U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

BULLETIN

Bureau of Justice Assistance

Protecting Judicial Officials: Implementing an Effective Threat Management Process

Overview

A successful threat management process consists of 10 basic elements, each integral to all the others. They compose the golden rules of contemporary threat management and demonstrate how the judiciary can identify, assess, investigate, and manage risks of violence to judicial officials. Following these 10 rules will allow the judicial threat manager to implement an effective threat management process.

10 Golden Rules for Effective Threat Management

Rule 1. Recognize the Need for a Threat Management Process

Rule 2. Assign Responsibility of Managing Cases to Trained Threat Managers

Rule 3. Provide Training for and Establish Liaison With Protectees and Court Staff

Rule 4. Create an Incident Tracking System With Well-Documented Files

Rule 5. Establish Liaison With Other Agencies

Rule 6. Use Consistent and Valid Threat Assessment Methods

Rule 7. Conduct Thorough Fact Finding

Rule 8. Apply Threat Management Strategies Flexibly and Intelligently

Rule 9. Communicate With Protectees in a Professional, Confident, and Competent Manner

Rule 10. Manage Cases Appropriately

Domingo S. Herraiz, Director
www.ojp.usdoj.gov/BJA
June 2006

BJA Bureau of Justice Assistance

Rule 1. Recognize the Need for a Threat Management Process

Courts resolve disputes. They provide a neutral arena for judging emotionally charged controversies. Disputants bring their quarrels before the bench. Each wants his or her claim sustained, each requests vindication. Most who stand before the court ultimately accept the court's rulings, however adverse to their own interests. But some will not and only care for the result that most benefits them. When these individuals' views clash with the court's decision, violence may result.

Why do courts need threat management programs? Because angry individuals, once denied their own sense of justice, may turn to violence for exoneration, vengeance, or even salvation. They may direct their anger, revenge, and fears at the officials who personify the judicial process: the judges, prosecutors, clerks, and others who work within the system. So it is no coincidence when these attacks occur at the courthouse, as the building itself symbolizes both dispensed and desired justice. Without a competent threat management process to identify, assess, and manage potential threats, the justice system risks missing any opportunity to intervene and defuse the situation.

In addition, the number of these disgruntled individuals appears to be growing. Reports at the federal level show a steady increase throughout the 1990s in inappropriate communications or contacts (IC&Cs) directed toward federal jurists. The number of IC&Cs reported to the U.S. Marshals Service rose from a couple of hundred a year in the early 1990s to more than 700 in 2004. Since 1979, three federal judges have been killed. In March 2005, a former claimant and suspect confessed to killing a federal judge's husband and mother. Prior to 1979, only one federal judge was killed.[1] Clearly, a ground shift occurred that resulted in a significant increase in the risk to federal judicial officials.

No comparable national data have yet been compiled on the risks to state and local judicial officials. Informal research by the National Sheriffs' Association (NSA) suggests that during the past 35 years, eight state or local judges have been killed. Another 13 were physically assaulted. Three local prosecutors were killed, four assaulted. At least 5 law enforcement officers have been killed at local courthouses, 27 assaulted. At least 42 court participants have been killed at local courthouses and 53 assaulted. In March 2005, a Fulton County, Georgia, jail prisoner delayed his escape long enough to seek out the judge presiding at his trial. After overpowering a deputy sheriff, he killed the judge and a court reporter in the courtroom, then killed another deputy sheriff outside the courthouse.

Risks to State and Local Judicial Officials: The Past 35 Years

- 8 state or local judges have been killed.
- 13 state or local judges have been physically assaulted.
- 3 local prosecutors have been killed.
- 4 local prosecutors have been assaulted.
- 5, if not more, law enforcement officers have been killed at local courthouses.
- 27 law enforcement officers have been assaulted at local courthouses.
- 42 court participants have been killed at local courthouses.
- 53 court participants have been assaulted at local courthouses.

A 1999 survey of 1,029 Pennsylvania state judges found that 51.8 percent reported being the target of

[1] Calhoun, Frederick S. 1998. *Hunters and Howlers: Threats and Violence Against Federal Judicial Officials in the United States, 1789–1993.* Arlington, VA: U.S. Department of Justice, U.S. Marshals Service.

an IC&C sometime during the previous year. In addition, more than 25 percent of the 1,029 state judges were physically approached, 1.2 percent were assaulted, and—more disturbing—more than one-third admitted that they had changed their judicial conduct as a result of the experience. Judges compelled to change their judicial conduct may sacrifice justice for security. The risk extends beyond the individual jurists and goes directly to the ability of government at the state, local, or federal levels to ensure justice to its citizenry. Attacks on the judiciary are assaults on the system of justice—one of the most crucial elements of democratic self-government.

Rule 2. Assign Responsibility of Managing Cases to Trained Threat Managers

Establishing a threat assessment process must be emphasized, rather than a threat management unit or program, because a specific composition or quantity of resources should be determined locally. Depending on the size of the court, potential number of IC&Cs that might be reported, and number of cases that might be opened, the threat management process can be handled by a fully staffed unit of threat managers or by one person as a part-time collateral responsibility. Workload should be the principal criterion for determining the number of personnel and resources dedicated to the process.

Whatever the size or composition, whoever is assigned threat management responsibilities should be trained, and the training should be refreshed periodically. A number of organizations provide threat management training, and there is a growing library of research, articles, and books on contemporary threat management that can be accessed to better prepare staff. In addition, agencies and organizations, including the Office of Justice Programs' Bureau of Justice Assistance, are reexamining concepts such as "secure by design" to determine their role in this crime prevention arena.

Rule 3. Provide Training for and Establish Liaison With Protectees and Court Staff

The next step in establishing an effective threat management process is to train court staff in what to report and how to report IC&Cs. Training staff helps the threat manager obtain the initial facts, unembellished by exaggeration or worry, as quickly as possible. Although key staff like judges, prosecutors, and chief clerks should be well trained, the majority of reports the threat manager will receive will come from receptionists, mail handlers, perimeter security officers, parking lot attendants, telephone operators, cafeteria staff, and the newsstand operator. These are the people who deal most with the public. They are more likely to see, hear, or receive any IC&Cs, no matter who is targeted. Training them on what information to report and how to report it will ensure that the threat manager gets reports on IC&Cs in a timely and accurate manner.

Rule 4. Create an Incident Tracking System With Well-Documented Files

Controlling the flow of information requires information management. Depending on workload, managing the information may require something as simple as an index card system or as sophisticated as a computer database. The system needs to be designed to retrieve information quickly and efficiently. It should include not only demographics on the subject, but also key words used by or topics of known interest to the subject. The latter may prove crucial in identifying anonymous subjects. At a minimum, the following variables should be captured for each IC&C:

- Case synopsis.
- Case specifics.
- How the IC&C was delivered.

- Content of and exact quotes from the IC&C.
- Suspect's demographics.
- Target's demographics.
- Suspect's motive, especially in relation to a court case.

With information on these variables, the threat manager can manage current cases, cross-reference previous cases, share information on contentious cases or problem individuals as a case works its way up the appellate process or across jurisdictions, and create an institutional memory for that judicial setting. Whatever system is created, it should be designed for easy sharing with other agencies and jurisdictions, ideally as part of regional and national information-sharing networks.

Rule 5. Establish Liaison With Other Agencies

It is absolutely vital for the threat manager to reach out beyond the courthouse to make contact with law enforcement agencies, private security firms that provide protective services, and other judicial entities. The threat manager must have information flowing from all sources, both inside and outside the courthouse, because only through information can the threat manager begin to fill in the pieces of the puzzle. Information from disparate sources can link one IC&C to another and reveal relationships, motives, past behaviors, and previous actions of the subject—in and out of court.

Rule 6. Use Consistent and Valid Threat Assessment Methods

After receiving the initial IC&C report and gathering as many facts as are immediately available, the threat manager must next make an initial assessment from which to design the immediate protective response, set a course of fact finding, and begin identifying the most appropriate threat management strategies. A number of experts have developed some facile assessment tools to help the manager think through the case. For example, there are now tools that provide a comprehensive approach when used together. Threat managers can apply each tool in every assessment, as each allows the threat manager to examine what is known from a different angle. In combination, they provide a thorough assessment of the entire situation. Employing all of these tools helps the threat manager identify what is *not* known, thus giving direction to the protective fact finding.

These assessment tools address four broad but related questions. In each case, the threat manager should always ask:

- What are the circumstances surrounding and context of the IC&C?
- What stakes are involved, from the subject's point of view?
- Is the subject acting like a hunter?[2]
- Is the subject acting like a howler?[3]

Each of these questions focuses on different aspects of the subject's behaviors, motive, and intentions. The first question simply requires the threat manager to describe the IC&C, how it was delivered, to whom it was delivered and directed, what message it says or conveys, and what may have prompted it. The second question deals with what may be at stake in any court case involving the subject. It addresses how desperate or driven toward violence the subject feels. The third question seeks to determine if the subject has engaged in behaviors common to attackers or assassins. The fourth question takes the opposite

[2] Hunters are people who attack without threatening.

[3] Howlers are people who threaten without ever attacking.

tack and asks if the subject's behaviors compare similarly to the way nonattackers behave.

Rule 7. Conduct Thorough Fact Finding

Protective fact finding focuses on collecting facts concerning the circumstances of the IC&C and what prompted it, the subject, the target's relation to the subject, the subject's past behaviors, and the subject's current behaviors. The purpose is to gather enough information and evidence to support an accurate and complete reassessment of the potential risks and the best way to defuse them. The judicial setting contains two valuable aspects, each of which offers a distinct advantage to the threat manager.

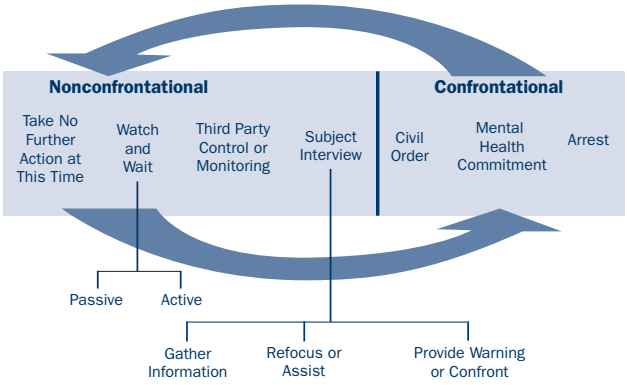
First, the target and his or her staff can be an invaluable source of information about the subject, the subject's issues and motive, and the subject's demeanor under stress. For instance, because most IC&Cs to judicial officials are initiated by a court case, the target frequently has some knowledge or suspicion about the subject and knows the details of the case. Often, court employees have observed how the subject behaved in court. In addition, court records are readily available in the clerk's office. Reviewing the records of the case may educate the threat manager about the issues and motivations that may have prompted previous and/or future inappropriate or even dangerous actions or behaviors.

Second, the threat manager should remember that, from the subject's point of view, the courts may be threatening to the subject. The IC&C might be a defensive reaction prompted by some action or potential action by the court. The judiciary has the authority to take an individual's freedom, home, and assets. It can order an individual to stay away from former spouses and loved ones. It can punish expressions of contempt. People driven to desperation often act desperately. Information for assessing how desperate the subject may feel is readily available from the case files, the target, the IC&C, court staff who have dealt with the subject, and the subject's friends and family, as well as through interviews with the subject.

Rule 8. Apply Threat Management Strategies Flexibly and Intelligently

The strategies for defusing the risk to judicial officials are best conceptualized as different options arrayed along a spectrum, where each option falls within the range that is determined by the option's effect on the subject. The spectrum reaches from discreet, passive defensive measures at one end to intrusive, confrontational acts at the opposite end. The strategies run the gamut from doing nothing that directly affects the subject to using the authority of the law to restrain the suspect. The figure below illustrates the range of threat management strategies available for defusing the risk to judicial officials.

Figure 1: Threat Management Strategies



The threat manager should consider all of the strategies, weighing the effectiveness of each given the particular and unique aspects of the case at

hand. Each one has specific advantages and disadvantages, and each should be used only when certain conditions apply. The threat manager must determine which one offers the best chance for defusing the risk in the case at hand at that particular moment. Once a strategy has been identified and implemented, the threat manager should immediately recognize that the situation has changed *precisely because a strategy has been employed.* The change requires reevaluating the case, assessment, and strategy, which may result in using other strategies.

Rule 9. Communicate With Protectees in a Professional, Confident, and Competent Manner

The threat manager should take care, by word and deed, to reassure the target and his or her staff that the threat manager is a professional problemsolver and that the responses to the incidents are under control. In implementing the appropriate protective responses, the threat manager should never increase the protectee's and staff's fears by projecting the wrong attitude or sharing information they might misinterpret. Frequent updates and open lines of communication with the protectees and their staff will help the threat manager keep them calm, attentive to instructions, and willing to follow the threat manager's lead. Judges, counted on to "be in charge," are frequently tempted to take charge. This should be avoided.

The threat manager should always provide some protective response every time an IC&C is reported. Protective responses range from providing a security briefing at a minimum to a full-fledged protective detail or target relocation at the maximum. The selection of the appropriate protective response should be directly proportioned to the assessment and findings of any protective investigation.

Always providing some level of protective response serves two purposes. First, it enhances the protectee's security. Even a security briefing reminds the protectee to take simple precautions and be aware of and immediately report any suspicious incidents. Naturally, going up the scale of protective responses adds even more security. Provided that each response is in proportion to the threat assessment, the results of the protective fact finding, and the success of the threat management strategies, the threat manager will maintain a balance between needed security and limited resources.

Second, always implementing some degree of protective response sends a positive signal to the protectee. It helps underscore the threat manager's professionalism, competence, and concern. That signal will help allay the protectee's fears and give him or her the reassurance that everything necessary is being done.

Rule 10. Manage Cases Appropriately

Threat management cases are seldom open and shut. They begin when an IC&C, not necessarily a crime, has been directed toward a protectee. But unlike criminal cases, they have no climactic point of closing. Even the most blatant and direct threatener can be arrested and convicted of that crime but continue threatening or, worse, plotting, from jail. An anonymous subject may direct an IC&C toward a judicial official, then never be heard from again. When can either case be closed? Neither arrest and conviction nor time's cooling effects seem enough to support case closure.

Threat management cases are not about investigating or solving crimes. They are about managing an

individual's behavior. Threat managers do not have a caseload of crimes assigned to them. Rather, threat managers are assigned problem individuals. Consequently, a threat manager's caseload is a hybrid between a criminal caseload and a parole or probation officer's caseload.

Hence, it is recommended that threat managers avoid the terminology that has been historically used when opening or closing a threat management case. Instead, it is preferred that cases be designated as one of the following:

- Active.
- Inactive.
- Chronic or habitual.
- Long term.

These designations are best suited for handling threat management cases.

Contemporary threat management for judicial officials seeks to avert violence altogether. The judiciary must expand its security from simply fortifying courthouses and reacting to violent attacks. It needs to incorporate an effective threat management process for defusing the risk of violence before the violence erupts. An effective threat management process does not infer the ability to predict violence. Instead, it entails establishing procedures to enable the threat manager to identify potential problem individuals, assess the seriousness of the risk, investigate the circumstances, and then devise the appropriate strategies for managing the subject. Implementing an effective threat management process requires the judiciary to follow the "10 golden rules." Doing so will further enhance the judiciary's security.

Bureau of Justice Assistance Information

BJA's mission is to provide leadership and services in grant administration and criminal justice policy to support local, state, and tribal justice strategies to achieve safer communities. For more indepth information about BJA, its programs, and its funding opportunities, contact:

Bureau of Justice Assistance
810 Seventh Street NW.
Washington, DC 20531
202–616–6500
1–800–859–2687
Fax: 202–305–1367
www.ojp.usdoj.gov/BJA
E-mail: AskBJA@usdoj.gov

The BJA Clearinghouse, a component of the National Criminal Justice Reference Service, shares BJA program information with federal, state, local, and tribal agencies and community groups across the country. Information specialists provide reference and referral services, publication distribution, participation and support for conferences, and other networking and outreach activities. The clearinghouse can be contacted at:

Bureau of Justice Assistance Clearinghouse
P.O. Box 6000
Rockville, MD 20849–6000
1–800–851–3420
Fax: 301–519–5212
www.ncjrs.gov
Questions/Comments: www.ncjrs.gov/App/ContactUs.aspx

Clearinghouse staff are available Monday through Friday, 10 a.m. to 6 p.m. eastern time. Ask to be placed on the BJA mailing list.

To subscribe to the electronic newsletter *JUSTINFO* and become a registered NCJRS user, visit *www.ncjrs.gov/subreg.html.*

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

This document was prepared by the National Sheriffs' Association via funding from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Additional Resources on Protecting Judicial Officials

This publication was written by **Frederick S. Calhoun** and **Stephen W. Weston** and based on the authors' book, *Defusing the Risk to Judicial Officials: The Contemporary Threat Management Process.* Mr. Calhoun was the lead researcher and principal architect in developing the threat assessment process used by the U.S. Marshals Service for analyzing risks to federal judicial officials. At the request of the National Sheriffs' Association, Mr. Calhoun also coordinated a curriculum and led a nationwide training program on contemporary threat management for local law enforcement.

Mr. Weston is a 31-year veteran of California law enforcement. Since 1991, he has been the supervisor of a specialized unit responsible for the investigation of threats against California state officials. Mr. Weston also is on the faculty of California State University, Sacramento, in the Criminal Justice Division.

For information about available threat management training, visit the Bureau of Justice Assistance's training and technical assistance web page at www.ojp.usdoj.gov/BJA/tta/index.html. The National Sheriffs' Association (www.sheriffs.org) and Specialized Training Services (www.specializedtraining.com/index.htm) also provide exceptional trainings, seminars, conferences, and home-study programs. And the national chapter of the Association of Threat Assessment Professionals (www.atapusa.org) holds annual conventions in Southern California every August, while its local chapters host 1-day seminars in various cities throughout the year. These organizations, as well as the library of research, articles, and books on contemporary threat management, are what will keep best practices in the forefront and judicial officials safe.

NCJ 213930