. In the past eight years, that number has exceeded 10,000. The Administrative Office of the United States Courts (AOUSC) reports that there were 96,000 self-represented litigant filings in the past year in the district courts and circuit courts of appeals. Approximately 10 percent of the inappropriate communications investigated stem from these self-represented litigants. Judge Michael S. Kanne, Seventh Circuit Court of Appeals, is chair of the Committee on Judicial Security, Judicial Conference of the United States. His committee and the AOUSC are working on ways to assist these litigants with legal advice so they have a fuller understanding of the complexities and nuances of court proceedings. This type of effort is essential to the education of self-represented litigants and lessens the potential for inappropriate behavior or communications.

The U.S. Marshals Service utilizes a robust and innovative protective methodology to mitigate threatening and potentially threatening behaviors. Educating protectees is the first step in the proactive law enforcement process, as the judge or other public safety official will be the likely recipient of the behavior or communication. It is important to note that persons who pose an actual physical risk of danger often do not make advance threats, especially direct threats to the target. Educating protectees in risk behaviors will enhance reporting and the prevention of harm. This educational process is a critical step in risk management. With timely reporting, protective intelligence measures function more effectively and proper security assessments can be conducted in order to ensure safety. The successes of these protective measures rely heavily on the ability of law enforcement to be proactive in a reactive situation.

There are four bedrock, proven principles of a protective investigation: (1) *identify* the communication to ensure that it meets the definition of an "inappropriate" communication and determining whether there was a triggering event; (2) *assess* the communication to determine if the subject poses a risk and whether the risk is immediate, conditional, or delayed; (3) *investigate* to determine the appropriate response to the threat or inappropriate communication; and (4) *manage* the case to include all updates and status of the activity. The key to this protective investigation is that it is a "behavior-based approach." Threat assessment professionals are more focused on the actions of the threatener than on merely looking at the words he or she used.

In the findings of their groundbreaking Exceptional Case Study Project (ECSP), Robert A. Fein, PhD, and Bryan Vossekuil stated, "Frequently, thinking about assassination is compartmentalized; some potential assassins engage in ongoing internal discussions about attacks while maintaining outward appearances of normality. In every ECSP case, assassination was the result of an understandable and often identifiable process involving the attacker's pattern of thoughts, decisions, behaviors and actions that preceded the attack." Barry Spodak, a Licensed Independent Clinical Social Worker (LICSW), trains the U.S. Marshals Service, U.S. Secret Service, and other federal agents on behavioral threat assessments and is director of Action Training Institute. He states:

> This finding has significant implications for individuals conducting threat assessment interviews. Rather than focusing on the difficult goal of getting the subject to admit to planning an assassination attempt, an interview can take the form of an unthreatening conversation that allows the subject to vent . . . his anger, frustrations, hopes or fantasies. Working from the assumption that people act in their perceived best interest, the interviewer can frame the conversation as a rare opportunity for the subject to share his perceptions and beliefs with a receptive audience. In this way, without raising the issue of illegal activity, the interviewer can influence the subject to talk openly about a broad range of noncriminal behaviors that serve as markers along a path to violence and help to identify a "pattern of thoughts, decisions, behaviors and actions" that can identify people who pose a threat to a protectee.

Assessing these behaviors is paramount to providing quality protective measures. The next step is to ensure that the threatened official understands the risks, measures, countermeasures, and level of security that will be provided and for how long. None of these measures are cookie-cutter, as each threat, inappropriate communication, and person under protection is unique and must be handled as such. Behavioral threat assessment methodologies are consistent whether the threat is to the president of the United States, a judge, or an electedofficial. All public officials are at risk from individuals who perceive that they have been wronged and want to inappropriately affect change by their actions in a way that favors their cause. Judges are part of a system that decides winners and losers in the court of law. The amount of loss and the type of court hearing are largely insignificant, as the reason for the attack may only make sense to the attacker alone.

Judge Joan Humphrey Lefkow of the U.S. District Court for the Northern District of Illinois was the fourth federal judge since 1978 known to be the target of assassination as a result of her work on the bench. Her husband and mother were murdered in February 2005 by self-represented litigant Bart Ross. Ross wanted to exact revenge for Judge Lefkow's dismissal of his medical malpractice case. Judge Robert S. Vance, Eleventh Circuit Courtf Appeals; Judge Richard J. Daronco, Southern District of New York; and Judge John H. Wood Jr., Western District of Texas, were the other federal judicial victims of assassination. Also victimized were their spouses, children, and family (not to mention their judicial families). What we have learned from these murders is that: (1) All attacks happened as a result of involvement over a specific court case, (2) none of the assailants conveyed a threat prior to the attack, (3) all attacks occurred away from the courthouse, and (4) three of the attacks stemmed from civil cases.

In the book *Murdered Judges of the 20th Century*, Judge Susan P. Baker chronicles the deaths and disappearances of 42 judges from 1908–99 in the United States. Of those 42 individuals, two went "AWOL" while under investigation for corruption and six were killed by family members whose deaths were not job related. Of the 34 remaining murdered judges, 13 were killed at the courthouse (prior to modern-day weapon screening programs) and 21 were killed away from the courthouse. Of those 21, 11 died in transit and 10 died at home. It must be noted that four spouses of these targeted judges were also killed at the time of the fatal attack.

We can glean from this that judges are at risk both in and away from the courthouse, but that the risks are higher away from their security details. What can judges and other justice personnel do to make themselves and their families safer? Here are some suggestions.

1. **Treat others with respect and do not become embroiled in the controversy or allow things to become "personal."**

Interviews with a number of suspects who have carried out violent attacks against judicial officers reveal that the suspects felt they were being treated unfairly and were not provided an opportunity to be heard during the court proceedings. Many felt they had no recourse other than to respond with violence. Judges are advised to do their best to explain the process, particularly to self-represented litigants. Sometimes even using terms like "The Court is required to impose a mandatory sentence of . . ." instead of "You richly deserve the punishment that I'm going to impose . . ." helps communicate that you are just doing your job and that it is not personal.

2. **Become invested in your own security**.

Judges who develop mindsets that they are powerless to stop an attack or that they have a predetermined fate are doing themselves a tremendous disservice. Join your court's security committee if one exists. If one does not exist, create one. That committee should include not only judges but your court's security provider, administrators, and staff, as well as facilities personnel. Work collaboratively with your court's security provider and local law enforcement to share information, evaluate your vulnerabilities, and develop appropriate mitigation strategies. Your court security provider can also obtain assistance and guidance from the U.S. Marshals Service.

3. **Be cautious of exposure in the public arena.**

Being away from a secured site makes you vulnerable; this is compounded when your appearance is broadcast. While it is best to keep your schedule unpredictable when out in public, many judges and public officials must be out in the public arena to allow their constituency to feel connected, in accordance with a fundamental part of the democratic process. Speeches and meetings at nonsecured sites may require advance law enforcement notification and/or a special security detail. The deterrent effect of law enforcement is hard to measure, but it stands to reason that an agent or police officer present at a function and visual to all may deter someone with bad intentions. For example, in the past year U.S. Marshals secured over 400 off-site conferences and speeches for their protectees with minimal incidents reported.

4. **Be aware of your surroundings.**

Whether you are on the bench, driving your car, or sitting in a restaurant, it is important to be aware of your surroundings at all times. Stay near the exits if possible, and sit with your back to a wall. If you carry judicial identification, carry it in a separate wallet so you can discard it during a robbery. When driving, select an outer lane so you can escape if necessary by driving over a curb or median. Stop with enough distance to see the car's tires in front of you touching the ground. This will leave enough room to drive around that car. Remember: if confronted in public, your priorities should be, first, to escape and evade and go to a secure location; second, to barricade and wait for help if you can't escape; and last, to stand and fight where there is no other choice.

5. **Practice "what if" scenarios.**

To stay sharp and prepared, do what law enforcement officers do: envision possible dangerous scenarios and think about your reactions and alternatives. Involve your spouse and staff with these scenarios for a collaborative and coordinated outcome. In this way, you pre-plan your responses and your reaction times become much faster in emergencies.

6. **Harden the target.**

Courthouses are attractive targets for disgruntled litigants and terrorists alike. New facilities should be designed, and older facilities should be modified if possible to utilize modern threat mitigation standards, including set-backs to minimize damage from bomb blasts, bollards to prevent vehicles from ramming the buildings, weapons screening, controlled access points, and personnel flow patterns to segregate members of the public, staff, judges, and inmate populations.

7. **Beef up the security measures at home.**

The measures you employ at work should also be considered to make your home safer. Do you have adequate exterior motion-sensor lighting? Have you installed deadbolt locks on your doors that are "pick" and "bump" proof? Do you have a "safe room" with a solid core door and deadbolt to barricade yourself inside and await help in an emergency? Is there an alarm system that has sensors on all exterior doors and windows? Do you and your family members activate it every time your home is occupied and unoccupied? Is it hard-wired? Is there a monitoring

service available to dispatch the police? Do you have a surveillance system to continuously record what is happening around the perimeter of the house? Does this system provide Internet password-protected access and viewing capabilities through a smartphone or similar device?

8. **Utilize all available privacy protection techniques.**

Meaningful privacy protection, namely being able to "hide in plain sight," should be the first, and not the last or only, line of defense. Privacy protection is important even in small communities. Potential stalkers or attackers could be strangers from out of town as well as locals. Keeping an unlisted phone number is important, as is maintaining a post office box, rather than having your name and home address listed on your checks, correspondence, and bills. Consider doing the following:

- Hold title to your residence in a trust not containing your last name to avoid being discovered by someone simply searching public records. You should confer with counsel before creating the trust to avoid potential tax consequences.
- If your state permits it, apply for home address and telephone confidentiality on public records such as your driver's license and registration, voter record, marriage license, etc.
- If possible, opt out of all Internet postings that display your home address, telephone number, or other personal identifying information. Over the last decade, California has enacted some of the most advanced privacy protection laws for "public safety officials" in the nation. These laws were enacted in response to the 1999 murders of Los Angeles Superior Court Commissioner George Taylor and his wife Lynda at their home. California public safety officials have the right to have their home addresses and home and cellular telephone numbers removed from Internet websites. The failure to comply with a public safety official's written demand to remove his or her home address and telephone numbers from the Internet website puts the information data vendor at risk for civil damages of a minimum of $4,000, up to treble damages, attorneys' fees, and injunctive relief. Intentionally posting the home address or telephone number of a public safety official on the Internet with the specific intent to cause intimidation or harm is a felony/misdemeanor. (See CA Gov. Code § 6254.21 et seq.) If your state does not have similar privacy protections, consider motivating your association to lobby your state's legislature or congress to enact these types of protections.
- There are two types of information on the Internet to be concerned about: personal identifying information and threats or inappropriate communications. Most sites offer ways to "opt out" from having your personal identifying information displayed. In addition, law enforcement can investigate and attempt to remove inappropriate, threatening, or dangerous communications, but it generally cannot keep personal information completely off the Internet. According to Carl Caulk, U.S. Marshals Service Deputy Assistant Director for Judicial Security, social networking sites belonging to a protectee, family member, or staff member are a constant source of concern and vulnerability to protected officials. Since these are private sites, they need constant self-policing. Often, sensitive information such as personal schedules or future plans of a judge or family member are broadcast, not to mention photographs that are placed on the site by family or friends. This type of information is particularly dangerous in the hands of a stalker.

Essentially, the aforementioned protective modalities incorporate what law enforcement and military personnel call getting off the "x," or bull's eye. The idea is to move and place time and distance between you and an attacker, be it inches, feet, or miles. Education, protective investigations, and intelligence techniques are ways to protect you when on the "x." However, attackers can't hit what they can't find. Privacy protection and hidingin plain sight are goals, but when you can't totally become invisible, you should try to move off the "x" even by staggering entrance and exit times and routes of travel, and by not engaging in routines where patterns of your behavior become predictable to the attacker.

Partnering with judicial and law enforcement entities has been a force multiplier when it comes to protective intelligence information sharing. These multipliers have strengthened the American justice system. Communication and collaboration among marshals and state entities have resulted in greater awareness and readiness on both levels. Marshals are members of the National Sheriff's Association (NSA) and International Association of Chiefs of Police (IACP) and present at their national conferences. Executives from the NSA and the IACP hold membership with federal and state judges on the Executive Advisory Committee of the U.S. Marshals Service's National Center for Judicial Security, a national think tank on best practices for security and safety in the courts. The AOUSC has

funded two educational "Project 365" security videos. These videos were designed to educate judges, their families, and law enforcement on how to lower their profiles, as well as raise their security awareness, and they were produced using federal and state judges, marshals, and sheriffs.

The recent tragic shooting in Tucson and the murders of Commissioner Taylor, his wife Lynda, and Judge Lefkow's husband, Michael, and mother, Donna Grace Humphrey, have all been seminal events highlighting the profound importance of protecting the court system, its judicial officers, and their loved ones. These events have led to comprehensive and positive protective mitigation strategies. As a result of these horrific murders and attacks upon our system of justice, stronger bonds, friendships, and new partnerships have been and continue to be forged, laws passed, and strategies shared. These measures have helped make our justice system safer and have intrinsically improved the quality of justice provided by our courts.

John F. Muffler is the Administrator of the National Center for Judicial Security, U.S. Marshals Service Headquarters, Washington, D.C. He has a master's degree from St. Joseph's University, is a faculty member of the National Judicial College, and has conducted security assessments and speaking engagements worldwide on judicial protection. He can be reached at john.muffler@usdoj.gov. Judge James R. Brandlin has been a judge for more than 18 years and serves as the chair of the Los Angeles Superior Court's Judges Security Committee. He is a retired Santa Barbara County Sheriff's Deputy and Los Angeles County Deputy District Attorney. Judge Brandlin teaches privacy protection and personal security techniques to judges and law enforcement personnel across the country. He has authored six privacy protection bills for CA Public Safety Officials. He can be reached at 310-222-8868 or jbrandlin@lasuperiorcourt.org.