June 2003
Volume 72
Number 6

**United States
Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001**

**Robert S. Mueller III
Director**

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 935 Pennsylvania Avenue, N.W., Washington, D.C. 20535-0001. Periodicals postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

Internet Address
leb@fbiacademy.edu

Cover Photo
©stockbyte

Send article submissions to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

FBI Law Enforcement Bulletin

Features

The New ViCAP
By Eric W. Witzig
1
The New ViCAP has enhanced technology to assist agencies attempting to solve violent crime cases.

Police Work Addiction
By Gerard J. Solan and Jean M. Casey
13
Being too dedicated to the profession can cost law enforcement officers their families, friends, and, ultimately, their lives.

A Four-Domain Model for Detecting Deception
By Joe Navarro
19
Investigators can focus on four domains to help them detect deception during interviews.

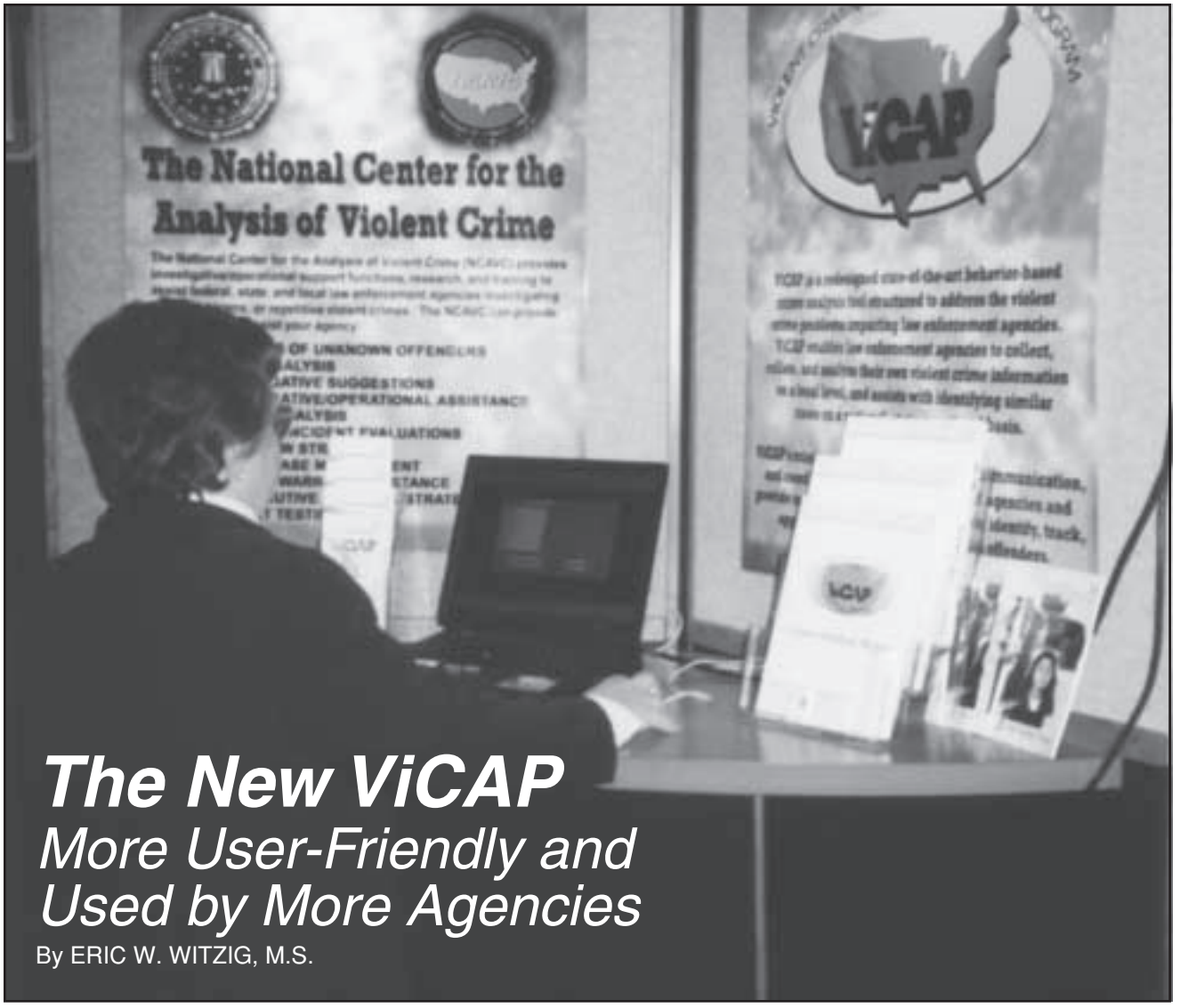
Foreign Intelligence Surveillance Act
By Michael J. Bulzomi
25
The FISA and USA PATRIOT Act provide oversight to law enforcement officers investigating terrorist and intelligence cases.

Departments

8 **Perspective**
Career Criminals, Security Threat Groups, and Prison Gangs

18 **Book Reviews**
Practical Law Enforcement Management

ISSN 0014-5688 USPS 383-310



The New ViCAP

More User-Friendly and Used by More Agencies

By ERIC W. WITZIG, M.S.

Where should officers go to obtain information about unsolved violent crime cases? Where do they direct their inquiries? Who do they ask? Officers in small departments might ask their colleagues during morning roll call. Those in mid-sized agencies might question investigators working other shifts. Personnel in large departments might ask officers in the next jurisdiction by sending a teletype or similar communication.

Yet, the communication might not reach the employees who have the necessary information. Generally, personnel who need information about violent crime cases do not connect with the investigators who have that knowledge. Information technology (IT) has enhanced communication for law enforcement, allowing departments to close violent crime cases with the arrest of an offender.

ORIGIN OF VICAP

The Violent Criminal Apprehension Program (ViCAP)[1] originated from an idea by local law enforcement and the late Pierce Brooks.[2] In 1956, Mr. Brooks investigated the murders of two Los Angeles women who had replied to an advertisement for photographic

> ***"...a tremendous change has occurred in the way ViCAP now provides services to state and local law enforcement."***

Mr. Witzig, a former detective in the Homicide Branch of the Washington, D.C., Metropolitan Police Department and agent of the chief medical examiner for Washington, D.C., is a major case specialist with the FBI's Violent Criminal Apprehension Program.

models. Their bodies, tied with rope in such a fashion as to suggest that the killer might practice bondage, subsequently were found in the desert.

Mr. Brooks, convinced that these were not the killer's first murders and that the offender would kill again, devised an early form of ViCAP. For 18 months, he used his off-duty time to visit the Los Angeles central library and read out-of-town newspapers to look for information on murders that exhibited characteristics similar to those he was investigating. He found such an article in a newspaper and, using pieces from that case coupled with evidence from his own cases, arrested an individual who subsequently was tried, convicted, and executed for the murders.

Mr. Brooks refined his idea and concluded that a computer could capture relevant information about murders. If open and closed cases were stored in the computer, investigators easily could query the database for similar ones when they first confront new, "mystery" cases. They could use clues from other cases that exhibit similar characteristics to solve more cases. Moreover, when officers identify offenders, a search of the computer using their modus operandi (MO) would reveal other open cases for which they might be responsible.[3]

In 1983, the Office of Juvenile Justice and Delinquency Prevention and the National Institute of Justice gave a planning grant, the "National Missing/Abducted Children and Serial Murder Tracking and Prevention Program," to Sam Houston State University in Huntsville, Texas. After three workshops, with the last held in November 1983, the National Center for the Analysis of Violent Crime (NCAVC) emerged. The U.S. Department of Justice provided the initial funding for the NCAVC and stipulated that it would be "...under the direction and control of the FBI training center at Quantico, Virginia."[4]

ViCAP became a part of the NCAVC with its goal to "...collect, collate, and analyze all aspects of the investigation of similar-pattern, multiple murders, on a nationwide basis, regardless of the location or number of police agencies involved."[5] Mr. Brooks envisioned ViCAP as a "nationwide clearinghouse...to provide all law enforcement agencies reporting similar-pattern violent crimes with the information necessary to initiate a coordinated multiagency investigation."[6] ViCAP attempts to identify similar characteristics that may exist in a series of unsolved murders and provide all police agencies reporting similar patterns with information necessary to initiate a coordinated multiagency investigation.[7]

REDESIGN OF VICAP

Since ViCAP's beginning at the FBI Academy in July 1985, its goal of identifying cases exhibiting similar characteristics and providing that information to law enforcement agencies for a coordinated, case-closing investigation has remained constant. But, a tremendous change has occurred in the way ViCAP now provides services to state and local law enforcement. In 1996, a business analysis revealed several details about ViCAP.[8]

- Only 3 to 7 percent of the total cases were reported each year. Of the 21,000 homicides (average) reported per year in the 1990s,[9] only about 1,500 to 1,800 were submitted to the nationwide database.

- An urban void existed. While most murders occurred in large cities, the cities were not contributing their homicides to the nationwide database.
- ViCAP users reported that the 189-question ViCAP form was cumbersome and difficult.
- Users perceived that ViCAP case submissions entered a bureaucratic "black hole" never to emerge or be seen again.
- Chronic understaffing caused a failure to address incoming case work on a timely basis.

The beginning of the ViCAP change originated with the 1994 crime bill. Legislation in this bill directed the attorney general to "...develop and implement, on a pilot basis with no more than 10 participating cities, an intelligent information system that gathers, integrates, organizes, and analyzes information in active support of investigations by federal, state, and local law enforcement agencies of violent serial crimes."[10]

From the business analysis, ViCAP learned that the program had to be placed in the hands of state and local law enforcement. This concept of program delivery required two conditions of ViCAP software: 1) migration of the application from a mainframe computing environment to a platform more affordable by state and local law enforcement and 2) a choice of software that eliminated the need for a computer programmer to extract information from a database. To accomplish these objectives, ViCAP had to create a powerful, object-oriented, user-friendly, software seamlessly integrating data, mapping, reporting, and image-capturing tools. This high-end software would have to operate on a modestly priced desktop computer. Crime bill monies provided the initial funding to create completely new software for ViCAP and to move it as an application from a mainframe to a client-server environment.

ViCAP decided that users of the new ViCAP software would receive the service free of charge. Moreover, ViCAP loaned high-end computers loaded with the new software to more than 50 law enforcement entities. These computers had a modem that enabled users to exchange information with each other and forward case information to state hubs where it was downloaded to the national database. A memorandum of understanding (MOU) formalized the conveyance of new ViCAP software, the loan of a desktop computer to participating agencies, and

Case Example: Victim by the Lake

In 1996, a suspect in a drug case in a northeastern state made an offer to the authorities—in exchange for leniency in his prosecution or at the time of his sentencing, he would give information linking his brother to a murder. He advised that a white male in a southeastern state died from repeated strikes with a blunt object. The investigators questioned the suspect about where the crime occurred, and the suspect advised that he did not know the exact location, but that he thought it happened near a body of water. Further, the suspect advised that his brother ran over the victim with an automobile.

Investigators from the northeastern state contacted ViCAP and related the details of the case as told to them by the suspect. A crime analyst searched the ViCAP database and found a case from 1986 in a southeastern state that matched the details offered by the suspect in the drug case. The victim's cause of death was blunt force trauma, and he was run over by an automobile. Further, the murder occurred near a small lake. Authorities in the northeast with the information contacted investigators in the southeast with the open homicide case. The southeastern case successfully was closed with the identification and arrest of the offender.[11]

Case Example: Texas Railroads

In 1999, a series of homicides occurred in Texas. Early in the series, the cases were presented as murders in the victims' homes. Female victims were sexually assaulted, blunt force trauma was the cause of death,[12] and items of value were stolen from the homes.[13] The murder scenes were close to railroad tracks, sometimes only a few feet away.

In May 1999, personnel from the command post in Texas called ViCAP with information about three of the murders. One of the ViCAP crime analysts remembered a case from Kentucky where railroad tracks were prominently mentioned. The analyst searched the database and quickly found the case in Kentucky where a male was killed along a pair of railroad tracks. The cause of death was blunt force trauma.[14] His female companion was sexually assaulted and left for dead. ViCAP relayed information concerning the Kentucky rape/homicide to the command post in Texas. Subsequent DNA examinations linked the Texas cases with the Kentucky case.

An itinerant freight train rider was identified as the suspect in the series of cases.[15] He was apprehended by authorities on July 13, 1999, when he surrendered at the border in El Paso, Texas. Charged with nine murders, two in Illinois, one in Kentucky, and six in Texas,[16] the subject was tried, convicted, and sentenced to death.

In July 2000, he confessed to the 1997 murders of two teenagers on a railroad track near Oxford, Florida.[17] The male victim's body was found on March 23, 1997; the female victim's body was not found until July 2000, when authorities, following the killer's directions, found her skeletal remains wrapped in a blanket and jacket.[18]

While confessing to the two murders in Florida, the subject said that he once killed a woman in a southeastern state, somewhere along railroad tracks. She was an old woman, hanging her wash on the line, and he killed her inside her house. He did not provide more details.

A check of the ViCAP database revealed a 1998 case from a southeastern state where an elderly woman was hanging laundry in her backyard just a few feet from a pair of railroad tracks that ran by her property. The command post in Texas and the investigator in the southeastern state were notified of the case match. When interviewed by the investigator, the subject confessed in detail and drew a diagram of the inside of the victim's house. In this case, no fingerprint or DNA evidence matched the defendant to the murder.

these agencies' relationship with ViCAP.

Additionally, the 189-question ViCAP form was completely redesigned, streamlined to only 95 questions, and became more appealing to the eye. The paper form both looked and became more user-friendly.

In 1998, Congress provided additional funding for ViCAP crime analysts. Today, 19 well-trained and experienced crime analysts serve with ViCAP, and they address incoming work and requests on a more timely basis. They handle high-profile or immediate case requests rapidly, frequently within the same hour or day. In a symbolic, but important, perceptual break with the old ways of doing business, ViCAP reflected its new software and energy with a new name—the New ViCAP.

THE NEW VICAP

Some agencies run the New ViCAP system in their own departments, others prefer to run the software on a stand-alone desktop, and several put the software on their internal networks. Agency networks support as few as three users, through the entire investigative staff, and up to five different boroughs and the precincts therein. New ViCAP software operating in

participating agencies allows direct access to all of the information that they enter and the ability to perform their own crime analysis.

Cold case squads can store their cases without resorting to wall-filling filing cabinets. With just a piece of information, a nickname, an address, or the name of a bar or other business, investigators can retrieve decade-old cases for additional investigation. Conversely, cold case squads looking for cases exhibiting an MO used by a suspect, or a series of cases matching a particular MO, can make those searches as well.

Research has shown that administrators like the reports package in New ViCAP. Standard reports include—

- cases by day of the week, month, or district;
- case status (open or closed);
- causative factors;
- offender age or ethnicity;
- victim age or ethnicity;
- victim-offender relationship; and
- all weapons used or firearms used by caliber or type.

Perhaps most useful to administrators and investigators is the one-page New ViCAP summary report, which collects the main facts from a violent crime and prints them to the screen or, typically, two sheets of paper. The summary report proves an excellent briefing tool for administrators, managers, or elected officials.

Some investigators and prosecutors like to have all of the information about a case in one place, but the concept of electronic storage of case information proves unsettling to some people. To overcome this problem, New ViCAP provided a hard copy. This multipage report prints on screen or on paper and includes all of the information entered into the database. The printed document can be placed in the case folder or jacket and preserved indefinitely.

> ***"New ViCAP understands that unique cases require distinctive database queries."***

New ViCAP understands that unique cases require distinctive database queries. To provide for discrete, particular questions of the database, the program has a powerful ad hoc query tool, whereby any combination of New ViCAP variables and attributes can be strung together to produce a set of possibly related cases. Refinement of the ad hoc query produces more, or fewer, cases delivered to the crime analyst through the possibilities set. When the listing of cases is returned, the crime analyst can contrast and compare them in a matrix of variables specified by the analyst. Particularly valuable case matrixes can be titled and printed for more formal presentations, such as multiagency case meetings. The ad hoc query and resulting matrix analysis prove a very powerful combination of tools for any analyst examining violent crime.

Sexual Assault Data Collection

Many New ViCAP users have reported that the homicide-oriented version was a helpful crime analysis tool. But, what the users really needed was a crime analysis tool for sexual assaults. ViCAP currently is working on that product by determining data elements for the paper form and the electronic version and designing the paper form for sexual assault data collection to mirror the existing homicide-oriented form. ViCAP is developing the electronic portion of the system in a Web-enabled fashion. This will permit users to exchange information more easily and potentially will provide limited access to the nationwide database.

More Developments

A recent development in New ViCAP is the ability to store one or more images and associate them with a particular case. The images can be photographs scanned into the system or maps or other graphics imported into the system. This tool has important implications for training new investigators, refreshing case-specific recollections of experienced investigators, or exchanging precise information to identify unknown victims.

An envisioned tool, not yet a part of the software, is a mapping capability. New ViCAP already captures graphic information system (GIS) data. This information

could be used for traditional pin maps. Alternatively, investigators could use GIS data to store and search offender time lines like those prepared for suspected or known serial killers. Once offender time lines are stored, GIS data for each newly entered case could be automatically compared with the time lines. For example, an automated hit system could report to the analyst that plus or minus 3 days, a killer was in the town where the murder occurred.[19]

A Communication Tool

Police agencies across the country recognize New ViCAP as a valuable violent crime communication tool. The first pair of cities to use New ViCAP were Kansas City, Missouri, and Kansas City, Kansas. Now, police and sheriff departments in the largest metropolitan areas are using New ViCAP, including Baltimore, Maryland; Chicago, Illinois; Los Angeles, California; Miami, Florida; New York, New York; and Washington, D.C. Further, MOUs and the New ViCAP system are in place with 40 states. More than 400 state and local law enforcement entities use the New ViCAP software.

The architecture of the New ViCAP network is as varied as the needs of its users. For some states, such as Colorado, a "hub and spoke" design works well. MOUs are created between the Colorado Bureau of Investigation (CBI) and cities and counties in the state. Cases can be entered at the local level and uploaded to the state. In addition to its networking arrangements, CBI selected New ViCAP as the statewide tool for sex offender registry.

Other states have implemented a regional model. For example, the Los Angeles County Sheriff's and Los Angeles Police Departments provide an excellent example of regional concept application. The sheriff's department serves as the collection point and analysis hub for cases in the county. MOUs are in place between the sheriff's department and 45 of the 46 police agencies in the county, thus

Case Example: Bag of Bones

In 2001, a ViCAP crime analyst reviewed a state police publication that mentioned a bag of human bones found by hunters in a seaboard forest of an eastern state. The victim was a white male, about 40 to 60 years old, and between 5' 7" and 5' 9" in height. His cause of death was blunt force trauma to the head. Recovered with the remains was a 14-carat gold ring with engraved letters. Authorities had no leads for identification of the remains.

A ViCAP crime analyst searched the database using the physical description of the victim and then made an additional search, thinking that the letters engraved in the ring might be the initials of a name. A possible match was made with a July 1998 case where three people were reported missing from a midwestern state. The report was made by a fourth member of the family, a son, who waited a week before reporting his mother, father, and sibling as missing persons. Personnel had exhausted all investigative leads.

Authorities in the eastern and midwestern states contacted each other. In January 2001, ViCAP learned that forensic odontology had identified the bones in the bag as those of the father missing from the midwestern state. The letters in the recovered ring represented the maiden name of the missing mother and the name of the missing father.

ViCAP learned later that a suspect was identified and charged with the murder—the oldest son who made the report in the midwest. The remains of his mother and his sibling have not been located.

providing a web of case-sharing information for participating law enforcement entities, including the two largest, the police and sheriff's departments.

Data Security

New ViCAP created a standard of information for exchange between law enforcement agencies. Naturally, a law enforcement entity would express concern for violent crime data sent to a national database with information no longer under an agency's direct control. ViCAP recognizes its responsibility to provide security for violent crime case data and has provided that security for more than 16 years. New ViCAP continues to recognize the sensitive nature of violent crime data and provides appropriate security.

CONCLUSION

The FBI's Violent Criminal Apprehension Program Unit has helped local and state law enforcement agencies solve violent crimes for almost 20 years. As technology has improved, ViCAP has ensured that its objectives change to support such advancements. New ViCAP represents an instructional and technological violent crime analysis tool suitable for use in a law enforcement agency of any size. It provides a standard method for the communication of violent crime information between and among agencies.

New ViCAP software is free to agencies that formalize their relationship with a state hub or ViCAP. The software is case-management and case-matching capable with an easy-to-use data retrieval scheme and a package of reports that serves the needs of administrators and commanders. Initially designed for homicide-oriented violent crime, New ViCAP soon will provide an information technology system to capture and analyze sex offenses as well. Forty years after Mr. Brooks' idea of putting all homicides into a computer, law enforcement is on the cusp of making his thinking a practical reality. ✦

Endnotes

[1] ViCAP has been distinguished by several acronyms since its inception. To ensure consistency in this article, the author used the current acronym for the program.

[2] Mr. Brooks was a former commander of the Los Angeles, California, Police Department's Robbery-Homicide Division. See, Bob Keefer, "Distinguished Homicide Detective Dies at 75," *The Register-Guard*, Eugene, Oregon, March 1, 1998, p. 1, in which he wrote that Mr. Brooks investigated the murder of a Los Angeles officer in an onion field outside of Bakersfield, California. Joseph Wambaugh wrote the book *The Onion Field* based on this crime. Subsequently, Mr. Brooks served as a technical consultant to Jack Webb and the television show "Dragnet," as well as "Dragnet 1969," the made-for-television production of the case outlined here.

[3] Author interviews with Pierce R. Brooks, Quantico, Virginia, 1985 and Vida, Oregon, April 1992.

[4] Steven A. Egger, *Serial Murder—An Elusive Phenomenon* (New York, NY: Prager Publishers, 1990), 192-193.

[5] Ibid.

[6] Pierce Brooks, "The Investigative Consultant Team: A New Approach for Law Enforcement Cooperation," (Washington, DC: Police Executive Research Forum, 1981), unpublished report, in Steven A. Egger, *Serial Murder—An Elusive Phenomenon* (New York, NY: Prager Publishers, 1990), 193.

[7] Supra note 4, 193.

[8] Arthur Meister, ViCAP lectures at Quantico, Virginia, 1999-2000.

[9] U.S. Department of Justice, Federal Bureau of Investigation, *Crime in the United States* (Washington, DC: U.S. Government Printing Office, 1991-2000), 8, 13, 14, or 15. In 1991, a high of 24,526 homicides were reported, contrasted with a low of 15,533 reported in 1999.

[10] U.S. Congress, Senate, *Violent Crime Control and Law Enforcement Act of 1993, H.R. 3355 Amendment*, 103rd Cong., 1st sess., 1993, 267-268.

[11] Arthur Meister, ViCAP lectures at Quantico, VA, 1999-2000.

[12] David McLemore, "Aliases, Trainhopping Obscure Suspect's Trail," *Dallas Morning News*, June 17, 1999, sec. A., p. 16.

[13] Pauline Arrillaga, "Town Copes After Slayings by Suspected Rail Rider," *Dallas Morning News*, June 11, 1999, sec. A., p. 29.

[14] Supra note 12, sec. A., p. 17.

[15] Michael Pearson, "Railroad Killer," *Associated Press*, June 22, 1999.

[16] Mark Babineck, "Railroad Killer," *Associated Press*, 2000.

[17] "Railroad Killer," *Associated Press*, July 2000.

[18] Ibid.

[19] This represents an arbitrary number; analysts could select any number of days.

Career Criminals, Security Threat Groups, and Prison Gangs
An Interrelated Threat

By David M. Allender and Frank Marcell

Just after midnight, a young police officer stopped a vehicle unaware that the driver was a gang member recently released from prison, strung out on crystal meth, and resolved not to return to jail. Upon approaching the vehicle, the officer first noticed a female passenger and then saw the driver, wearing a trench coat, quickly exit the vehicle. The officer instinctively knew that something was wrong. He immediately searched the driver and found a .45-caliber handgun in a shoulder holster. A fight ensued during which the driver shouted to the female, "Shoot him, shoot him!" As the officer turned toward the vehicle, he saw the woman in a crouched position, pointing a weapon at him. He immediately drew his service weapon and fired, terminating the threat and the life of this accomplice.

Such incidents occur, sometimes daily, involving individuals who belong to criminal gangs and have served time in prison. Who are these individuals, these "career criminals," who seemingly have chosen crime as a way of life? What are some characteristics that law enforcement officers can learn to assist in identifying them? And, most important, what can officers do to protect themselves and the citizens they serve from such threatening individuals?[1]

Defining the Threat

A broad spectrum of people use the term *gang* to describe diverse groups with a wide range of characteristics. Academicians, police investigators, politicians, researchers, and residents of crime-ridden neighborhoods all have a mental picture based on their experiences of what constitutes a gang. To some, a gang is a loose confederation of neighborhood youths engaged in delinquent activity. Other people refer to gangs as highly structured drug-dealing organizations, and still others form mental images of outlaw motorcycle clubs when they think of gangs.

This brief sketch shows the necessity for, and the difficulty of, achieving a consensus for the definition of the term *gang*.[2] The authors, however, have employed the FBI's definition of a criminal street gang: "A group of people who form an allegiance based on various social needs and engage in acts injurious to public health and morals. Members of street gangs engage in (or have engaged in) gang-focused criminal activity either individually or collectively; they create an atmosphere of fear and intimidation within the community."[3]

When criminal street gangs engage in violence or large-scale illegal pursuits, they threaten the communities where they exist. Criminal street gangs, or sets, operate in neighborhoods throughout the United States. Some are small, whereas others have many members or associates, and all vary greatly in organizational sophistication.

Captain Allender serves with the Indianapolis, Indiana, Police Department.

Mr. Marcell is an executive board member of the National Major Gang Task Force and a jail intelligence supervisor with the Maricopa County, Arizona, Sheriff's Department.

Correctional officers have special concerns when it comes to identifying criminal gang members. To maintain order in the facilities, they must know which groups are in conflict with each other and what threats these sets pose an officer working in the institution. A number of states and the Federal Bureau of Prisons have determined that when an identifiable collection of individuals poses a hazard to order inside their penal systems, they will label these subjects a security threat group (STG). The same situation exists with criminal sets living in open society. For example, the term *community threat group* has emerged as a way to provide a clearer understanding of the hazards these groups represent to American communities.[4]

Individuals labeled as criminal gang or STG members are not "kids" drawn unknowingly into a dangerous situation. Rather, these people pose a viable threat to the safety and security of communities throughout the country. Such individuals, or "career criminals," have chosen to make crime a way of life and seldom worry about the consequences of their actions until after their apprehension. Then, they tend to put all of their efforts into rationalizing or minimizing their crimes in an attempt to manipulate the judicial system.

> **"Prison gangs communicate with persons on the outside in a variety of ways."**

Examining Career Criminals

The career criminal personality may vary broadly and is best left to the clinicians to analyze. The authors, however, have learned that career criminals often demonstrate certain types of behavior, and law enforcement professionals may find this information useful as a predicator to what these criminals are capable of and what to expect when interacting with them. If, indeed, experience is the best teacher, then the authors submit the results of their education as an overview of some of the behaviors exhibited by the career criminals they have encountered.[5]

- Career criminals have no boundaries; they reside in every state. They migrate to communities that afford them opportunities to pursue their criminal activities. They learn of these criminal ventures from other like-minded criminals, or they travel to a new location to avoid police scrutiny, attempting to blend into a new environment.
- Career criminals disdain authority. They often show their contempt through aggressive behavior or words. They can react violently over the slightest perceived provocation, especially when under the influence of alcohol or other drugs. They also have a propensity for sudden physical violence, especially those who have worked their way through the prison system. However, when preparing for or committing crimes, they can be deliberate, calculating, and rational in their actions.
- Career criminals have an acute awareness of their surroundings and possess many survival skills, learned traits during incarceration. They know how to size up a situation quickly to pursue criminal objectives or scam their way out of a situation.
- Career criminals rarely stick to one type of crime. Revolving in and out of county jails and other prisons, they learn how to pursue a multitude of different types of criminal activities.
- Career criminals view themselves with an inflated ego. They even may have contempt for fellow inmates and scorn law-abiding people and authority. They know and use the psychological tactics of fear and intimidation and can switch quickly into this mind-set. While committing a crime, they may have a false sense of invincibility, making them all the more dangerous. Moreover, they continue their criminal enterprises even while incarcerated.

Understanding Security Threat Groups

The authors have observed that during periods of incarceration, career criminals often align themselves with groups or cliques that control illegal activities through force or cunning. They set out to distinguish

themselves from the mainstream inmate population. This explains why STGs are a magnet for career criminals.

Corrections practitioners who have identified STGs within their systems know that the groups' criminal activities extend beyond prison walls. Their success inside a corrections facility largely depends on an infrastructure on the outside to further their criminal enterprises, providing financial assistance and communication (i.e., intelligence). The overriding trait of these like-minded career criminals who comprise these groups is commitment. Upon release from prison, most of these offenders will continue to prey upon the community or those who dare to oppose them.

Recognizing Prison Gangs

Criminal gangs may participate in a wide range of illegal activities. Profits from unlawful actions, like drug dealing, can prove important to the cohesion of a street gang. To realize the desired profits, small, disorganized groups need a reliable drug source or a buyer for large amounts of stolen property. Bigger criminal enterprises, such as prison gangs, may provide the resources sought by a street crew. Managing the source of the illegal profits allows the larger gang to exert influence over street-level operations. Control is further strengthened when the upper-tier gang pays a street-level crew to perform tasks, such as assault or murder. As the connection between the groups solidifies, reputation and rumor can make a prison gang even more powerful, drawing other street-level crews into their sphere of influence.

A hierarchy exists in the criminal gang world.[6] Gangsters typically start out in a street crew, usually in a neighborhood or crowd where they have connections. These associations often will be rooted in family ties or friendship because gangs need both to trust partners in their criminal enterprises and to fraternize with during their social functions. At some point in their lives, criminal gang members eventually may be incarcerated in a local jail and then in a longer-term state or federal facility. If they have a reputation among their peers that indicates their desirability as a candidate for induction into an STG, members inside the facility will approach them. Inmates may remain an associate of an STG or may earn a chance to become a full member. Either way, they will fulfill assignments given to them by the prison gang.

The motivation driving the prison gang member is complex. While many sources have cited the need for protection from predatory inmates, other factors enter in, including the human need to seek acceptance, increased status, and financial profit from gang activities. When gang members are released from custody, they often return to their neighborhoods and renew old associations. They then may reenter the gang subculture, which led to their incarceration. If they return to criminal activity, the contacts made in the prison system will become more important. The prison gang will allow the gangster on the outside to network with other criminals or provide regular secure sources for illegal products, such as drugs. The STG also will serve as protection for others in the gangster's crew when they are incarcerated. The STG even may provide income to the street gang with compensation for missions it assigns.

Because other street gangs will have similar situations, the prison gang can use the same methods to gain influence over a multitude of street crews. STGs will pick which sets they hope to influence and build a coalition. To control the street, a prison gang may withhold the desired product from an uncooperative set while ensuring that a competitor gets ample amounts. A more direct approach might occur, whereby an incarcerated member of an uncooperative gang may suffer an assault orchestrated by the STG. Or, a powerful group may order a cooperative street gang to use violence to force a reluctant clique to conform to the rules as formulated by the STG. In

exchange for the protection and profit associated with cooperation, the street crews will continue to do the bidding of the prison gang. Over time, the relationship may grow strong, but rarely will the prison gang allow a street gang to "patch over" and become members of the STG. For this reason, many more criminal street gangs than prison gangs exist. Criminal street gangsters accepted into an STG normally return to their original gang upon release from prison. Street gang members inducted into an STG will have increased status due to the connections made in prison. Unless they have committed some infraction against the STG, the gangsters will be accepted back into the prison gang during any subsequent incarcerations.

Prison gangs communicate with persons on the outside in a variety of ways. Although corruption is sometimes an issue, the majority of communication methods are legal. Persons unfamiliar with the gang subculture tend to underestimate gangsters. They are not stupid or slow, even though, for the most part, they do poorly in structured educational settings. Criminal gang members have chosen an alternate lifestyle that often engages in illegal activity. Gang members in general, but prison gangsters especially, study and train to improve their crime-related skills. The authors have found that a review of security videos or literature confiscated from gang members can provide evidence of the enormous amount of effort that they put into being gangsters. The literature from most gang members includes some type of coded alphabet, often based upon a foreign language that members must master. For example, some Hispanic gangs use the Aztec language to code their documents. Although learning this language expresses pride in a common heritage, it becomes sinister when used to shield illegal acts from appropriate law enforcement scrutiny.

"Because career criminals have been through the criminal justice system extensively, they become aware of the nuances in corrections settings."

Responding to the Threat

Generally, when criminal justice professionals attempt to assess STGs and prison gangs, they typically focus on group behavior as opposed to the commonalties of individual members. Yet, understanding career criminals, their perceptions, characteristics, and traits as individuals should rank among the most paramount objectives of improving officer safety. This proves especially important when deciding to employ undercover personnel or conduct search warrant application. It also is useful in assessing criminal activity trends or modus operandi patterns within a jurisdiction.

Similarly, during police contacts or in corrections settings, officers must realize that career criminals constantly scrutinize them. The authors have found that these criminals think that they are smarter than criminal justice professionals and attempt to use techniques to take control or manipulate situations. A favorite is the "stare down," an intimidation tactic used to see if an officer will break eye contact and, if so, is seen as a sign of weakness. Also, career criminals may be smooth talking or manipulative in one instant and verbally abusive the next. They may test officers to gauge reaction or see how much they can get away with. Regardless of the tactic employed, officers must remain aware of such techniques and immediately inform subjects of their knowledge and intolerance of such actions.

Corrections officers should know the career criminals in their units and housing locations. Because career criminals have been through the criminal justice system extensively, they become aware of the nuances in corrections settings. They look for security breaches; examine the relationship between staff members and administrators; take into account any staff shortages; and seek ways to access materials, people, or contraband. Career criminals also tend to gravitate to leadership positions within the inmate population or STGs. Therefore, officers should review the institutional files on such inmates to gain insight into their backgrounds. How extensive are their criminal histories? Are there prior charges or convictions for escape or assaulting officers? What

does the psychological profile say about high manipulation or violence potential? Are there any past incarcerations in other state or federal prisons? Corrections officers should find out as much as possible about the criminals they face daily.

Likewise, law enforcement officers should apply these same techniques. If career criminals reside within the community, officers should know who they are and what kind of danger they present. This illustrates the importance of maintaining liaison with parole divisions, departments of corrections, and county jail facilities. These institutions can share important information about such criminals. Are they involved in multiple criminal activities, such as narcotics, armed robbery, and burglary? Are they spontaneous or methodical in their criminal activities? Do they have a history of high violence potential? Were they members of an STG while in prison? Answers to these types of questions can mean the difference between life and death for officers responding to calls for service, executing search warrants, or making traffic stops or other contacts, as illustrated dramatically by the opening scenario of this article.

“If career criminals reside within the community, officers should know who they are and what kind of danger they present.”

In short, to effectively curtail the activities of career criminals and the groups to which they often belong, criminal justice professionals must learn the mind-sets, traits, and characteristics of these offenders. Officers must know how and where to obtain information on these individuals. To this end, communicating this type of information between corrections and law enforcement personnel becomes paramount for the safety of both professional entities, as well as the communities they serve.

Conclusion

A growing trend seems to be developing among prison gangs to organize criminal street crews to facilitate the drug trade. The enormous profits available to those willing to take the risks inherent in this and other lucrative illegal enterprises are leading to a change in the way gangs do business. Other indications exist that imply increasing cooperation among criminal gangs.

Current gang trends, while disturbing, are not unexpected when considering the history of gangs in America and in other countries. Historically, gang activity has flourished during those periods of time when sources of illegal profit were readily available and social conditions encouraged the existence of gangs. The entire criminal justice system needs to educate itself to combat this most recent form of organized criminal behavior and profit. The first important step in this process rests with an exchange of information between the law enforcement and corrections communities that will allow for the tracking of criminals as they increasingly migrate around the country. As the flow of information increases so will the effectiveness of combating such criminal activities. Although the criminal justice system never will stop all criminal activity, gang enforcement is an area where police and corrections, with increased intelligence information sharing, can make a major impact in reducing the interrelated threat posed by career criminals, security threat groups, and prison gangs. ✦

Endnotes

[1] The authors based this article on a research project they participated in that compiled information about gangs obtained from personal interviews with local, state, and federal police officers, as well as officers working in local, state, and federal correctional institutions.

[2] For additional information, see Mike Langston, “Addressing the Need for a Uniform Definition of Gang-Involved Crime,” *FBI Law Enforcement Bulletin*, February 2003, 7-11.

[3] U.S. Department of Justice, Federal Bureau of Investigation, *An Introduction to Violent Street Gangs in the United States*, 2nd edition, 1999.

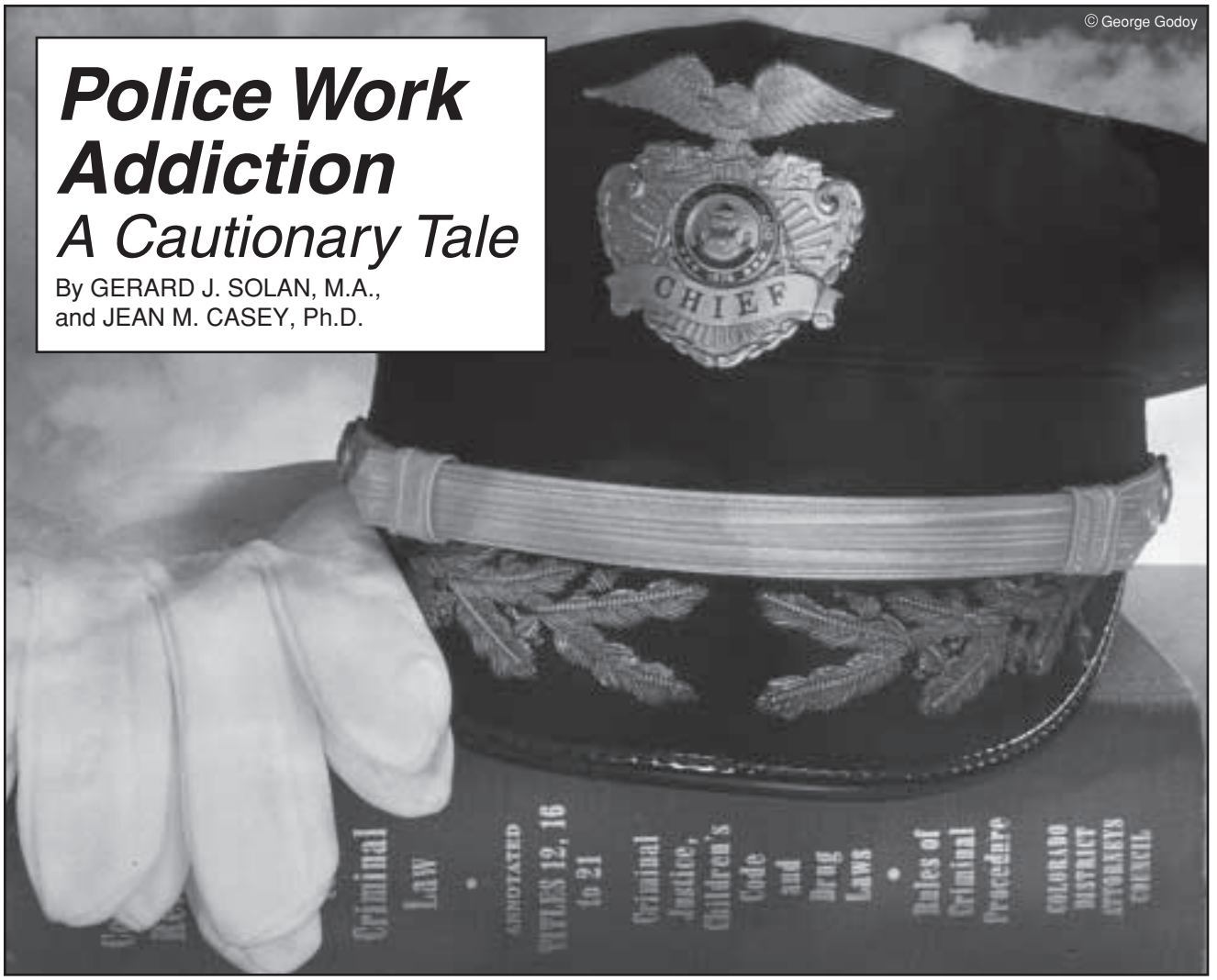
[4] FBI analyst, Safe Streets Gang Unit.

[5] The authors’ education results from their personal interactions with career criminals, security threat groups, and gang members during their many years of working in the criminal justice system.

[6] For additional information on gang structure, see David M. Allender, “Gangs in Middle America: Are They a Threat?” *FBI Law Enforcement Bulletin*, December 2001, 1-9.

Police Work Addiction
A Cautionary Tale

By GERARD J. SOLAN, M.A.,
and JEAN M. CASEY, Ph.D.



Everyone is bound to bear patiently the results of his own example.
—Phaedrus

Great leaders lead by example, and Police Chief William Smith was no exception. He was totally selfless and always available, arriving at his command each morning before eight o'clock and not leaving until everyone else had gone home. It was not uncommon to find him working on Saturday or Sunday. The deputy chief told those assembled at the church that he actually was reluctant to leave each night before the chief. Everyone felt sad that Chief Smith left a young family and even sadder that he should pass away in the prime of his life.

Certainly, police officers are expected to put aside all other needs when duty calls, and, without question, duty does call. Commanders and officers alike must sustain an endless capacity to meet this demand. Communities hold fast to the expectation that the police will do all that can be humanly done and, at times, much more than should be expected of mere humans. Therein lies the great challenge for law enforcement officers and supervisors,

maintaining a healthy balance in meeting *reasonable* responsibilities to the job, to themselves, and to their families.

The Old Covenant

Some in public safety view the aphorism "work ethic," surely a curious juxtaposition of words, as representative of the old covenant. This paradigm celebrates the job above all else. Team players count the most; the job comes first; no sacrifice is too great.

Police supervisors, socialized within this old covenant, operate in a world that expects human carnage as a by-product. Work ethic represents a "code" for doing whatever it takes, and, perhaps, the only ethic involved is the certainty that the job must be done. Lost in this reasoning is the moral responsibility that supervisors hold for the fair and ethical treatment of officers and their families. As a practical matter, getting the job done through people requires consideration of, and for, those very people.

The Price of Work Addiction

Perhaps, Chief Smith represents an extreme example of the dangers inherent in the work-addicted lifestyle. However, literature on work addiction asserts that work constitutes the drug of choice for some 30 percent of the population, for whom working is so vital to their emotional well-being that in fact, they have become addicted to it.[1] While the actual mortality rate for work addiction may be low, the social lethality of this behavior proves overwhelming. These unfortunate individuals are predisposed to involve themselves—and their families—in a life not unlike that of Chief Smith. Clearly, work addicts (or workaholics, the more common descriptor) cannot assess what is important in healthy lifestyle choices and, thus, experience a diminished quality of life. Regrettably, they do not suffer alone. They unwittingly share this pain with their families and colleagues alike.

Workaholics are married to their work. Their vows to love and honor their spouses above all "others" no longer holds meaning or possibility. No spouse and no family can compete with this all-consuming obsession.

Workaholics themselves are a key contributor to the unhealthy family patterns resulting from work addiction for a number of reasons. First, they may have grown up in a dysfunctional family system where role models taught unhealthy patterns of relating to others. Research indicates that the family of origin contributes greatly to the development of the workaholic, and the roots of the workaholic's perfectionism often lie in childhood experiences.[2] In these dysfunctional homes, families reward children for good performance, not for who they are. They give praise and conditional love only whenever children perform a certain way or meet certain high expectations. In adulthood, this same need for perfection is the basis for the obsession for work—everything must be done properly and always at a very high level of competence and perfection.

Second, the need for workaholics to feel dominant and "in control" may make them less able to relate to peers. They may interact more easily with older and younger people or those of a lower status or socioeconomic level than themselves. This need for continually being in control of themselves and in charge creates tension in family relationships. The one

Mr. Solan, a retired law enforcement officer, currently is an adjunct faculty member at Columbia College in Syracuse, New York.

Dr. Casey teaches counseling and psychological services at the State University of New York at Oswego.

constant involved in this work mind-set devalues the quality of social interactions. Loved ones have a reasonable expectation that time spent together is time well spent and, therefore, should not be made to feel that such time comes at the expense of personal productivity. Loved ones can sense "just going through the motions." The same holds true for relationships with peer groups and clients. People have a strong sense for those who are too busy to make time to properly address issues. Conflict becomes inevitable, and everyone "gets drawn into the act by waltzing around the workaholic's schedule, moods, and actions."[3]

Chief Smith was the proud father of two sons, ages 10 and 14. His wife of 18 years, a stay-at-home mother, formed a close relationship with the children, having adjusted to the irregular and long hours of the chief's workday. After his death, Mrs. Smith explained that her husband lived on the periphery of the family's life. She said that whenever he spent time with her and their children, he seemed to do so grudgingly, as though they were depriving him of valuable time away from his office. She noted that sometimes when he was home, he only slept and never interacted with the family. She also spoke about going to family gatherings, such as birthday parties, with only the children and finding it hard to explain to friends and family that her husband was either sleeping or working on his day off, rather than celebrating a special occasion. She thought that he ignored his family, and she felt taken for granted and unwanted. Other times, he came home and treated the three of them like the police officers he supervised. He was demanding, controlling, and very jealous of her close relationship with their children. She never knew which personality he would exhibit.

The self-imposed behavior of work addiction also causes physical symptoms. Excessive pumping of adrenaline resulting in abnormal blood pressure, heart trouble, stomach sensitivity, nervousness, and the inability to relax under any circumstances are commonplace.

> ***"While the actual mortality rate for work addiction may be low, the social lethality of this behavior proves overwhelming."***

Workaholics report feeling pressure in their chests, dizziness, and lightheadedness.[4] Obviously, any long-term stress that manifests such symptoms as these can result in dangerous health consequences of many types. Chief Smith's protracted work addiction led to serious illness and his ultimate, untimely death.

Those people obsessed with work share the traits of others with such addictions as substance abuse, food dependencies, or sexual compulsions. A classic definition of a workaholic describes "a person whose need for work has become so excessive that it creates noticeable disturbance or interference with his bodily health, personal happiness, and interpersonal relations, and with his smooth social functioning."[5] The unique difference between work addiction and other addictions, however, is that supervisors often sanction work addiction. Supervisors and peers admire this so-called work ethic, and it can be both financially and professionally rewarding.

Without question, healthy work can provide a sense of accomplishment and greatly enhance an individual's well-being. Employees who work hard, with great energy and dedication, are not necessarily addicted to their work. Most of the time, they thoroughly enjoy their work. However, the key is their ability to maintain a balance in their lives so that their work does not consume them.

Workaholics, on the other hand, become gradually more emotionally crippled as they become embroiled with the demands and expectations of the workplace. They are "addicted to control and power in a compulsive drive to gain approval and success."[6] The obsession with work grows out of the workaholic's perfectionism and competitive nature. As with other addictions, work is the "fix," the drug that frees the workaholic from experiencing the emotional pain of the anger, hurt, guilt, and fear in the other areas of the workaholic's life. Workaholics constantly focus on work, seeking to meet their personal emotional needs through their professions.

Work-Addiction Risk Test

To find out if you are a workaholic, rate yourself on each of the statements below, using a rating scale of 1 (never true), 2 (sometimes true), 3 (often true), or 4 (always true). Put the number that best describes your work habits in the blank beside each statement. After you have responded to all 25 statements, add up the numbers for your total score. The higher your score, the more likely that you are a workaholic, whereas the lower your score, the less likely that you are a workaholic.

__ 1. I prefer to do most things myself, rather than ask for help.
__ 2. I get impatient when I have to wait for someone else or when something takes too long.
__ 3. I seem to be in a hurry and racing against the clock.
__ 4. I get irritated when I am interrupted while I am in the middle of something.
__ 5. I stay busy and keep many irons in the fire.
__ 6. I find myself doing two or three things at one time, such as eating lunch, writing a memo, and talking on the telephone.
__ 7. I overcommit myself by accepting more work than I can finish.
__ 8. I feel guilty when I am not working on something.
__ 9. It is more important that I see the concrete results of what I do.
__ 10. I am more interested in the final result of my work than in the process.
__ 11. Things just never seem to move fast enough or get done fast enough for me.
__ 12. I lose my temper when things do not go my way or work out to suit me.
__ 13. I ask the same question again, without realizing it, after I already have received the answer.
__ 14. I spend a lot of time mentally planning and thinking about future events while tuning out the here and now.
__ 15. I find myself continuing to work after my coworkers have stopped.
__ 16. I get angry when people do not meet my standards of perfection.
__ 17. I get upset when I am in situations where I cannot be in control.
__ 18. I tend to put myself under pressure from self-imposed deadlines.
__ 19. It is hard for me to relax when I am not working.
__ 20. I spend more time working than socializing with friends or on hobbies or leisure activities.
__ 21. I dive into projects to get a head start before all of the phases have been finalized.
__ 22. I get upset with myself for making even the smallest mistake.
__ 23. I put more thought, time, and energy into my work than I do into my relationships with loved ones and friends.
__ 24. I forget, ignore, or minimize celebrations, such as birthdays, reunions, anniversaries, or holidays.
__ 25. I make important decisions before I have all of the facts and a chance to think them through.

For clinical use, scores on the test are divided into three ranges. Those scoring in the upper third (67-100) are considered highly workaholic. If you scored in this range, it could mean that you are on your way to burnout, and new research suggests that family members may be experiencing emotional repercussions as well. Those scoring in the middle range (57-66) are considered mildly workaholic. If you scored in this range, there is hope. With acceptance and modifications, you and your loved ones can prevent negative long-term effects. Those scoring in the lowest range (25-56) are considered not workaholic. If you scored in this range, you are probably an efficient worker instead of a workaholic and have no need to worry that your work style will negatively affect yourself or others.

Source: B.E. Robinson, Chained to the Desk *(New York, NY: New York University Press, 1998), 52-54. Minor editorial revisions have been made to several test items.*

With this information in mind, law enforcement supervisors must understand the dangers that work addiction presents. These supervisors also must remember that they have an ethical responsibility to intervene when they observe the telltale signs of the work-addicted personality.

A New Covenant

Perhaps, the poet Robert Frost had Chief Smith in mind when he observed, "By working faithfully 8 hours a day, you may eventually get to be boss and work 12 hours a day." Certainly, expectations run high in the law enforcement profession. Establishing and maintaining relationships creates tremendous demands on time, resources, and energy; life balance easily becomes lost. The wise boss must understand and accept this reality.

Twenty-first century police management has embraced a sea of change. Police supervisors now routinely use technology to gather and analyze data across the full spectrum of police performance measures, and, more important, they hold officers accountable for results. Today, supervisors acknowledge a new covenant, which demands that they set out quantifiable work standards to measure work performance.

Prudent and ethical supervisors must measure subordinate productivity in many ways. They must consider the relative limits of what can be reasonably achieved by different officers, with diverse skills and abilities, across the spectrum of assignments and work shifts, as well as family and personal situations. Supervisors must understand that officers have different tolerance levels to manage the personal, as well as the professional, issues that they encounter. Most important, commanders must realize that the quickest route to supervisory negligence is a shortsighted focus on results, not people.

Conclusion

While law enforcement professionals should possess a strong sense of duty and responsibility for the public's welfare, they must not forget the well-being of their families, friends, and, most important, themselves. The sad lesson of Chief William Smith demonstrates the need for officers to take the long-term view, beyond the crisis of the moment. Thomas Merton, a Trappist monk and prominent author, said, "We cannot be happy if we expect to live all the time at the highest peak of intensity. Happiness is not a matter of intensity, but of balance and order and rhythm and harmony." The real challenge for law enforcement professionals rests with at least seeking, if not achieving, that balance for their families, their peers, their communities, and, most of all, themselves. In so doing, they will become better spouses, friends, coworkers, and officers who value their work, but do not let it overwhelm their lives. ✦

Endnotes

[1] B.E. Robinson, *Chained to the Desk* (New York, NY: New York University Press, 1998), 3.

[2] B. Killinger, *Workaholics: The Respectable Addicts* (Buffalo, NY: Firefly Books, 1991).

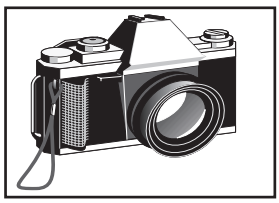
[3] Supra note 1, 75.

[4] Supra note 2.

[5] W.E. Oates, *Confessions of a Workaholic* (New York, NY: Abingdon Press, 1971), 4.

[6] Supra note 2, 6.

Wanted: Photographs



The *Bulletin* staff is always on the lookout for dynamic, law enforcement-related photos for possible publication in the magazine. We are interested in photos that visually depict the many aspects of the law enforcement profession and illustrate the various tasks law enforcement personnel perform.

We can use either black-and-white glossy or color prints or slides, although we prefer prints (5x7 or 8x10). We will give appropriate credit to photographers when their work appears in the magazine. Contributors should send duplicate, not original, prints as we do not accept responsibility for damaged or lost prints. Send photographs to:

Art Director
FBI Law Enforcement Bulletin, FBI Academy,
Madison Building,
Room 209, Quantico,
VA 22135.

Book Reviews

Practical Law Enforcement Management
by Roger Fulton, Gould Publications, Inc., Longwood, Florida, 2002.

"Practical" is the operative word in describing *Practical Law Enforcement Management*. The book represents a straightforward, no-nonsense approach to managing issues in today's law enforcement environment.

Dr. Fulton examines the components of management through five chapters titled "Supervision," "Management," "Administration," "Leadership," and "Your Career." He begins each chapter with a brief synopsis outlining the topic and a statement of fact on what the reader might do to reach a successful conclusion to each dilemma. He also requires the reader to actually interact with him by asking questions, such as "How do you stack up?" in the chapter on supervision and "Are you part of the problem?" in the one on management. And, he provides a step-by-step road map on becoming a complete law enforcement manager by presenting a guideline or framework for each individual reader.

In addition to discussing management styles, Dr. Fulton addresses preparing for promotion, as well as working toward retirement. He not only provides the question mark of how to be a leader and manager but he also presents an outline on how to successfully manage a law enforcement agency by using common sense, along with the known policies and procedures. Whether readers are preparing for a promotion or just wanting to hone their skills as a supervisor, this book offers invaluable information.

Reviewed by
Deputy Chief Brenda J. Smith
Omaha, Nebraska, Police Department

Practical Law Enforcement Management by Roger Fulton stands as an excellent resource for current law enforcement managers and for those who have aspirations of being promoted through the chain of command. Dr. Fulton, a retired captain with the New York State Police, a management consultant, and an author of two successful books and dozens of articles, has taken his many years of expertise in police management and training and condensed it into an outstanding guide for veteran law enforcement managers, as well as the up-and-coming leaders of tomorrow.

As an additional plus to Dr. Fulton's credentials, Michael Carpenter, who edited the book, brings more than 26 years of experience in various aspects of law enforcement, including serving as a police training specialist for the state of New York. Currently an assistant professor of criminal justice at Adirondack Community College in Queensbury, New York, he also has authored one book, contributed to another, and written numerous articles for national law enforcement publications.

Between the two, Dr. Fulton and Professor Carpenter share a wealth of experiences with the reader through an engaging and highly readable format. *Practical Law Enforcement Management* is recommended for law enforcement officers and managers who want a successful career in police supervision, management, and leadership.

Reviewed by
Chief John M. Eller
Brookhaven, Pennsylvania,
Police Department

A Four-Domain Model for Detecting Deception

An Alternative Paradigm for Interviewing

By JOE NAVARRO, M.A.

For 30 years, the literature on interviewing has emphasized the use of both verbal and nonverbal cues in detecting deception during the interview process.[1] Much of that emphasis paralleled the immense amount of research during that same time period in the area of psychology and the study of nonverbal behavior. Unfortunately, many people still misinterpret a significant amount of nonverbal behavior as indicative of deception when, in fact, it just may be nervousness or such behavior as face touching that also can indicate honesty.[2]

Repeated studies have shown that traditional methods of detecting deception during interviews succeed only 50 percent of the time, even for experienced law enforcement officers.[3] In spite of this, investigators still need the ability to test the veracity of those they interview. To do so, investigators require a model that incorporates research with empirical experience to differentiate honesty from deception. They can use an alternative paradigm for detecting deception based on four critical domains: comfort/discomfort, emphasis, synchrony, and perception management.

Comfort/Discomfort

Comfort is readily apparent in conversations with family members and friends. People sense when

> ***"In interviewing and detecting deception, synchrony plays an important role."***

Special Agent Navarro is assigned to the FBI's Tampa office and also serves in the FBI's National Security Division's Behavioral Analysis Program.

others have a good time and when they feel comfortable in their presence. Experiencing comfort in the presence of strangers becomes more difficult, especially in stressful situations, such as during an interview. A person's level of comfort or discomfort is one of the most important clues interviewers should focus on when trying to establish veracity. Tension and distress most often manifest upon guilty people who must carry the knowledge of their crimes with them. Attempting to disguise their guilt places a distressing cognitive load on them as they struggle to fabricate answers to what otherwise would be simple questions.[4]

When comfortable, an individual's nonverbal behavior tends to mirror the other person present.[5] For example, if one person leans forward, the other tends to do so as well. Or, if one leans to the side with hands in pockets and feet crossed, the other person may do the same. Subconsciously, people demonstrate their comfort with whom they are talking. When touched, people may touch back to emphasize a point. Some may display their comfort more openly, such as showing more of their torso and the insides of their arms and legs. People who speak the truth more often display comfort because they have no stress to conceal nor do they have guilty knowledge to make them feel uncomfortable.[6]

While seated at a table, people comfortable with each other will move objects aside so that nothing blocks their view. Over time, they may draw closer so that they do not have to talk as loud, and their breathing rhythm, tone of speech, pitch, and general demeanor will become similar.

Subtleties of comfort contrast with discomfort. People show discomfort when they do not like what is happening to them, what they are seeing or hearing, or when others compel them to talk about things that they would prefer to keep hidden. People first display discomfort physiologically—heart rates quicken, hairs stand up, perspiration increases, and breathing becomes faster. Beyond the physiological responses, which are autonomic and require very little thinking, people primarily manifest discomfort nonverbally instead of vocally. They tend to move their bodies by rearranging themselves, jiggling their feet, fidgeting, or drumming their fingers when scared, nervous, or significantly uncomfortable.[7]

If, while the interviewer remains relaxed and poised, the interviewee continually looks at the clock, sits tensely, or does not move ("flash frozen"), the interviewer may discern a lack of comfort even though everything may appear normal to the untrained eye.[8] Interviewees show discomfort when they repeatedly talk about finalizing the interview or when disruptions appeal to them.

People tend to distance themselves from those with whom they feel uncomfortable. Even while sitting side by side, people will lean away from those with whom they feel uncomfortable, often moving either their torsos or their feet away or toward an exit, which nonverbally exhibits displeasure.[9] These actions can occur in interviews due to the subject matter discussed. Likewise, people create artificial barriers with either their shoulders and arms or with inanimate objects in front of them. For example, by the end of one interview, a very uncomfortable and dishonest interviewee had built a little barrier in front of himself using soda cans, pencil holders, and various documents, ultimately planting a backpack on the table between himself and the interviewer. At the time, the interviewer did not

recognize the subject's obvious intent of creating a barrier.

Other clear signs of discomfort include rubbing the forehead near the temple region, squeezing the face, rubbing the neck, or stroking the back of the head with the hand.[10] Interviewees often will show their displeasure by rolling their eyes out of disrespect; picking lint off themselves (preening); talking down to the interviewer; giving short answers; becoming resistant, hostile, or sarcastic; or displaying "micro gestures" with indecent connotations, such as "giving the finger."[11]

Eyes also serve as formidable communicators of discomfort, yet investigators often ignore them during interviews. People use their eyes as a blocking mechanism similar to folding their arms across their chest or turning away from those with whom they disagree. In a similar response, when people do not like something they hear, they usually close their eyes as if to block out what they just heard. They do this subconsciously and so often that others do not pay attention to it in day-to-day affairs. People may close their eyes before touching or rubbing them as if to further block or relieve themselves of what they just heard. Interviewers can capitalize on this behavior by noting when interviewees block with their eyes. This may point to questions that trouble the subject or to issues with which they are struggling. In most cases, eye blocking proves extremely accurate in highlighting issues problematic to the interviewee. Additionally, when people feel troubled or frustrated or they have a subdued temper tantrum, their eyelids may close or flutter rapidly as an expression of their sentiment.[12] Research also has shown that when people are nervous or troubled, their blink rate increases, a phenomenon often seen with liars under stress.[13] In one case where investigators closely videotaped the interviewee, observers in another room catalogued the subject's blink rate increase from 27 times per minute to 84 times a minute during stressful questions. Investigators should consider all of the eye manifestations that fall under the comfort/discomfort domain as powerful clues to how subjects register information or what questions prove problematic.

> ***Subtleties of comfort contrast with discomfort.***

When interpreting eye contact, however, many misconceptions still exist. Little or no eye contact is perceived erroneously by some as a classic sign of deception, especially during questioning, while the truthful should "lock eyes." This may be accurate for some but not for all. For instance, research shows that Machiavellian[14] people actually will increase eye contact during deception.[15] This may occur because they know that many interviewers look for this feature. Also, some people learned to look down or away from parental authority as a form of respect when questioned or scolded. Investigators should remain aware of changes in eye contact and eye behavior during interviews. They should establish the interviewee's default pattern of eye behavior during benign questioning then look for changes or indicators of discomfort as the interview progresses, which often gives clues to deception.

Emphasis

When people speak, they naturally incorporate various parts of their body, such as the eyebrows, head, hands, arms, torso, legs, and feet, to emphasize a point for which they feel deeply or emotionally. This movement proves important to investigators because, as a rule, people emphasize when genuine. Liars, for the most part, do not emphasize with nonverbals.[16] They will think of what to say and how to deceive, but rarely do they think about the presentation of the lie. When compelled to lie, most people do not realize how much emphasis or accentuation enters into everyday conversations. For the interviewer, emphasis accurately reflects reality or the truth.[17] When liars attempt to fabricate an answer, their emphasis looks unnatural or is delayed; they rarely emphasize where appropriate, or they choose to do so only on unimportant matters.

People accentuate both verbally and nonverbally in their interactions. They emphasize verbally through voice, pitch, tone, or repetition. On the other hand, they

emphasize nonverbally, which can prove even more accurate and useful to investigators. People who typically use their hands while speaking punctuate their remarks with hand gestures that emphatically illustrate or exclaim. They also may thrust forward, point, or pound the desk as they emphasize. Others accentuate with the tips of their fingers, either touching things or gesturing with them. Hand behaviors compliment speech, thoughts, and true sentiments.[18] Raising eyebrows (eyebrow flash) or widening eyes also emphasizes a point.[19]

When interested, people lean their torsos forward and, often, employ gravity-defying gestures, such as raising up on the balls of their feet as they make a significant or emotionally charged point. While sitting down, some emphasize by raising the knee to highlight important points. Occasionally, people will add emphasis by slapping their knee as it comes up, indicative of emotional exuberance. Gravity-defying gestures symbolize emphasis and true sentiment, both of which liars rarely possess.

In contrast, people de-emphasize or show lack of commitment by speaking behind their hands or showing limited facial expression as if to control their countenance because they are not committed to what they are saying.[20] Deceptive people often show deliberative, pensive displays, such as touching fingers to their chin or stroking their cheeks, as though they still are thinking about something, rather than emphasizing the point they are making. They are evaluating what they said and how it is being received, which is inconsistent with honest behavior.

Synchrony

In interviewing and detecting deception, synchrony plays an important role. Ideally, synchrony (e.g., harmony, congruence, and concordance) should occur between the interviewer and the interviewee; between what is said vocally and nonverbally; between the circumstances of the moment and what the subject is saying; and between events and emotions, including synchrony of time and space.

In an interview setting, the tone of both parties should mirror each other over time if synchrony exists.[21] A certain amount of harmony occurs in speech patterns, sitting styles, touching frequency, and general expressions. An interviewer and subject "out of sync" become subtly palpable because each will sit differently, talk in a manner or tone dissimilar from the other, and possibly have expressions at odds, if not totally disparate, with each other. These circumstances prohibit effective communication, an element pertinent to successful interviewing.

When interviewed, people who answer in the affirmative should have congruent head movement supporting what they say. Lack of synchrony often occurs when people say, "I did not do it," while nodding their heads up and down as if to say, "yes, I did." Or, when asked, "Would you lie about this?" their heads again bob up and down. Upon catching themselves in this faux pas, they then reverse their head movement. When observed, these instances are almost comical and amateurish. More often, a mendacious statement, such as "I did not do it," precedes a noticeably delayed and less emphatic negative head movement. These behaviors are not synchronous and, therefore, more likely to be equated with a lie.

Synchrony should occur between what is being said and the events of the moment. During a street interview, if the subject interjects with superfluous information or facts totally irrelevant, the officer should note the disharmony. The information and facts should remain pertinent to the issue at hand, the circumstances, and the questions. When the answers are asynchronous with the event and questions, officers may assume that something likely is wrong or the person is stalling for time to fabricate a story.

For instance, when parents report the alleged kidnapping of their infant, synchrony should occur between the event (kidnapping) and

their emotions. The complainant should be clamoring for law enforcement assistance, emphasizing every detail, feeling the depth of despair, showing an eagerness to help, and willing to retell the story, even at personal risk. When placid individuals make such reports, they appear more concerned with furnishing one particular version of the story, lacking consistent emotional displays or seem more concerned about their well-being and how they are perceived vis-a-vis the egregious event (alleged kidnapping of a loved one). These examples do not exhibit synchrony with circumstances and prove inconsistent with honesty.

Last, synchrony should exist between events, time, and space. A person who delays reporting a significant event, such as the drowning of a fellow passenger, or one who travels to another jurisdiction to report the event rightfully should come under suspicion. Additionally, interviewers should remain cognizant of subjects who report events that would have been impossible for them to observe from the vantage point from which they tell the story. People who lie do not think of how synchrony fits into the equation; yet, it plays a major role during interviews and the reporting of crimes.

Perception Management

Perception management occurs both verbally and nonverbally. During interviews, liars often use perception management, a concept with which psychopaths are well acquainted, to influence their intended targets of deception.[22] For instance, nonverbally, subjects will yawn excessively as if to show that they feel bored. If the person is sitting, they may slouch or splay out on a couch, stretch their arms, and cover more territory as if to demonstrate their comfort.

Verbally, liars will try to vocalize their honesty, integrity, and the implausibility of their involvement in committing a crime. They will try to "look good" to the interviewer.

> ***...investigators require a model that incorporates research with empirical experience to differentiate honesty from deception.***

They may use perception management statements, such as "I could never hurt someone," "Lying is below me," "I have never lied," "I would never lie," or "I would never do such a thing," all of which should alert investigators to the possibility of deception. Other statements, such as "to be perfectly frank," "to be honest," "to be perfectly truthful," or "I was always taught to tell the truth," are solely intended to influence the perception of the interviewer.[23]

Other forms of perception management include attending the interview with someone of prominence in the community or a retinue of so-called close friends. Further, subjects may self-medicate through the use of alcohol or prescription drugs to appear placid and content. They may change their clothing or hair styles to appear more genuine or more socially conventional.

In all of these examples, subjects attempt to manage the perception of the interviewer. People practice perception management every day, such as getting dressed for a date. However, when it manifests itself in an interview setting, investigators should recognize such efforts and question the intent.

Conclusion

The detection of deception remains a difficult task. Interviewers can enhance their ability to detect deception by focusing on four domains—comfort/discomfort, emphasis, synchrony, and perception management—rather than merely trying to detect traditional signs of deception, which, in some cases, may be misleading.[24] The research in this area over the last 20 years is unequivocal. Nonverbal behaviors, in and of themselves, do not clearly indicate deception.[25] However, when interviewers notice a display of discomfort and a lack of comfort, emphasis, synchrony, and perception management, a greater certitude for assessing deception exists.

Investigators can expect subjects to react poorly in one or two areas. But, to do so in all four domains indicates communication problems, which may originate from the interviewee's antipathy toward the interviewer or law enforcement or result from culpability, guilty knowledge, or

dishonesty. Regardless, in these cases, information likely did not flow freely from the interviewee, which rendered an interview of limited value or, worse, a complete fabrication. ✦

Endnotes

[1] Fred E. Inbau and et. al., *Criminal Interrogation and Confessions*, 4th ed. (Gaithersburg, MD: Aspen Publishers, Inc., 2001), ix.

[2] Charles V. Ford, *Lies! Lies! Lies!: The Psychology of Deceit* (Washington, DC: American Psychiatric Press, Inc., 1996), 200.

[3] Ibid., 217.

[4] B.M. DePaulo, J.I. Stone, and G.D. Lassiter, *Deceiving and Detecting Deceit*, in *The Self and Social Life*, edited by B.R. Schlender, (New York, NY: McGraw-Hill, 1985), 323-370.

[5] Mark L. Knapp and Judith A. Hall, *Nonverbal Communication in Human Interaction*, 3d ed. (Orlando, FL: Harcourt Brace Jovanovich, College Publishers, 1997), 277.

[6] Paul Ekman, *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage* (New York, NY: W.W. Norton & Co., 1985), 185.

[7] Gavin De Becker, *The Gift of Fear* (New York, NY: Dell Publishing, 1997), 133.

[8] Supra note 5, 321.

[9] Supra note 5, 320.

[10] David G. Givens, *The Nonverbal Dictionary of Gestures, Signs & Body Language Cues* (Spokane, WA: Center for Nonverbal Studies, 1998-2002); *http://members.aol.com/nonverbal2/diction1.htm*

[11] Supra note 6, 101-103.

[12] Joe Navarro and John R. Schafer, "Detecting Deception," *FBI Law Enforcement Bulletin*, July 2001, 10.

[13] Supra note 5, 467.

[14] "Suggesting the principles of conduct laid down by Machiavelli; specifically marked by cunning, duplicity, or bad faith," *Merriam Webster's Collegiate Dictionary*, 10th ed., s.v. "Machiavellian."

[15] R.E. Exline, J. Thibaut, C.B. Hickey, and P. Gumpert, *Visual Interaction in Relation to Machiavellianism and an Unethical Act*, in R. Christie and F.L. Geis (eds.), *Studies in Machiavellianism* (New York, NY: Academic Press, 1970).

[16] David J. Lieberman, *Never Be Lied to Again* (New York, NY: St. Martin's Press, 1998), 37.

[17] Supra note 6, 107.

[18] Supra note 5, 277-284.

[19] Desmond Morris, *Body Watching* (New York, NY: Crown Publishers, 1985), 61 and supra note 5, 68.

[20] Supra notes 5, 320, and 15, 37.

[21] Robert B. Cialdini, *Influence: The Psychology of Persuasion* (New York, NY: William Morrow and Company, Inc., 1993), 167-207.

[22] J. Reid Meloy, *The Psychopathic Mind: Origins, Dynamics, and Treatment* (Northvale, NJ: Jason Aronson, Inc., 1998), 139.

[23] Supra note 16, 46.

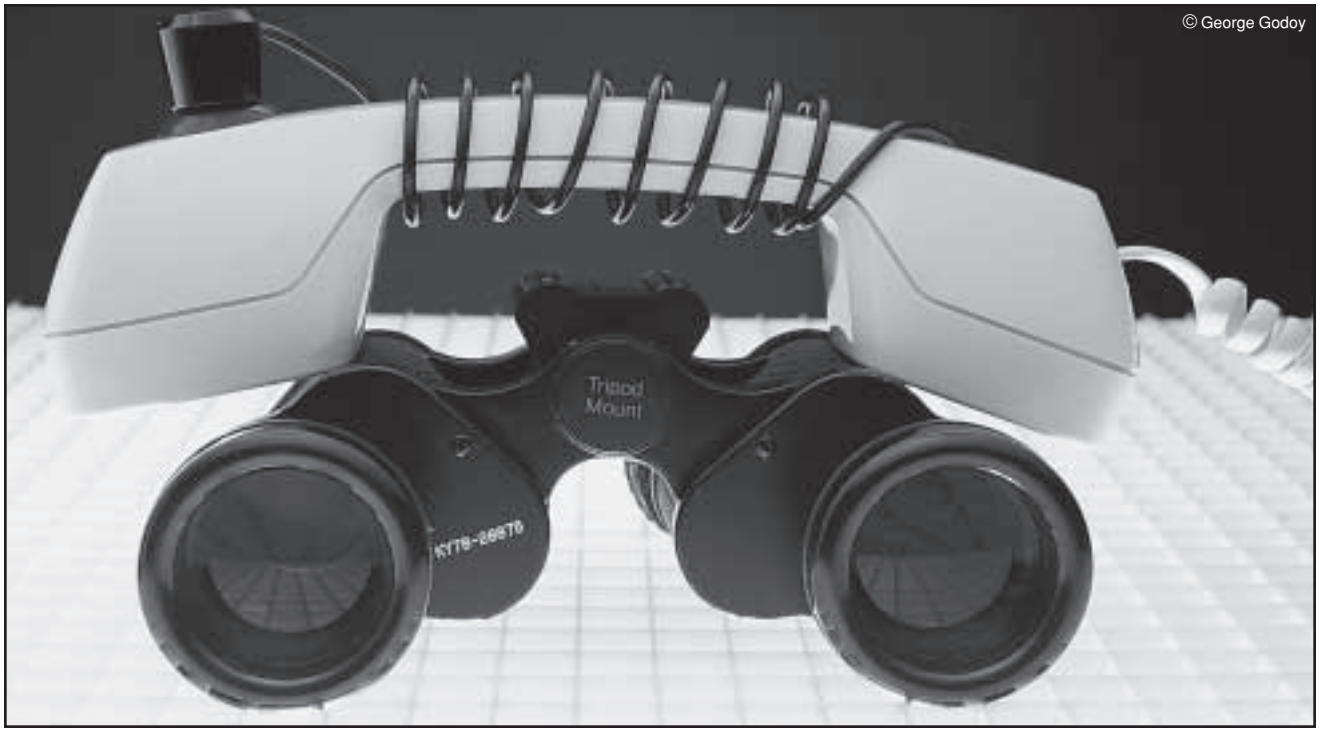
[24] Supra note 6, 162-189.

[25] Supra notes 2, 217, and 6, 98.

Foreign Intelligence Surveillance Act

Before and After the USA PATRIOT Act

By MICHAEL J. BULZOMI, J.D.



The terrorist attacks of September 11, 2001, left an indelible mark upon America and an overshadowing feeling of vulnerability. They also created a determination to respond to the new national security threats they represented. Congress reacted to these threats by passing laws providing new tools to fight terrorism. Perhaps, the most controversial recent act of Congress is the United and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001[1] (USA PATRIOT Act) and its impact upon the use of electronic surveillance and physical searches authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)[2] to combat foreign threats.

Some Americans fear the actions taken by Congress may infringe upon basic American liberties. Benjamin Franklin warned that " those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety."[3] The government must use its new tools in a way that preserves the rights and freedoms guaranteed by America's democracy, but, at the same time, ensure that the fight against terrorism is vigorous and effective. No American should be forced to seek safety over liberty. This article briefly examines FISA and the impact of the USA PATRIOT Act upon it.

FISA

Electronic monitoring (including both wiretaps and microphone installations) and physical searches

are excellent, and sometimes essential, sources of information for both foreign intelligence and criminal activities. In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act. Title III of that act[4] contains provisions concerning the authorization and use of electronic monitoring by the government to gather information regarding criminal activities. Under Title III, the government has specific authorization procedures and rules to follow when it monitors people and places to collect evidence of violations of criminal laws. But, Title III did not answer the question of whether or not the government is required to obtain court authorization for electronic monitoring conducted, not for criminal investigations but for the collection of information regarding threats to national security.

The U.S. Supreme Court faced this issue in the case of *United States v. United States District Court.*[5] In this case, a group of Vietnam War protesters tried to blow up the local CIA recruiting office in Ann Arbor, Michigan, and a number of other government buildings. Evidence obtained during a domestic national security wire interception, undertaken without a formal court order, was used in the subsequent criminal trial. The use of this evidence was contested. The issue was whether or not the president had the authority, through the attorney general, to authorize electronic surveillance for national security matters without prior judicial review. The Court held that the government does not have unlimited power to conduct national security wiretaps for domestic security matters, and that prior judicial authorization is needed before using wiretaps for national security purposes. However, the Court recognized that such wiretaps involve different policy and practical considerations from ordinary criminal wiretaps. It suggested that Congress consider exploring the issue and decide if the authorization for and rules governing the use of national security wiretaps should be the same as those governing criminal wiretaps. The Court made it clear that it was not deciding the issue of the government's authority to conduct wiretaps in cases of foreign threats to the national security.

To establish the necessary authority and procedures for the government to conduct wiretaps in response to foreign threats, Congress passed FISA. FISA established a requirement of judicial approval before the government engages in an electronic surveillance (as well as physical searches) for foreign intelligence purposes. The act established the FISA Court, consisting of U.S. District Court judges designated by the chief justice of the U.S. Supreme Court. The court's purpose is to review government applications for national security electronic monitoring and searches and authorize their use with appropriate limitations. If the FISA Court denies an application for an order authorizing a national security wiretap or search, the matter is referred under seal to the FISA Court of Review, comprised of three federal judges selected by the chief justice of the U.S. Supreme Court. The court of review determines whether the application was properly denied.[6] Its decision can be appealed directly to the U.S. Supreme Court.

Special Agent Bulzomi is a legal instructor at the FBI Academy.

"The government must use its new tools in a way that preserves the rights and freedoms guaranteed by America's democracy, but, at the same time, ensure that the fight against terrorism is vigorous and effective."

FISA Contrasted with Title III

In essence, the purpose of a FISA order is to gather foreign intelligence information,[7] while the purpose of a Title III wiretap order is to gather evidence for criminal prosecution. The FISA application

need only state facts supporting probable cause to believe that the target of the intercept (or search) is a foreign power, or an agent of a foreign power, and that the facilities to be monitored or searched are being used, or are about to be used, by a foreign power, or an agent of a foreign power, and to certify that a significant purpose of the surveillance is to obtain foreign intelligence information.[8] To show that a person is an agent of a foreign power, the government need only relate facts demonstrating that the subject is an officer or employee of a foreign power or acts on the foreign power's behalf; or knowingly engages in clandestine intelligence-gathering activities that may involve a violation of U.S. criminal statutes; or knowingly engages in sabotage, international terrorism, or in the preparation of these activities on behalf of a foreign power.[9]

In contrast, a criminal Title III wiretap must be supported by probable cause to believe that a specific individual, using an identified phone or location, is committing a particular crime.[10] It requires that the government show that a predicate offense is, has, or will be committed by the subject of the surveillance[11] and that particular communications concerning the predicate offense will be obtained through the wiretap[12] at a specified location or through a specified device used by the target.[13]

FISA Information for Criminal Prosecutions

It is important to note that both FISA and Title III require a showing of probable cause to authorize electronic monitoring (and physical searches in the case of FISA). However, because of the differing objectives of the two acts, the degree of specificity required differs markedly. Arguably, because of the different probable cause showing required by FISA, it is easier for the government to obtain a FISA order than it is to obtain a Title III order. Because of this, the courts became concerned that the government would obtain FISA electronic surveillance orders in what were essentially criminal investigations to avoid the stricter requirements of Title III.

> ***"...both FISA and Title III require a showing of probable cause to authorize electronic monitoring (and physical searches in the case of FISA)."***

This concern surfaced in an espionage case that predates FISA. In *United States v. Truong Dinh Hung,*[14] the government used a warrantless wiretap to overhear and record telephone conversations of the defendant and to bug his apartment. The wiretapping and bugging were authorized by the attorney general under the "foreign intelligence" exception to the Fourth Amendment. The defendant moved to suppress the evidence collected by means of the wiretap and bug as violations of the Fourth Amendment. The U.S. Court of Appeals for the Fourth Circuit admitted the evidence collected during the early days of the collection but held that evidence obtained after the primary purpose of the investigation had shifted from securing intelligence information to accumulating evidence of a crime and must be suppressed because of the failure to comply with the requirements of Title III. This ruling is the origin of the "primary purpose" test that was to create problems in later cases.

Subsequent cases decided after the passage of FISA distinguished *Truong* on the grounds that the surveillance authorization in that case was not obtained pursuant to a FISA warrant.[15] These courts noted that FISA contains a statutory mechanism for the dissemination of criminal information obtained during an intelligence intercept and have held that when such evidence is discovered "incidentally" during an authorized FISA intercept it may be admitted in subsequent criminal prosecutions.[16] This would include situations where "the government can anticipate that the fruits of such surveillance may later be used, as allowed by [the statute], as evidence in a criminal trial."[17] This line of reasoning became known as the "primary purpose" test and was adopted by several circuits.[18] In other words, when the primary object of the electronic monitoring (or search) was to collect foreign intelligence information, FISA was the appropriate mechanism to seek authorization from the courts. When the primary purpose was to seek criminal prosecution, Title III was the appropriate mechanism. Failure

to strictly observe this distinction resulted in a possible suppression of the evidence.

The "primary purpose" test led the FISA Court and the U.S. Department of Justice (DOJ) to adopt a policy of building a "wall" between intelligence investigators and criminal investigators for fear of tainting FISA court ordered surveillances. Intelligence investigators were not to discuss ongoing foreign intelligence or foreign counterintelligence investigations with criminal investigators. In this way, FISA orders could not be used by criminal investigators to avoid seeking Title III orders. This practice led to a critical lack of coordination in investigations, such as international terrorism cases, which have both intelligence and criminal aspects.

FISA AS AMENDED BY THE USA PATRIOT ACT

Following the September 11, 2001, terrorist attacks, Congress reassessed intelligence-gathering procedures and passed the USA PATRIOT Act. The most significant changes involve the purposes for which FISA-authorized electronic monitoring and searches may be used and the exchange of information between criminal and foreign intelligence investigators.

Previously, FISA-authorized electronic monitoring and searches only could be used if high-level executive officials certified that "the purpose" was to obtain foreign intelligence information. As noted, that language came to be interpreted as the "primary purpose" by the courts and DOJ. The USA PATROIT Act now requires that foreign intelligence information gathering be a "significant purpose."[19] The act amends FISA so that intelligence officials may coordinate efforts with law enforcement officials to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities without undermining the required certification of the "significant purpose" of FISA orders. The result is that Congress rejected the idea of having a "wall" between foreign intelligence and law enforcement officials when the object of the investigation is to detect, prevent, or prosecute foreign intelligence crimes.

On March 6, 2002, Attorney General John D. Ashcroft implemented the USA PATRIOT Act by establishing a new DOJ policy regarding information-sharing procedures. The new procedures permitted the complete exchange of information and advice between intelligence officers and law enforcement officers regarding FISA surveillances and searches.

On May 17, 2002, the FISA Court rejected the attorney general's new policy.[20] The FISA Court ruled that law enforcement officials cannot a) direct or control an investigation using FISA searches or surveillances for law enforcement objectives, b) direct or control the use of FISA procedures to enhance a criminal prosecution, c) make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances, or d) that representatives of DOJ's Office of Intelligence Policy and Review (OIPR) be invited to ("chaperone" in the view of the DOJ) all meetings between FBI and DOJ's Criminal Division to consult regarding efforts to investigate or protect against foreign attack, sabotage, or international terrorism to ensure that foreign intelligence gathering remains the primary purpose of any FISA-authorized technique. The FISA Court's rejection of the new guidelines led to the first-ever appeal to the FISA Court of Review.

In its decision, the FISA Court of Review decided that FISA does not preclude or limit the government's use of foreign intelligence information, including evidence of crimes, in certain types of criminal prosecutions.[21] The court of review determined that the restrictions imposed by the FISA Court on the government are not required by FISA, as amended by the USA PATRIOT Act or by the Constitution and that the USA PATROIT Act amendments of the FISA statute do not violate the Fourth Amendment of the Constitution.

The court of review made several important points. First, there must be a significant foreign intelligence information-gathering

purpose for every FISA application for electronic monitoring or search, such as recruiting a foreign spy as a double agent, identification of foreign intelligence taskings, or the discovery of foreign spy tradecraft.[22]

Second, the court determined that FISA could be used to obtain evidence primarily for a criminal prosecution if the prosecution is an offense related to a foreign intelligence threat (a foreign intelligence crime) and a significant foreign intelligence-gathering purpose also is present.[23] The court defined foreign intelligence crimes as those listed in the FISA statute, including espionage, international terrorism, unlawful clandestine intelligence activities, sabotage, identity fraud offenses committed for or on behalf of a foreign power, and aiding or abetting or conspiring to commit these offenses.[24] Additionally, any ordinary crime intertwined with a foreign intelligence activity is included, such as bank robbery to finance terrorist actions or even credit card fraud to hide the identity of a spy.[25]

Finally, the court recognized that the USA PATRIOT Act lawfully breached the "wall" between criminal law enforcement and intelligence or counterintelligence gathering. Congress' intent in this matter is demonstrated amply by its addition of a new section to FISA by the USA PATRIOT Act. The new FISA Section 1806(k) reads:

> 1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with federal law enforcement officers to coordinate efforts to investigate or protect against
>
> a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

> 2) Coordination authorized under paragraph 1 shall not preclude the certification required by Section [1804](a)(7)(B) of this title or the entry of an order under Section [1805] of this title.[26]

This decision by the FISA Court of Review vindicates Congress' and the attorney general's view of FISA. It is permissible for intelligence and law enforcement officials to coordinate their efforts using all available resources, including FISA surveillances and searches, to detect, frustrate, and convict spies and terrorists.

It is important to note that additional safeguards are built into FISA if the target of the monitoring or search is a U.S. citizen or an alien admitted for permanent residence. The burden placed upon the government to obtain a FISA order is higher if the target is a U.S. person.[27] The act clearly states that the simple exercise of First Amendment rights by U.S. persons cannot be the basis for considering that person to be an agent of a foreign power.[28] The act also clearly establishes how and when information regarding a U.S. person may be used.[29]

USA PATRIOT Act and Information Sharing

An extremely important aspect of the USA PATRIOT Act is that it permits greater sharing of intelligence information between law enforcement and national security investigators, regardless of the source of the intelligence information. Section 203 of the USA PATRIOT Act amends Rule 6 of the Federal Rules of Criminal Procedure to permit the disclosure of grand jury information containing foreign intelligence information to "any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties."[30] The reporting requirement differs in that the name of the individual receiving the information is not given to the court, only

the department or agency receiving the information. This section also amends Title III (the federal wiretap statute) to permit the same type of disclosure of intelligence information gathered during a court authorized criminal wiretap.[31]

Section 905 of the act[32] underscores the importance that Congress assigns to information sharing. That section requires the attorney general, or any head of a federal department or agency with law enforcement responsibility, to promptly disclose to the director of the CIA any foreign intelligence information gathered as a result of a criminal investigation.

Other Related Amendments

The USA PATRIOT Act amended many federal statutes in significant ways that are important to criminal and intelligence investigators. It is impossible to discuss all of these amendments in this limited space. However, some of these amendments should be mentioned.

A very significant change is that the USA PATRIOT Act makes terrorism a predicate offense allowing for a wiretap under Title III.[33] Investigators now have a choice, depending on the nature of the investigation, to apply for a FISA order or a Title III wiretap order.

In addition, the act also allows for a roving wiretap under FISA.[34] Roving wiretaps allow law enforcement to respond to time-sensitive criminal or terrorist activity by continuing court sanctioned electronic surveillance, even if the target of the surveillance rapidly switches cellular telephones, Internet accounts, or meeting venues.

USA PATRIOT Act and Pen Registers and Traps and Traces

FISA contains specific provisions regarding the use of pen registers and traps and traces in foreign intelligence investigations.[35] Section 214 of the USA PATRIOT Act changes the standard for issuing pen registers and trap and trace orders. FISA pen registers and traps and traces now can be obtained when the government certifies that the information likely to be obtained is foreign intelligence information not concerning a U.S. person or is relevant to ongoing investigations to protect against terrorism or clandestine intelligence activities.[36] Prior to the USA PATRIOT Act, pen register and trap and trace orders required showing that there was relevance to an investigation and that there was reason to believe that the targeted line was being used by an agent of a foreign power or someone in communication with such an agent under certain circumstances. The second requirement no longer exists.

> ***"...the USA PATRIOT Act makes terrorism a predicate offense allowing for a wiretap under Title III."***

The USA PATRIOT Act also amended Title III, FISA, and the federal statute related to pen registers to explicitly authorize the use of pen registers and traps and traces on communication networks other than just telephones.[37] Computer networks and cellular telephones are now specifically subject to this technique.

Criminal pen register and trap and trace orders are no longer limited to the geographic area within the jurisdiction of the issuing court.[38] All service providers necessary to the execution of the order, regardless of their location, are covered by such orders.

USA PATRIOT Act and Physical Searches

Historically, some federal courts permitted the government to search premises, but delay for a reasonable time the required notice that the government had entered the premises.[39] The USA PATRIOT Act amended federal law to statutorily recognize the practice.[40] Delayed notice, or sneak-and-peek warrants, are now permissible where the court finds reasonable cause to believe that immediate notification of the execution of the warrant would have an adverse result.[41] The warrant must prohibit the seizure of tangible property unless the court finds it necessary. The warrant also must provide for giving notice of the search within a reasonable time, but extensions of time can be granted.

The act expands the reach of search warrants in domestic and international terrorism cases.[42] Ordinarily, criminal search warrants must be issued in the districts where the searches will occur.[43] Under the new rule, however, a magistrate judge in a district "in which activities related to the terrorism may have occurred"[44] may issue a war-

rant in that terrorism investigation that can be executed within or outside that district.

It is important to note that there is a 4-year sunset provision for some parts of the act.[45] The sharing of grand jury information portion of the act does not expire as of December 31, 2005. However, the "significant purpose" certification for FISA intercepts, the provosions regarding roving FISA surveillance, and the pen register and trap and trace do.

CONCLUSION

From a national security and law enforcement perspective, the United States has made considerable progress through recent court cases and congressional action toward ensuring that threats to national security are effectively investigated and countered. At the same time, care must be taken to ensure that the new tools provided by Congress in the USA PATRIOT Act are employed within the constraints of the Constitution. The Supreme Court has said "the police must obey the law while enforcing the law, that in the end life and liberty can be as much endangered from illegal methods used to convict those thought to be criminals as from the actual criminals themselves."[46]

FISA's different standards for intelligence surveillance have been viewed suspiciously by some who fear the loss of individual liberty. Care must be taken to avoid any abuse of this tool by law enforcement. The Court has warned that "the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."[47] Government should not overstep its bounds.

Law enforcement must act aggressively to investigate and prevent attacks from those who wish this country harm. At the same time, there must be oversight, both internal and external, to ensure that law enforcement is not overzealous. FISA and the USA PATRIOT Act provide such oversight. While the USA PATRIOT Act removed many of the obstacles that hindered terrorist and intelligence investigations in the past, it did not give law enforcement and intelligence agencies a free hand. The actions of

the government still are conducted under the watchful eye of the courts. In the end, law enforcement and intelligence investigators must be mindful that the constitutional protections that limit their authority also serve to protect their own rights as citizens of the United States. ✦

Endnotes

[1] PL 107-56, October 26, 2001, 115 Stat 272.

[2] 50 U.S.C. §§ 1801-1863(1994).

[3] Reply of the Pennsylvania Assembly to the governor, November 11, 1775.

[4] 18 U.S.C. §§ 2510-2520.

[5] 407 U.S. 297 (1972).

[6] 50 U.S.C. § 1803(b).

[7] 50 U.S.C. § 1804(a)(7)(B). Foreign intelligence information is defined as "(1) information that relates to, and if concerning a U.S. person is necessary to, the ability of the United States to protect against (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to (a) the national defense or the security of the United States; or (b) the conduct of the foreign affairs of the United States." *See* 50 U.S.C. § 1801 (e).

[8] 50 U.S.C. § 1804.

[9] 50 U.S.C. § 1801 (b).

[10] 18 U.S.C. § 2518(3).

[11] 18 U.S.C. § 2518(3)(a).

[12] 18 U.S.C. § 2518(3)(b).

[13] 18 U.S.C. § 2518(3)(d).

[14] 629 F.2d 908 (4th Cir. 1980).

[15] *United States v. Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

[16] *United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987), and *United States v. Duggan*, 743 F.2d 59, 73 n.5 (2d Cir. 1984)

[17] *United States v. Duggan*, 743 F.2d 59, at 78 (2d Cir. 1984) and *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987).

[18] *United States v. Megahey*, 553 F.Supp. 1180 (E.D.N.Y. 1982) *aff'd sub nom. United States v. Duggan*, 743 F.2d 59 (2nd Cir. 1984); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987); *United States v. Badia*, 827 F.2d 1458 (11th Cir.1987), *cert. denied* 485 U.S. 937 (1988); *United States v. Johnson*, 952 F.2d 565 (1st Cir. 1991), *cert. denied* 506 U.S. 816 (1992).

[19] PL 107-56, October 26, 2001, 115 Stat 272, § 218 (amending 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)).

[20] *In re All matters Submitted to Foreign Intelligence Surveillance Court*, 218 F.Supp. 611.

[21] *In re Sealed Case*, 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev., 2002).

[22] *Id.* at 736.

[23] *Supra* note 21 at 743.

[24] *Supra* note 21 at 723; 50 U.S.C. § 1801(a)-(e).

[25] *Supra* note 21 at 736.

[26] *Supra* note 21 at 733; 50 U.S.C. § 1806(k).

[27] 50 U.S.C. § 1801(b) distinguishing between agents of a foreign power who are U.S. persons and non-U.S. persons and setting out a somewhat higher standard for a U.S. person to be considered an agent of a foreign power; § 1801(e) setting out a stricter definition of foreign intelligence information where U.S. persons are involved.

[28] 50 U.S.C. § 1805(a)(3)(A); § 1824(a)(3)(A); § 1842(c)(2).

[29] 50 U.S.C. § 1801(h); § 1805(f); § 1806(a),(j); § 1821(4); § 1824(e)(4); § 1825; § 1843(c)(2); § 1845.

[30] *Supra* note 1, § 203a, amending Rule 6(e)(3)(c)(I)(V).

[31] *Supra* note 1, § 203b.

[32] *Supra* note 1, § 905.

[33] *Supra* note 1, § 201, amending 18 U.S.C. 2516(1).

[34] *Supra* note 1, § 206, amending 50 U.S.C. § 1805(c)(2)(B).

[35] 50 U.S.C. §§ 1841-1846.

[36] *Supra* note 1, § 214, amending 50 U.S.C. § 1842(c)(2).

[37] *Supra* note 1, §§ 214 and 216 (amending 50 U.S.C. §§ 1842, 1843, and 18 U.S.C. §§ 3121, 3123, and 3127).

[38] *Supra* note 1, § 216 (amending 18 § 3123; 3123(b)(1)(C) no longer requires that geographic limits be specified; however, 3127(2)(A) imposes a "nexus").

[39] *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986); *United States v. Ludwig*, 902 F.Supp. 121 (W.D. Tex. 1995); *United States v. Villegas*, 899 F.2d 1324 (2nd Cir.1990); *United States v. Pangburn*, 983 F.2d 449 (2nd Cir. 1993).

[40] *Supra* note 1, § 213, amending 18 U.S.C. § 3103a.

[41] Adverse result is defined as one resulting in endangering a life or a person's physical safety; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; serious jeopardy of an investigation or undue delay in trial; *see* 18 U.S.C. § 2705(a)(2).

[42] *Supra* note 1, § 219, amending F.R.C.P. Rule 41(b)(3). International terrorism is defined in Title 18 U.S.C. § 2331(1); domestic terrorism is defined in 18 U.S.C. § 2331(5).

[43] There is an exception to this rule for movable objects; see F.R.C.P. Rule 41(b)(2).

[44] *Supra* note 42.

[45] *Supra* note 1, § 224(a).

[46] *Spano v. New York*, 79 S. Ct. at 1206 (1959).

[47] *Olmstead v. United States*, 48 S. Ct. 564 at 572-573 (1928).

Law enforcement officers of other than federal jurisdiction who are interested in this article should consult their legal advisors. Some police procedures ruled permissible under federal constitutional law are of questionable legality under state law or are not permitted at all.

The Bulletin Notes

Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. The *Bulletin* also wants to recognize those situations that transcend the normal rigors of the law enforcement profession.

Officer Tillman

Heading home from his daily tour of duty, Officer Christopher R. Tillman of the Danville, Virginia, Police Department witnessed an apartment building engulfed in flames. Without hesitation, he exited his vehicle and ran toward the burning complex. Hearing a child screaming from inside, Officer Tillman kicked down the front door and rescued a 5-year-old boy from the flames. Once the child was safe from the flames and the falling electrical wires outside, Officer Tillman returned to the burning building to assist any other occupants. Over the next few minutes, he rescued three adults and two children from the fire. Officer Tillman's courage and quick judgement saved the lives of all six individuals.

Corporal Larner

Corporal Martin J. Larner of the Rosenburg, Oregon, Police Department responded to the scene of a terminated pursuit involving a suspect and other officers. The suspect previously had fired several shots at officers during the pursuit, then fired several additional shots into the air after wrecking his vehicle and finally rolling to a stop. The suspect then held a weapon to his head at various intervals during the subsequent negotiations. Corporal Larner, who also is a marksman with the department's tactical team, directed officers into a perimeter to contain the suspect, divert traffic, and protect neighboring residents. After nearly an hour of negotiations, the suspect exited his vehicle to urinate and turned his back to the officers. Corporal Larner used the opportunity to tackle the suspect from behind, even though the suspect still was holding a rifle. The courageous actions of Corporal Larner prevented the subject from harming himself or others and precluded the need for greater force being used to end the standoff.

Nominations for the ***Bulletin Notes*** should be based on either the rescue of one or more citizens or arrest(s) made at unusual risk to an officer's safety. Submissions should include a short write-up (maximum of 250 words), a separate photograph of each nominee, and a letter from the department's ranking officer endorsing the nomination. Submissions should be sent to the Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 209, Quantico, VA 22135.

U.S. Department of Justice
Federal Bureau of Investigation
FBI Law Enforcement Bulletin
935 Pennsylvania Avenue, N.W.
Washington, DC 20535-0001

Official Business
Penalty for Private Use $300

Periodicals
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Patch Call

The patch of the North Bend, Oregon, Police Department features the McCullough Bridge, built in 1936, which spans Coos Bay from North Bend to Glascow, Oregon. The tree and sunset symbolize the beauty and serenity of the southern Oregon coast.

The city of Show Low, Arizona, received its name as the result of a game of Show Low Poker between two ranch owners; the winner gained sole possession of the ranch. This tale became widespread and the city of Show Low later was created nearby. The patch of the Show Low Police Department features a deuce of clubs, the winning card in the game and the namesake of the city's main street.