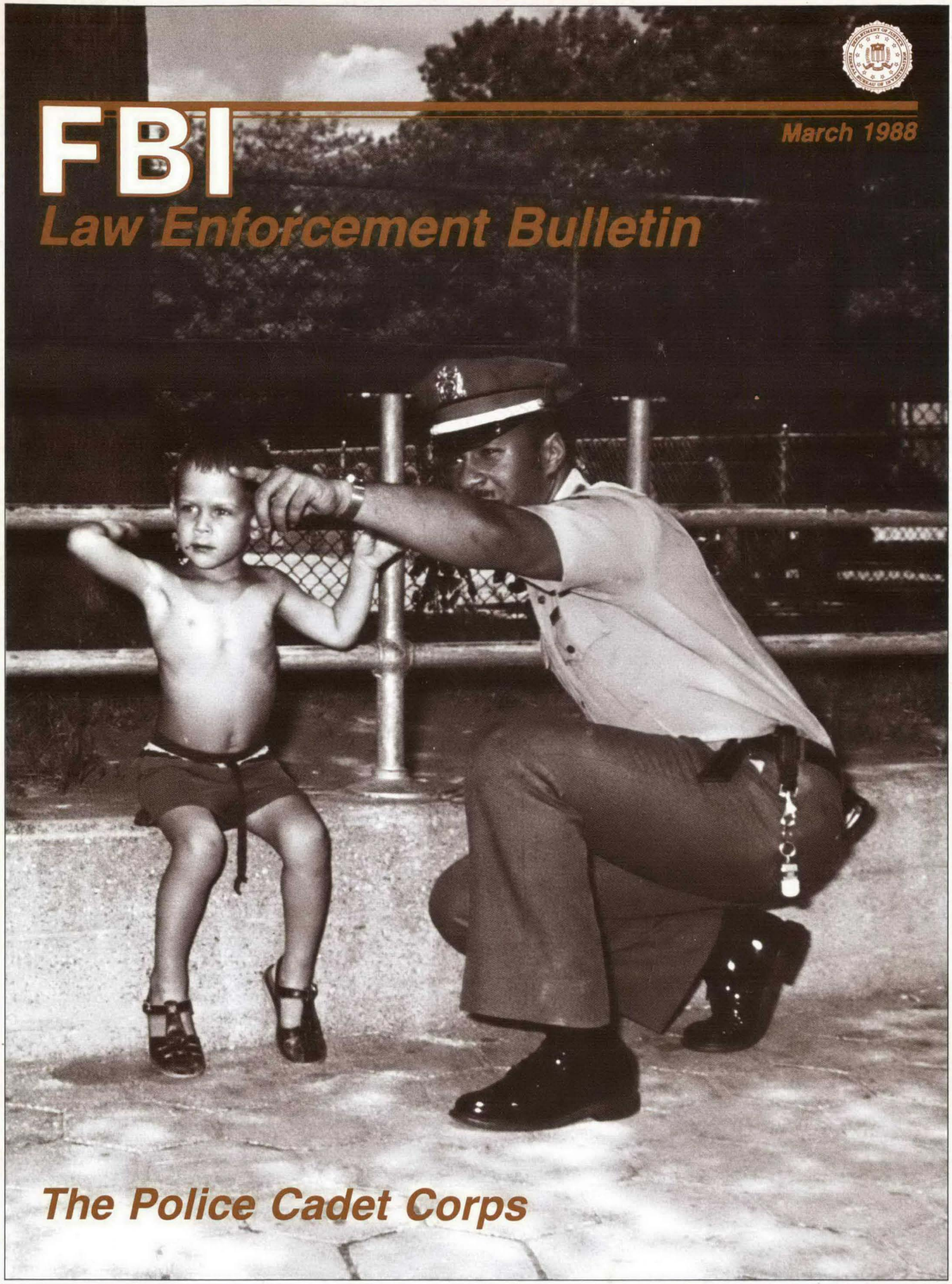
FBI
Law Enforcement Bulletin

March 1988



The Police Cadet Corps

Contents

March 1988, Volume 57, Number 3

Personnel — 1 **Recruiting Police From College**
By Ordway P. Burden

White Collar Crime — 7 **Executing Search Warrants in an Office Automation Environment**
By Charles Luisi, Wallace R. Zeins, and Alan E. Brill

Training — 12 **Law Enforcement and Financial Institutions: A Need to Train and Communicate**
By Roger Zeihen, Michael Zeihen, and Thomas E. Burg

15 **Book Review**

White Collar Crime — 16 **Operation Defcon: A Multiagency Approach to Defense Fraud Investigations**
By Kathleen L. McChesney

Investigative Techniques — 20 **Power Theft: The Silent Crime**
By Karl A. Seger and David J. Icove

Legal Digest — 26 **The Electronic Communications Privacy Act: Addressing Today's Technology (Part II)**
By Robert A. Fiatal

31 **Wanted by the FBI**

FBI
Law Enforcement Bulletin

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

William S. Sessions, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs,
Milt Ahlerich, *Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Production Manager/Reprints—Mark A. Zettler

The Cover:

A police cadet gains field experience assisting a lost child (see article p. 1).

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-Class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688 USPS 383-310

Recruiting Police From College

"The Police Cadet Corps is based on the notion that if the city assists young people in paying for their education and gives them a closeup look at police operations, many of them will choose a police career after graduation."

By
ORDWAY P. BURDEN
President
Law Enforcement Assistance Foundation
and
Chairman
National Law Enforcement Council
Washington, DC

Late this spring, approximately 130 young men and women who have spent 2 years as police cadets in the New York City Police Department (NYCPD) will graduate from college. It will be the first moment of truth for an ambitious attempt by the NYCPD to recruit college graduates into police service. Will the graduating cadets choose to join the regular force?

The city is betting $1 million a year that many of them will. If so, it will raise the educational level of the department by only a fraction, because more than 2,000 of its 32,000 members already have college degrees. Yet, it will be a strong indication that the police cadet idea is viable.

The Police Cadet Corps is based on the notion that if the city assists young people in paying for their education and gives them a closeup look at police operations, many of them will choose a police career after graduation. The cadets are given loans totaling $3,000 toward the expenses of their last 2 years of college. If they serve at least 2 years after graduation, the loans are forgiven; if not, they must repay the loans with 3 percent interest.

As cadets, they are paid $7 an hour for two summers of full-time work and 3 days a month during their college years. Most of their service is done as observers with the Community Patrol Officer Program (CPOP) in 45 of the city's 75 precincts. Precinct CPOP units are comprised of 7 to 10 officers, under the command of a sergeant, who patrol neighborhoods and try to improve the quality of life, as well as arrest wrongdoers. The cadets wear uniforms that are quite similar to a patrolman's, but carry no weapons and have no law enforcement powers. Like the regular officers, they are issued bulletproof vests.

A typical cadet, a senior at City College of New York who was assigned to the 79th precinct in the Bedford-Stuyvesant section of Brooklyn, is enthusiastic about the work. "CPOP is a fabulous program. We attended community board meetings, tenant association meetings, block parties. Sometimes we talk to crime victims and tell them about compensation that's available to them. And people would come up to us and tell us about the problems they have with drug dealers or parking problems. We also escorted senior citizens to the bank because if they went by themselves, it's very likely they would be robbed."

Mr. Burden

This cadet recalls only one incident in two summers of patrol that was outside the service routine. That occurred when the patrol officer he was with arrested a purse snatcher. "But," he said, "helping people is exciting in itself to me." He admitted thinking about becoming a police officer before joining the Cadet Corps. "Now, " he added, "there's no question that I will."

This attitude reflects the police department's belief that college graduates may bring greater sensitivity to the officer's job. The Cadet Corps commander commented, "The feeling is that people who have been exposed to a broad education will be more able to deal with the complex job of policing that's facing us. I think the people with the education will be able to handle more things, more confidently, and to understand the things that might be unfolding before his eyes, like the poverty we see, the homelessness."

"A person who has not been exposed to the reasons for some of these conditions might be prone to say that it's because people don't want to work that they're homeless," he added. "If you have a narrow point of view and think they're homeless because they're lazy, then you might receive a homeless person who is coming to you for help as a police officer in a different manner than if you have a broader view and know that there are a multitude of reasons why people are homeless."

Some research indicates that in addition to having such intangibles as greater sensitivity, college graduates also perform better than their less-educated colleagues in measures that can be quantified. For example, in a study that compared the first 10 years of service by officers who joined the Los Angeles Police Department in 1965, B. E. Sanderson found that the college graduates did significantly better in the police academy, had fewer sick days and injured-on-duty days off, were less likely to be disciplined, and were much more likely to be promoted.

Other research has suggested that college makes little difference in police performance and may even be a detriment if less-educated officers resent the college men. In any case, the question may be of the chicken-or-the-egg variety.

The director of the Vera Institute of Justice, who is chairman of the Police Cadet Advisory Council which helped to set up the Police Cadet Corps, noted, "It's an open question, in part because, as you might expect, whatever correlations are found between college education and performance measures like promotions, absences, or disciplinary actions, you're stuck with not being able to determine whether it's the college education that makes the difference or whether it's the mix of personality, ambition and talent that leads people to get a college education."

Cadets must be citizens and New York City residents and must attend college in the city or in adjoining Westchester and Nassau Counties. They must pass the examination for regular police officers; 98 percent of the cadet applicants do, as compared with 63 percent overall.

Their initial week of training is at the city's police academy, but it is less police-oriented than that for regular rookies. They take driver training and some physical education and close-order drill. In addition, they are given instruction in the use of walkie-talkies and

" 'We want to show them that there's something in the department for every college major. . . .' "

Police cadets receive in-class training.

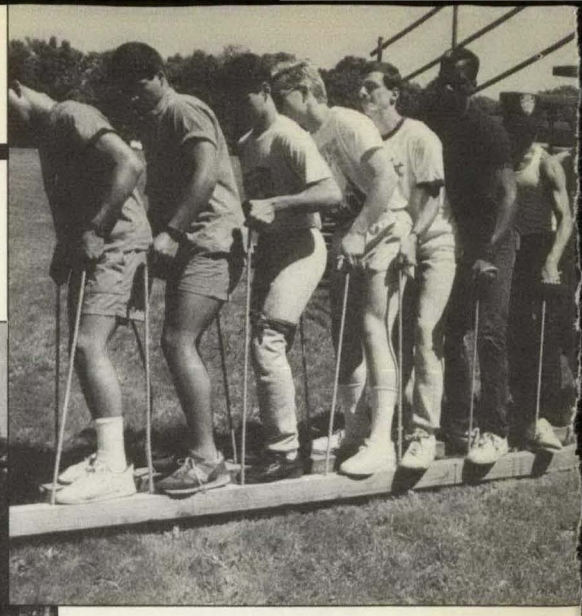
computers, but most cadet training focuses on leadership and management skills. "We try to be as non-police-specific as possible," added the corps commander. "We try to enhance and broaden their personal abilities."

In their second week of training, the cadets are given 4 days of physical and mental exercises aimed at melding them into a corps. "We recognize that they come from various communities throughout the city and they don't have the cohesiveness that we need," the commander explained. "So they go through these exercises that are designed to build team spirit, cohesiveness, and respect for leadership."

While original expectations were for the Police Cadet Corps to have around 400 members to start, only 332 have been hired thus far. Two-thirds of the cadets are men. The first class, hired in June 1986, is 71.5 percent white. But the latest hiring, in August 1987, reflects the city's composition more accurately. In this class, there are 38 whites, 33 blacks, 28 Hispanics, 1 Asian-American, and 1 Native American. Because the physical and mental requirements for cadets are as stringent as for regular officers, only 1 in 10 applicants make the grade.

Not surprisingly, many of the cadets were considering a law enforcement career before they joined the corps; about two-thirds were either committed to a police career or leaning that way. The department is hoping that the other one-third will be favorably impressed by their experience as cadets. As the corps commander noted, "Once they come in and are exposed to us, we think we can convince a lot of them to take a serious look at a career in policing. It's a career that can be very rewarding, very satisfying, in terms of serving people. We certainly hope that we will attract some of those who would, in ordinary circumstances, go to one of the Fortune 500 companies to come and be leaders in the department and provide a needed service to the people of the city."

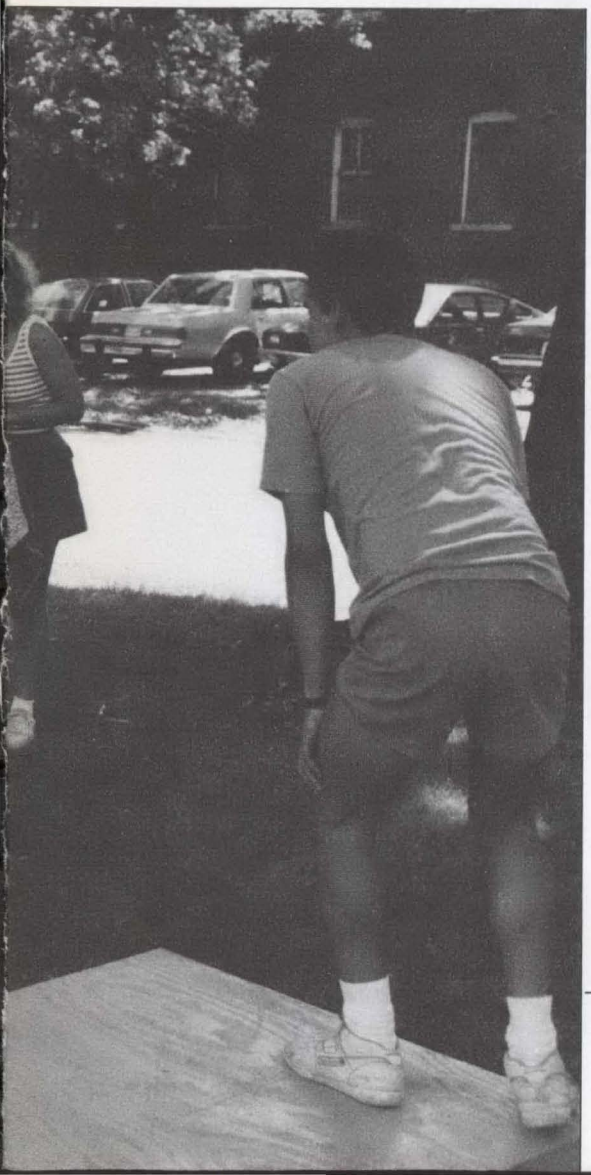
Some cadets join primarily to get the college loans. Some drop out when they face the reality of police work. A few have left the cadets to join the regular force immediately. But even those who drop out to pursue other careers aren't a complete loss to the city. In the commander's opinion, "They have seen the operation and will understand us better. The goodwill that is engendered from that relationship should go on for a long time."



Police cadets are given various tasks to develop teamwork and leadership skills.

One cadet who is undecided about a police career agrees with this opinion. "I'm really not sure whether I'll become a police officer," she said. "Right now I'm looking toward law. I think I probably will become an officer just to get the experience, but I'll continue my education, too. I think the training is great and really relevant whether you plan to go on and become a police officer or anything else. The things I've learned I'll never forget, and I can take them anywhere I go."

One of the things she has acquired is admiration for her tutors in the CPOP unit in the 114th Precinct in Astoria, Queens. She watched four officers subdue 15 battlers in a minor riot in a housing project and witnessed a drug arrest which she described as "beautiful, a work of art." In the drug case, she was riding in the CPOP van when she saw a man walk away from behind a post where he had been urinating. The CPOP officers stopped the van and began questioning another man who was working on his car in the street. The commotion attracted the walker back to the scene, whereupon the officers arrested him. "What happened was, the man hadn't been urinating, he was dropping vials of crack," she explained. "I don't know how the officers recognized he was doing that, but it was really good. There was no big, dramatic scene; it was a trick and I was really impressed."



In the beginning there was considerable concern about whether the cadets would be accepted by regular officers. "There was some apprehension among rank-and-file officers who didn't understand what the cadets are all about," the corps commander said. "There was an elitist-type stigma attached to the Cadet Corps because we are advertising that we wanted to increase the number of college-educated people in the police department and some officers thought it was a put-down. But as the cadets went out into the precincts and showed their mettle as good, energetic, motivated people who want to serve, the officers found out that these kids are like everybody else, and they began to accept them more readily."

Most cadets would agree. "At first we were tolerated," one cadet commented, "but then friendship grows. Within the CPOP unit you develop a sort of camaraderie. I'd say within a week or two we were accepted in the unit." Being accepted by the other 150-odd officers in the precinct took a little longer. "You do, I think, have to prove yourself," she added.

Police cadets are commanded to stay away when danger threatens, but sometimes cadets got involved in non-threatening situations. Once, for example, when a CPOP unit was summoned to an apartment where a woman had died, some of the cadets helped to console the woman's daughter. "I picked out her dress for the funeral and did things like that that she was too upset to do," said one female cadet. "We had some interaction like that with people in distress, but with crime, we were just observers."

Occasionally, some cadets accompanied officers when there was a potential for harm. One cadet joined the search for a handcuffed suspect who had escaped from police custody in the 70th precinct in the Flatbush section of Brooklyn. "When we got the call, natural instinct took over and everybody jumped out of the CPOP van and

" '. . . even if they were to perform no additional service, their presence in society would gradually have a positive effect on public life. Decency and order depend on both police and citizens.' "

started looking around the neighborhood," he said. When the cadet spotted the suspect in an alley, he shouted, "Police, don't move!" and joined in the subsequent chase through backyards. "But my officer was with me," he added. "You were never alone where you had to interact with a criminal or get yourself in jeopardy."

This cadet, a computer science major at Baruch College, was transferred to police headquarters to work in the department's computer unit for his second summer as a cadet. In that assignment, he helped to develop programming packages for the microcomputers that eventually will be in every precinct. "I had a great time down there," he said, "because the people were excellent and really knew their stuff."

Another cadet also spent the second summer at headquarters, working in the budget department. But most are assigned to CPOP units and with good reason. The corps commander explained, "The CPOP officers have been carefully chosen for liking to relate to people because that's what they're doing. We decided to put the cadets in CPOP units because we wanted those highly motivated officers to transmit that motivation to the cadets."

In the future, though, more cadets are likely to be exposed to other departmental operations. As an experiment last summer, some senior cadets spent 2 weeks visiting the department's special units — harbor, aviation, the special group that protects movie makers' sets, the computer unit, and the details for Yankee and Shea Stadiums, the Delacorte Theater in Central Park, city hall, and police headquarters. "We want to show them that there's something in the department for every college major," said the commander.

New York's Police Cadet Corps grew out of earlier proposals for adding more college-trained officers to the force. One plan, advanced by John Jay College of Criminal Justice and the Patrolmen's Benevolent Association, called for giving students who earned high marks on the police civil service test free tuition at John Jay and a $4,000 stipend to work 100 days a year in the police department. The other plan, proposed by a former chairman of the New York State Investigations Commission and a sociologist, was more sweeping. It would have created a statewide "police corps" of 30,000 who would get free college tuition in return for pledging 3 years of police service after graduation. New York City would have had two-thirds of them; the other third would be in upstate communities.

During their service as patrolmen, the Police Corps graduates would have received lower salaries and fewer benefits than regulars. It was estimated that a Police Corps grad could be put on the street for $20,000 a year, less than half of what a New York City officer costs in pay and benefits.

Critics of the Police Corps proposal pointed out that probably few members would serve more than their 3-year commitment. "True," said the proponents, "but even if they were to perform no additional service, their presence in society would gradually have a positive effect on public life. Decency and order depend on both police and citizens." The advocates added, "The professionalization and insulation of the police have often severed them from the communities they serve. The presence in society of well-trained, experienced former police officers in ever-increasing numbers would greatly aid efforts to mobilize the entire community to fight the criminality that is undermining our way of life."

The cadet plan finally adopted has elements from both proposals. Perhaps the chief difference between the Police Cadet Corps and the Police Corps plan is that cadets who join the department after graduation from college will become regular officers, with normal pay and benefits. The first duty, like all rookies, will be 5½ months of training at the police academy. There they will follow the normal curriculum, although they will be excused from the full driver training course if they took it as cadets.

The question now is, "How many of the cadets will opt for a police career?" Further down the road, there will be other questions, such as, "Will they stay in and how well will they perform?" The city will also have to decide whether the cadet recruitment package is sufficiently attractive to lure enough students to enlarge the corps. (In the original plan, the hope was that by the 1990's the department would be drawing half of its annual crop of 1,200 recruits from the Police Cadet Corps.) Some early answers to those questions will come after college commencements in the spring. FBI

Executing Search Warrants in an Office Automation Environment

By
CAPT. CHARLES LUISI
Chief Investigator
DET. SGT. WALLACE R. ZEINS
Deputy Chief Investigator
and
ALAN E. BRILL
Director
Investigative Support Information Systems
Department of Investigation
New York, NY

Editor's Note: This article does not address certain legal issues associated with executing a search warrant in an office environment. Law enforcement officers preparing to execute such warrants should consult their legal adviser.

In the past, execution of a documentary search warrant was a fairly straightforward business. Once the warrant was presented, you set about examining all documents that you could find, searching for those covered by the warrant, which you would log and seize.

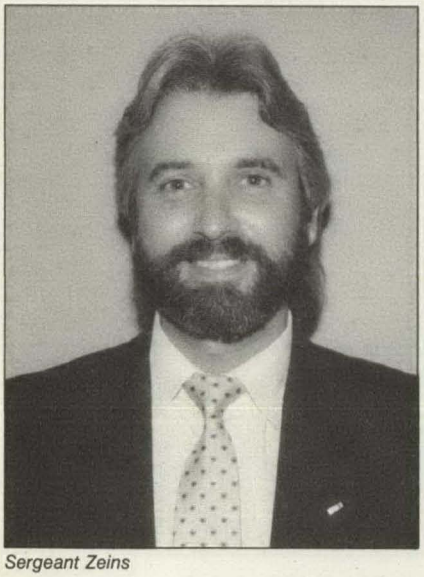
Today, most business organizations, even the smallest, have either memory typewriters or computer word processors. In today's technological environment, officers executing a warrant are faced with a series of challenges.[1] Does the search site contain computers or memory typewriters which could contain evidence? Does your warrant authorize you to search computer files or typewriter electronic memories? With memory typewriters, word processing programs, and personal computers, do you know how to read the memory, which may be in the form of tapes, disks, memory cartridges, or built permanently into the machine?

Identifying Office Automation

Before executing a search warrant, it is important to determine whether the site has computers or word processing memory typewriters. Computers range in size from room-sized mainframes to small, desktop personal computers. With their screens and printers, they are generally quite recognizable. However, there are small, laptop machines which can easily be concealed. Such small machines can store vast amounts of data.

The memory typewriter is frequently much more difficult to identify. While some have full TV-type screens, others have only a small display screen of one line and 10-40 characters. Still others have no special display and appear to be regular typewriters. Considering today's technological environment, it is wise to assume that all

Captain Luisi



Sergeant Zeins

typewriters have memory capabilities until it has been established on an individual basis that they do not. Therefore, to avoid intentional erasures of evidence, prohibit personnel at the search site from using any typewriter until the machine has been specifically cleared.

When examining a machine to determine whether it has memory features, first ask the operators if the machine can store documents or look at the labels. If it mentions the word "memory" or "word processor," it will have to be electronically searched. Next, determine whether there are removable storage devices. Look for slots where disks can be inserted and removed from the machine or memory cartridges that can hold hundreds of pages in an electronic memory chip. Some earlier-dated equipment store data on magnetic cards or tape cartridges. If the machine accepts any form of tape or disk, it has memory capabilities and must be searched.

On machines where there are no removable memory devices, carefully examine the keyboard for keys marked "store," "read," "write," "recall," "index," or any other similar markings. A key labeled "code" indicates that there are functions that can be called by pressing the code key either before or at the same time as another key. The code key is sometimes labeled "control" or "ctrl." On some older IBM memory typewriters, there is a control wheel adjacent to the keyboard with memory area numbers from 1 to 50 marked on it. When a machine has these keys or dials, it indicates that the machine has the capability of storing data within the machine itself. In such cases, avoid unplugging the machine at any time, as it is possible that some of the memory may be volatile and be lost if power is interrupted.

Because of difficulties associated with having to search unfamiliar equipment, it is important to obtain, if possible, a general description of the office automation equipment in use at the location to be searched. If a manufacturer and/or model number can be obtained, this obviously allows the search team to plan accordingly.

Of course, this is simply an extension of the intelligence gathering that always preceeds the successful execution of a warrant. In the case of office automation, this knowledge can be the difference between finding evidence or missing it completely. After all, those at the search site are not required to assist in the search. And instruction books, which are rarely found (once the operator understands the machine, the instructions are generally lost), are not particularly useful.

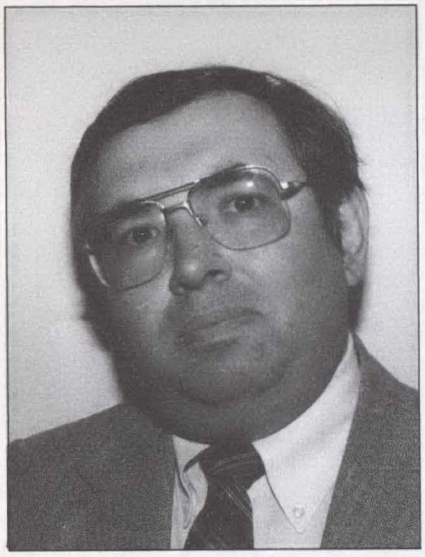
Realistically, it is practically impossible to become completely familiar with any piece of equipment in a short period of time from an instruction book. Remember that those who have information to conceal can use computers and business machines to their advantage. It is easy to hide completely the existence of a sensitive file from detection by the normal means described in instruction manuals.

Your list of intelligence gathering requirements, therefore, should include the following questions:

—Are there computers or word processors at the search site?

—If so, what brand and/or model?

—Are the machines used for word processing, data management, or financial analysis?



Director Brill

—What programs are used? If this can be determined, seek a person qualified in the use of the program to assist in the search.

—How sophisticated is the target organization in the use of their equipment? Sophisticated users can employ advanced techniques to hide data files.

Conforming Warrants to Technology

When defining the scope of the search warrant, it is important to include provisions authorizing the operation and search of automated systems. The language should authorize law enforcement officers to use the services of experts, as required. The warrant should also include authorization to search both the machine's memory and its machine-readable files. The following language was used in a recent warrant executed for a U.S. attorney in the Eastern District of New York.

> "As some or all of the above described records may be stored by means of a computerized information system, the items and materials to be searched shall include the following equipment components: central processing unit, printers, terminals (keyboards and display screens), magnetic tape drives, and magnetic disk drives; and storage media: magnetic tapes, magnetic disks, punched cards, paper tapes, and computer printouts. The Deputy United States Marshals conducting this search are authorized to utilize the services of computer experts, who may not be federal law enforcement officers, in order to use and operate the computer terminals at the above specified location for the purpose of retrieving the above specified computerized record information during the course of the above authorized search, provided that such experts operate under the direction, supervision, and control of the Deputy United States Marshals."

Recent changes in technology warrant a recommendation that this wording be expanded to include optical disk drives and optical disk storage media. Devices using laser technology are scheduled for wide use within the next year and will permit storage of up to one gigabyte (1,000 million characters) on a single 5¼-inch diameter optical disk. New devices also permit paper files to be replaced by video disks, each of which can store 100,000 or more document images.

Conducting Automation Searches

A technically qualified staff, proper supplies, and a plan of action are needed to conduct a search. As noted above, there are hundreds of combinations and permutations of hardware and software in use. Your ability to properly execute the search warrant depends on your ability to locate people that can search the office automation equipment. There are several sources.

Your department may use computers or office automation and those involved in the development or use of these systems, even if they are administrative rather than sworn personnel, are the first place to look for help. Identify those who have knowledge of or experience with computers. (A growing number of sworn personnel have home computers and routinely use word processing and data management programs in their investigations.) In larger departments, more permanent arrangements can be made. At the New York City Department of Investigation,

"...the degree to which you obtain the evidence you are seeking will depend in large part on your ability to search computer-based information storage and processing systems."

the Investigative Support Information Systems Unit, which develops in-house systems, provides the technical support for searches of automated offices.

Look to other government entities for assistance. While the police function may not have an in-house staff of technical experts, another agency may. In a cooperative local/State/Federal investigation, one law enforcement organization may well be able to support the other with a technical staff.

Many departments have established a working relationship with the computer stores where they purchase their equipment. In some cases, it may be possible to gain the cooperation of the store's technical staff for assistance.

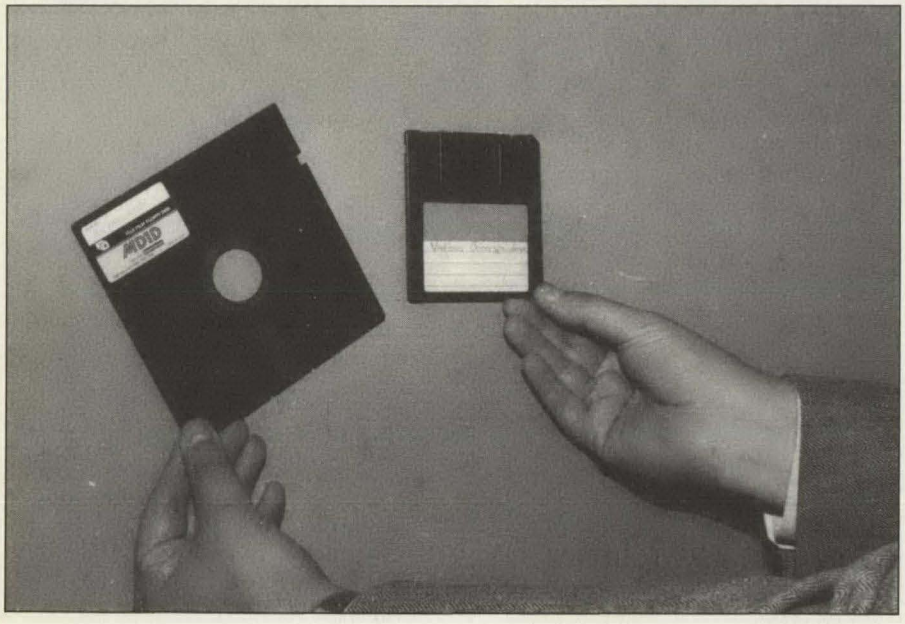
Determine whether there are consultants who could assist on an "as needed" basis. While many require payment of fees, some—particularly larger firms—may provide the service on a *pro bono* basis.

Once the staffing for the search is determined, supplies become important. While it is possible to seize small business machines, others are too cumbersome. And the cost of safeguarding a large machine for a long period when it must be left on site may be excessive. Therefore, take along on the search everything needed to operate the computer successfully and produce any evidence contained therein, e.g., blank computer printout paper, blank disks or tapes to copy files, and appropriate software. We routinely bring along programs that will enable us to copy files, examine them, and even remedy cases in which search targets suddenly erase files from their disks when the warrant is first executed. We can, in most cases, actually "unerase" the files using low-cost software.

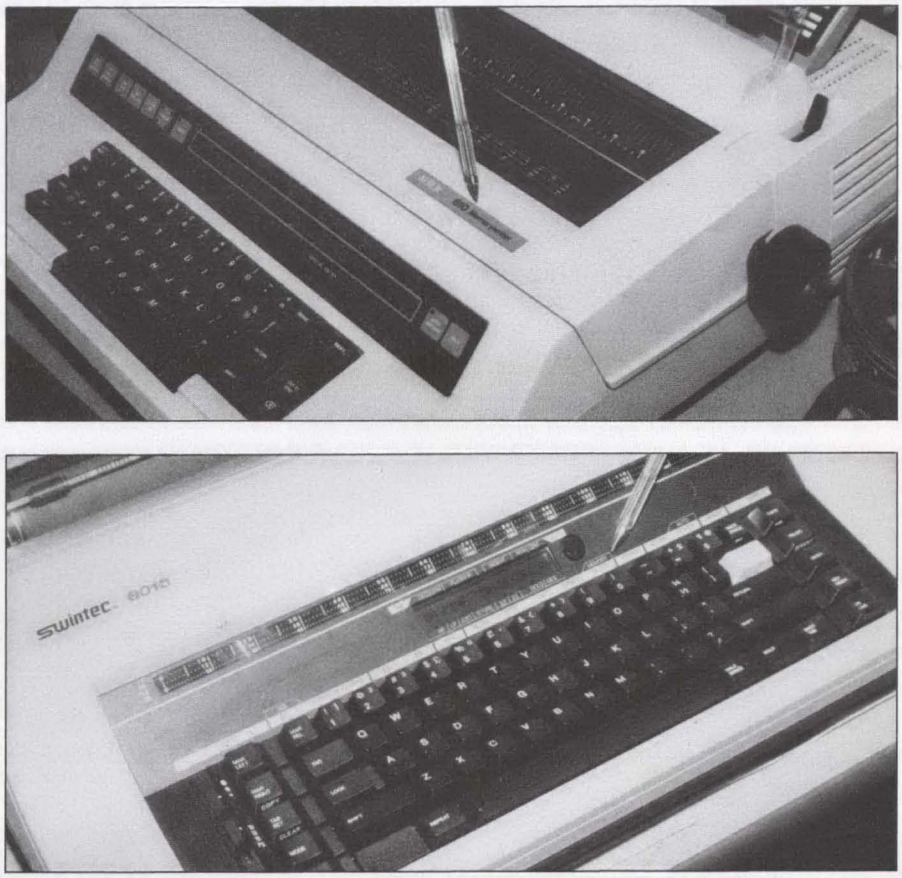
This brings up a vital point. It is very easy to destroy computerized records. On most computers, typing a simple command is all that is needed to blank out millions of characters of disk storage within seconds. Therefore, as a matter of policy, immediately take steps to move personnel at the search site away from all business machines, including typewriters, when the search warrant is executed. In these cases, seconds literally count.

Procedurally, the search of a machine is no different than a search of a file cabinet. It should be done by a team of two persons, a "searcher" and a "recorder." Begin by making an inventory of the storage media, identifying those disks or tapes that will have to be electronically searched. Remember that the label on a disk may not represent its true contents! Also remember that most personal computers have "hard disks" built into them that are not visible, but which hold tens of millions of characters of data. On memory typewriters, too, the storage devices may well be incorporated into the basic structure of the machine and not be a separate device.

For each disk or tape (including built-in disks or memory devices), proceed to identify the files stored. This may be done through the use of word or file processing software or by the use of the computer's built-in directory



These magnetic disks can store up to 1 million characters of text or the equivalent of 400 pages.



When examining a machine, look for indications of a memory capability.

search commands. Sophisticated users can easily hide files so that the names of selected files will not show up on normal directory listings. Consider the use of special software to identify these hidden files.

Examine each file on the screen to determine whether it falls within the bounds of the warrant. Consult with the prosecutor to determine whether, should you find relevant material, to seize the original files (which in many cases require seizing the entire machine that may contain volumes of material that are beyond the scope of the search warrant), or simply print out the file and mark it appropriately. In the case of large data base files, the appropriate option might be to produce a copy on your own magnetic disks. Of course, the copying process would have to be fully controlled and documented to assure that the copy was faithful to the original file in all respects. The specific evidentiary requirements for computer files and computer-produced data are beyond the scope of this article and differ by jurisdiction. However, these requirements should be included in the planning.

Conclusion

Computerized records represent the most significant challenge to those executing a documentary search warrant. As technology evolves, more and more businesses, individuals, and governmental bodies will have increasingly sophisticated office automation systems. Clearly, the degree to which you obtain the evidence you are seeking will depend in large part on your ability to search computer-based information storage and processing systems.

FBI

Footnote

John Gales Sauls, "Raiding the Computer Room: Fourth Amendment Considerations," *FBI Law Enforcement Bulletin*, vol. 55, No. 5 (Part 1) May 1986, p. 25; No. 6 (Conclusion) June 1986, p. 24.

Law Enforcement and Financial Institutions

A Need to Train and Communicate

". . . cooperation between all levels of the law enforcement community and financial institutions . . . can lead to an increase in arrests and the successful prosecution of criminals."

By
CAPT. ROGER ZEIHEN
Kenosha County Sheriff's Department
Kenosha, WI
MICHAEL ZEIHEN
Special Agent
Criminal Investigation Division
Internal Revenue Service
Wausau, WI
and
THOMAS E. BURG
Special Agent
Federal Bureau of Investigation
Wausau, WI

To the criminal mind, financial institutions are the pot of gold at the end of the rainbow. Many dream of walking off with the loot from a bank robbery, and most bank robbers are prepared for a violent confrontation to accomplish this objective. As such, all financial institution robberies must be considered very volatile and extremely dangerous.

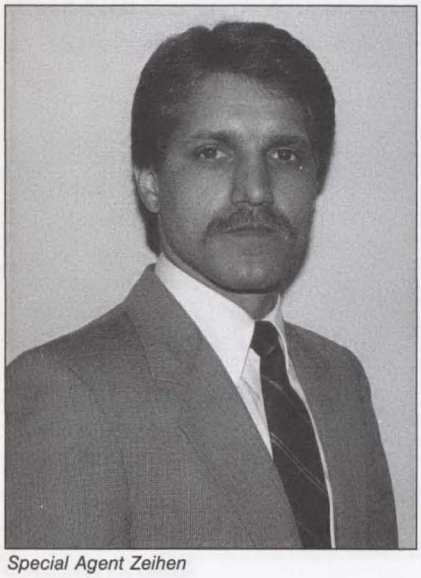
Robberies of financial institutions are a fact of American life. Since the first bank robbery by Frank and Jesse James over 100 years ago, this country has witnessed an abundance of this criminal act. Until recently, the rate of occurrence continued to increase. In fact, according to FBI statistics from 1975 to 1979, the rate increase was 48 percent. Recent rates of occurrence, however, appear to have leveled off.

As of October 1, 1987, FBI statistics showed that the solution rate of 1986 financial institution robberies was approximately 63 percent. This figure, as well as the rate of occurrence, may be improved through increased cooperation and coordination between law enforcement and financial institutions.

The Bank Protection Act (BPA) of 1968 mandated, among other things, the development of security procedures, a minimum level of security devices, and provisions for periodic training and retraining of employees of federally insured institutions. Enforcement of this act, as well as responsibility for investigating robberies, etc., falls within the jurisdiction of State and local law enforcement agencies, in cooperation with the Federal Bureau of Investigation.

The Bank Secrecy Act (BSA) of 1970 requires banks and certain other financial institutions to keep records and file certain reports, including currency transaction reports, which can provide law enforcement agencies with important information about possible criminal activity. Enforcement of the

Captain Zeihen



Special Agent Zeihen

provisions of the BSA is primarily the responsibility of the Criminal Investigation Division of the Internal Revenue Service. Since questions pertaining to the BSA, or indications of violations against it, are most likely reported to the agency most frequently involved with the financial institution, all levels of law enforcement should be familiar with the provisions of the BSA. It is also essential and beneficial to police operations that agencies maintain liaison with financial personnel in their jurisdiction who supervise the recording of these transactions.

In the financial arena, cooperation between all levels of the law enforcement community and financial institutions is vital. Cooperative investigative efforts can lead to an increase in arrests and the successful prosecution of criminals.

An important aspect of this cooperation is the training which can be provided by law enforcement agencies. Training increases the awareness of financial institution employees to suspicious persons and/or prepares them to react properly should a criminal act occur in their presence. This is particularly important in view of the changes that have evolved in the financial community.

For the most part, most financial institutions were located in the heart of the community. The amount of citizen activity around these institutions made the criminal hesitant to act. However, within the past few decades, small satellite financial facilities have emerged in the urban and rural areas of our country. These institutions, with their small number of employees and reduced citizen activity, appeal to the criminal because of their apparent vulnerability. For this reason, financial institutions and their employees must be better prepared to handle criminal activity and to work closely with law enforcement in an attempt to prevent and properly respond to any such activity.

Training Considerations

The primary purposes of coordinated law enforcement/financial institution training are:

—To assure the safety of everyone involved in a holdup situation (bank employees, customers, law enforcement officers, and criminals);

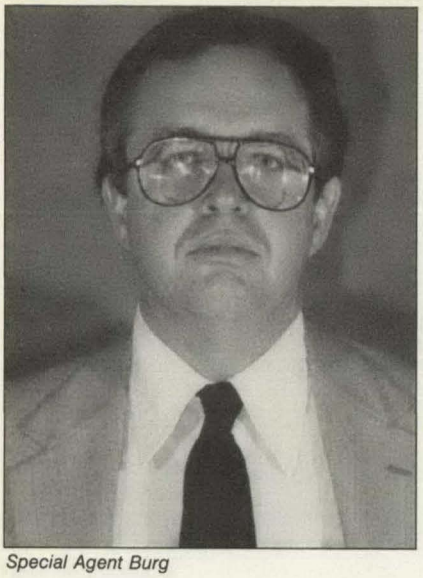
—To teach employees how to be attentive to suspicious persons and activities and what to look for during a robbery (i.e., to make them witnesses rather than victims); and

—To minimize the losses of the institution.

To accomplish these goals, training programs can be conducted at the individual institution or at a separate training facility.

On-site training allows representatives of the law enforcement agencies to discuss the actual security devices of the institution, examine the layout for problem areas, and answer specific questions of those attending. On-site training is recommended when a number of employees from a particular institution have to be trained, e.g., for larger institutions in metropolitan areas.

Joint training of employees of several different institutions can be accomplished at a separate training site. While this precludes specialized training, it is more manpower efficient to the



Special Agent Burg

law enforcement agencies. However, whether the training session involves one or many financial institutions, law enforcement and financial institution understanding and coordination are enhanced.

Coordination of training among the various law enforcement agencies and financial institutions not only educates employees but redefines each other's roles in the event of a robbery. Representatives from every law enforcement agency involved in the training should attend all sessions and be familiar with his or her department's operations. This facilitates the implementation of any modifications to policy or operations arising from the training discussions.

Financial institutions should require all employees to receive this type of training. Untrained employees, particularly those recently hired, may be reluctant to activate the necessary alarms, fearing a confrontation in the bank. Being aware of a law enforcement officer's duties in a silent response plan, i.e., to remain out of the institution and out of sight until assured safe entry, will instill confidence in activating alarms at the earliest possible moment.

Coordinated training accomplishes two important objectives. First, it updates each law enforcement agency's response operations, while at the same time standardizing the procedures in one locality. It also eliminates the uncertainty in the minds of financial employees should suspicious activities occur.

If conducted at the financial institution, training sessions should last no longer than 90 minutes and take place just prior to opening or after closing to allow for maximum attendance. It is recommended that some form of compensation be given to those attending an off-site location or for time spent which exceed normal working hours. Such compensation may prevent attendance problems and/or employee resentment and may increase enthusiasm and participation.

Training topics can be tailored to the particular institution or the employees. However, it is suggested that the following be incorporated into each session:

—General Security Procedures—including locking cash drawers at all times, keeping money out of reach of customers, limiting tellers to handling only their cash drawers, providing and replacing bait money, and protecting funds transported outside the institution,

—Safety and Protective Devices—including where they are located and how they operate,

—Specific Robbery Precautions—including low cash drawer limits and employee alertness to suspicious activity inside and outside the building,

—Specific Employee Actions During a Robbery—including the consideration of everyone's safety, complying with demands, giving bait money, handling demand notes and/or other evidence, observing what was said and done, and activating silent alarms and/or surveillance cameras,

—Specific Employee Actions After a Robbery—including the protection of the crime scene, notifying law enforcement officials, separating witnesses, and completing description forms, and

—Familiarization with Hostage/Extortion Situations.

Presentations should be kept simple and practical, yet interesting. This can be accomplished through the use of visual aids, by relating the topic being discussed to the physical layout of the institution where the training is taking place, or by explaining past robbery experiences. Visual aids (movies, video tapes, slides, etc.) can be obtained from the FBI, State training and standards bureau, security companies, and/or the financial institutions themselves. Using these training techniques eliminates boredom and increases comprehension.

Law enforcement agencies and financial institutions can work together to deter crime. Cooperative training programs, which can affect the occurrence and solution rates of financial institution robberies, are just one way toward this common goal. Also, well-trained, informed employees enhance personal safety and increase understanding of each other's roles. By exchanging information on physical operations and investigative techniques, i.e., by providing the most complete training possible, both the law enforcement and financial communities are better prepared to confront the crime problem of financial institution robberies. FBI

Book Review

Cop World: Inside An American Police Force by James McClure, NY, Random House, 1984, $16.95 (paperback, Laurel, NY $4.95)

The San Diego, CA, Police Department has a new look, described in this book as "anti-macho" or not intimidating. Patrol officers are hatless on routine patrol (their issued helmets are kept in the trunks of their patrol cars) and cannot wear black gloves or mirror, aviator-style sunglasses. This is part of the C.O.P., Community Oriented Policing program, begun in 1974, and now implemented by Chief of Police Bill Kolender, who rose from the ranks to take over the department in 1977.

James McClure, a South African newspaperman, previously wrote *Spike Island*, a study of the Liverpool, England, police after he emigrated to England. *Cop World* is another first-hand look at a police department; the author participated in San Diego's ride-along program and presents an honest picture of the San Diego police at work. Patrol work, as every police officer knows, often resembles military combat: hours of sheer boredom punctuated by moments of sheer terror.

Police patrol officers, after some experience, realize that the majority of their work is not law enforcement, but the order maintenance that our society expects, to various degrees depending on community values. And the need for order maintenance comes from abuse of alcohol (and drugs, today), altercations between human beings, and automobiles. These three "A"s are the day-to-day work of the police. Each affects the other: alcohol-related fights, driving under the influence, etc.

A work such as *Cop World* gives a more accurate picture of the realities of policing than hours of television or movies, with their dramatic necessities. Ride-along programs should be required of Hollywood writers — and of academics who pontificate on the ills of policing. The author understands the nature of today's policing, the improvements that have been made in recent years, but best of all, he can articulate the hopes and fears of all patrol officers, in their own words.

—By Thomas J. Benkin, J.D.

Operation Defcon

A Multiagency Approach to Defense Fraud Investigations

". . . Operation Defcon . . . represents one of the first approaches directed primarily at kickbacks in the aerospace/defense industry."

By
KATHLEEN L. McCHESNEY, Ph.D.
Special Agent
Federal Bureau of Investigation
Los Angeles, CA

Over $55 billion of the Federal defense budget is spent annually in the greater Los Angeles area, which is home to 1,900 Government contractors and subcontractors.[1] According to the Federal Procurement Data Center, the State of California receives approximately 20 percent of Pentagon expenditures.[2] In fiscal year 1986, 10 Los Angeles-based companies[3] each received more than 200 prime defense contracts.[4] Thus, the opportunities for massive fraud, waste, and abuse exist within Southern California, as well as in many other areas of the country.

During 1984 and 1985, instances of defense procurement fraud became increasingly known to the FBI. Information was received from a number of aerospace and defense employees who were dissatisfied with a procurement system wherein buyers from prime and first-tier defense contractors frequently solicited kickbacks from vendors and suppliers in return for favorable consideration in issuing subcontracts and purchase orders. In October 1985, the FBI, the Department of Defense, Office of the Inspector General-Defense Criminal Investigative Service (DCIS), and the Internal Revenue Service (IRS) joined forces in Los Angeles to conduct an investigation, called "Operation Defcon," into kickback schemes related to defense contracts and subcontracts.

While the concept of a task force approach to address a particular Government fraud problem is not unique, the Los Angeles effort represents one of the first approaches directed primarily at kickbacks in the aerospace/defense industry. With the cooperation of defense contractors and executives, and the information provided by many long-term participants in kickback arrangements, the task force was able to complete the first phase of its investigation by July 1986. Defendants have pled guilty to a variety of Federal offenses, including violations of the Anti-Kickback Act,[5] Mail Fraud,[6] and Tax Evasion.[7] The subjects had received kickbacks on such projects as the U.S. Air Force F-16 fighter aircraft and the U.S. Navy F-18 fighter attack aircraft, the Air Force B-52 bomber, the Navy CH-53 helicopter, the Airborne Optical Adjunct Program for Army research relating to the U.S. Strategic Defense Initiative, the Army Black Hawk helicopter, and the NASA space shuttle solid fuel rocket booster. Most of the individuals charged had no criminal record and had been successful members of the aerospace community for many years.

Special Agent McChesney

Kickback Schemes

A typical kickback scheme begins after a military agency awards a contract to a prime contractor. The prime contractor may subcontract certain portions of the contract to "first-tier" contractors who perform a particular portion of the work needed to complete the contract. Both the first-tier and prime contractors generally require services, supplies, or other products to complete the contract. These items and services are generally obtained from local vendors or machine/fabrication shops.

In each level of contracting, the Government requires that qualified, interested parties be allowed to bid for work to be performed on Government contracts. An initial Government contract may be valued at several million dollars, and the value of the corresponding subcontracts or purchase orders may range from a few dollars to hundreds of thousands of dollars.

In order to obtain lucrative subcontracts or orders for goods or services that relate to the prime Government contract, vendors and suppliers will often aggressively "market" their business with buyers from the prime or first-tier subcontractors. Some vendors and suppliers may also use the services of "manufacturer's representatives."

Manufacturer's representatives represent several vendors or suppliers dealing in similar products and are occasionally middlemen in kickback schemes. The investigation uncovered such aggressive "marketing" techniques by vendors and suppliers as the provision of free meals, trips, automobiles, tickets, or personal loans. Similarly, buyers for prime or first-tier contractors may solicit gratuities or cash in return for subcontracts and purchase orders.

Buyers may operate the schemes on their own or work with other company employees (i.e., quality control, engineering, production, management). By working with production or engineering personnel, buyers are able to write requests for bids which are so specific that only one vendor is likely to be able to obtain the contract.

Vendors or suppliers attempting to obtain defense contract business are often willing to pay up to 10 percent of the face value of a purchase order or subcontract to a buyer if the work is awarded to them. Despite Federal legislation prohibiting kickbacks related to Government contracts and company ethics programs, the expectation of a 10-percent personal profit in the awarding of a subcontract or purchase order is a strong motivating factor for participating in a kickback arrangement. Because the kickbacks are generally in cash, few are reported as "income" to the Internal Revenue Service.

In most kickback schemes, a portion of the kickback is paid "up front" as the contract or purchase order is awarded. The remainder is paid when the contract performance has been completed. These schemes have the effect of falsely increasing the costs to the Government for goods and services. Some of the methods used in kickback arrangements include "bid rigging," "courtesy bidding," "sole source contracts," and "bid-bumping/overage."

Bid Rigging—In a bid rigging scheme, buyers or other procurement officials make discrete arrangements with a particular bidder from whom they accept some type of personal payment or gratuity. The selected company is provided proprietary information, including critical pricing data, which en-

"A cooperative relationship between the Government and defense contractors is paramount to kickback prevention."

ables the company to submit a bid that is either the lowest or contains enough specific information to make the company appear best suited for the contract. Bid rigging destroys competition and eliminates the opportunity for legitimate businesses to compete equally for Government contract work.

Courtesy Bids—A buyer or procurement official may conduct business regularly with several vendors or suppliers who participate in this scheme by submitting bids on all potential contracts. In each instance, the amount of the lowest acceptable bid is provided by the buyer to one selected vendor or supplier on a rotating basis. The selected vendor is awarded the subcontract or purchase order, while the other participating vendors provide higher, unacceptable bids as directed by the buyer. The vendor who receives the bid or purchase order is responsible for paying the kickback to the buyer. Vendors "take turns" at being the designated awardee. This scheme differs from bid rigging in that courtesy bidding requires the participation of several vendors or suppliers, whereas bid rigging occurs between the buyer and the contract awardee only.

Sole-source Contracts—While only a few "sole-source" contracts are involved in fraudulent schemes, this arrangement is an easy way to award contracts and purchase orders to a favored vendor. In this scheme, a vendor or supplier is designated by the buyer as a "sole source" for a particular part, product, or service. A sole-source designation infers that one particular vendor or supplier is the only acceptable, approved source of the product or service. Sole-source items are generally unique and rare and are likely to be very expensive. The sole-source nature of the items or service is often inaccurate or exaggerated. As in other schemes, the designated vendor or supplier pays a specified percentage of each contract awarded to the buyer.

Bid-bumping/Overage—Prior to issuing subcontracts or purchase orders, buyers are aware of the maximum amount a company is willing to spend on the subcontract. In this scheme, the buyer advises a vendor or supplier how much his proposed bid can be raised ("bumped up") and his company still win the subcontract. A portion of amount of the "bump" (usually 50 percent) is kicked back to the buyer. The "bump" or "overage" portion is in addition to the original kickback paid by the vendor to the buyer for the receipt of the subcontract or purchase order.

New Legislation

The Anti-Kickback Act of 1986 stagnated in Congress in mid-1986. However, following the massive publicity generated by the indictments of Operation Defcon defendants, congressional interest in the bill was renewed, helping to ensure the bill's passage in October 1986. The passage of the act amended and strengthened the original Anti-Kickback Act of 1946 to include solicitation for kickbacks and attempts to provide or offer kickbacks as criminal acts. The act increased the criminal penalty to a maximum of 10 years' imprisonment and a $10,000 fine per violation. A unique part of the act requires that prime contractors have procedures in place to prevent and detect violations of the act. Prime contractors or subcontractors must report possible violations in writing to the inspector general of the contracting agency.

The False Claims Amendments Act of 1986 provides that any individual who knows of false claims made by a contractor to the Government may file a Federal lawsuit against a contractor on behalf of the Government and himself.[8] The complaining party is entitled to receive from 15-30 percent of any recovery obtained in the case. The strength of the act is the provision for triple damages and its 10-year statute of limitations. The act, often referred to as "whistle-blower" legislation, also contains strong protection against the harrassment or firing of complaining witnesses.

Kickback Prevention

Notwithstanding the mandate set forth in the amendments to the Anti-Kickback Act, it is extremely important for defense contractors, or any other contractor involved in business with the Government, to establish policies with respect to gratuities and kickbacks. These policies, of course, should be in conformance with Federal and State law. They must be communicated to each employee and followup conducted to ensure that the employee understands the policy. Finally, internal controls have to be established to ensure adherence to the policies.

A cooperative relationship between the Government and defense contractors is paramount to kickback prevention. The experience of Operation Defcon clearly showed the contractors' dedication to dealing with the kickback problem. Communication be-

tween the investigators and company security personnel enabled the investigation to proceed without delay.

Contractors benefit from the cooperative relationship with Government investigative agencies, especially when unscrupulous buyers or other employees are identified. These buyers reap extra personal profits and deprive vendors and suppliers from participating in fair business practices. Vendors and suppliers benefit from Government investigations by the deterrent effect of a Government prosecution. The deterrent effect of a case like Operation Defcon is difficult to quantify; however, industry sources indicate that most buyers and vendors are aware of the Government's investigation and commitment to eliminating this problem.

Conducting business with the U.S. Government is unlike business conducted between private sector corporations. It has long been a common practice for many private businesses to show signs of appreciation to their customers with gifts or other remembrances. This practice, or the appearance of this practice, is not acceptable among those companies who conduct business using taxpayer dollars. Government contractors should take every precaution to avoid even the perception that they are involved in unethical business procedures.

Summary

The major advantage of any task force approach is the complementary effect of investigative resources. By combining the unique abilities and expertise of Special Agents from the FBI, DCIS, and IRS, the Operation Defcon task force is uniquely able to investigate kickback schemes. The inclusion of the IRS in this investigation has allowed the Government to include tax avoidance or tax evasion charges, in addition to kickback counts. In those rare instances where individuals did claim money generated from kickbacks as "income," the source of the income was disguised. In addition, continued assistance from the U.S. attorney's office is particularly important. From the outset of this investigation, prosecutors were intrinsically involved with legal issues and task force goals.

The task force is located in a centralized office, allowing for the essential daily contact between the investigators from the participating agencies. Extraordinary investigative expenses are shared among the FBI, IRS, and DCIS. As the investigation progressed, additional assistance to the task force was provided by the Defense Contract Audit Agency (DCAA) and the National Aeronautics and Space Administration (NASA).

In kickback cases, as in all Government fraud cases, it is critical that the FBI work closely with the affected (victim) Government agency. These agencies have access to necessary information and documentation which might otherwise be unknown or unavailable to the FBI.

Investigations of defense procurement kickback schemes in the Los Angeles and Southern California area are continuing. A special hot-line has been instituted to accept information from the public regarding defense procurement fraud. In addition, the FBI works closely with the Air Force Office of Special Investigation (AFOSI), U.S. Army Criminal Investigative Division (USACID), and the U.S. Naval Investigative Service (USNIS) to investigate other types of defense fraud. These investigations involve contract mischarging, false certification of testing, defective pricing, and product substitution.

Operation Defcon investigators remain committed to identifying, investigating, and prosecuting subjects involved in defense fraud. During 1987, the expertise developed in investigating kickback cases was used to conduct briefings and training sessions for over 200 investigators from various defense investigative agencies throughout the country. Information regarding defense procurement fraud investigations may be obtained from Operation Defcon task force members through the FBI, Los Angeles.

FBI

Footnotes

[1]"Top 25 Defense Contractors in Los Angeles County," *Los Angeles Business Journal*, August 3, 1987, p. 24; the dollar amount given includes military salaries and facility expenses.

[2]Ibid.

[3]The companies are Hughes Aircraft, McDonnell Douglas, General Dynamics, TRW, Lockheed, Northrop, Litton Industries, Garrett Corp., Todd Pacific Shipyards, and Computer Sciences Corp.

[4]Prime contracts are defined as $25,000 or larger.

[5]41 U.S.C. 51-54.

[6]18 U.S.C. 1341.

[7]42 U.S.C.

[8]31 U.S.C. 3729-3731.

Power Theft
The Silent Crime

By
KARL A. SEGER, Ph.D.
President
Corporate Consultants
Lenoir City, TN
and
DAVID J. ICOVE, Ph.D., P.E.
Senior Systems Analyst
Behavioral Science Investigative Support Unit
FBI Academy
Quantico, VA

In 1981, FBI Special Agents armed with Federal search warrants raided several east coast buildings in search of evidence of gambling. During the raid, these Agents discovered an unusual condition—the electrical power in one of the buildings had been intentionally bypassed.

The theft of energy is an economic crime that adversely affects all utility customers. Utilities estimate that 0.5 to 1.0 percent of all customers steal from them[1] and that their annual losses exceed $1.7 billion in electricity and $1.3 billion in natural gas.[2]

New Orleans Public Service, Inc., was one of the first utilities to recognize its power theft problem and to develop a program to combat it.[3] In 1971, the first year of the program, the company provided information to law enforcement authorities that led to 27 arrests and 25 convictions. About 10 years later, the annual figures reached 453 arrests and 447 convictions. Among those caught stealing that year were a prominent lawyer, an electrical engineer, a State legislator, and a high school principal. The company estimates that two-tenths of a percent of its customers currently steal power and that without an aggressive deterrent program, 10 to 15 percent would steal.

Consolidated Edison (New York) investigated 88,942 cases of suspected power theft and caught 12,000 customers stealing $7 million worth of electricity and gas in a single year.[4] Potomac Electric Power Company (Washington, DC, area) discovered 2,800 cases in 1 year and recovered nearly $800,000 from guilty customers.[5]

Energy thieves do not restrict themselves to major utility systems of metropolitan areas. Rural electric cooperatives and smaller municipal systems also report losses to thieves. In a national survey, a group of rural cooperatives reported that they suspected more than 2 percent of their members of stealing power.[6]

Residential customers are responsible for about 80 percent of all detected thefts, while commercial and industrial users account for the remaining 20 percent. However, commercial and industrial users account for an estimated 80 percent of all dollar losses. Usually, thefts by industrial users exceed $100,000, and in several cases,

Dr. Seger

Dr. Icove

utilities estimated losses of almost $1 million.

When a customer steals from the utility, the company absorbs the loss into its rate structure, making honest customers pay for it. Theft of services costs each customer in the United States about $30 per year in additional utility expenses.[7]

Committing the Crime

There are more ways to steal power than most utilities care to admit. Some techniques are very simple, but effective, while others are sophisticated and difficult to detect. The utilities, for obvious reasons, dislike publicizing the methods used to steal power. Although we understand their concerns, we have two reasons for deciding to discuss some of the more common methods used. First, law enforcement may find it difficult to detect and investigate a crime without knowing the modus operandi (M.O.) used to commit it. Second, consumers already can acquire this information in a number of different "How To" pamphlets currently available through the mail.[8]

Three of the most common methods used for stealing power include inverting the meter, placing straps behind the meter, or switching meters. Inverting most meters (turning the meter upside down) will cause the meter to run backwards, which actually takes watt hours off the reading. Remarkably, some customers get so greedy that they reverse too many hours off their meters. Thus, they show a net loss from one meter reading to the next.

Placing jumpers or metal straps behind the meter is an effective, though dangerous, way to steal electricity. If done correctly, some of the electricity will flow through the straps and the remainder will continue to register on the meter. Unfortunately, some of the thieves attempting to use this method have electrocuted themselves. Others have created dangerous conditions that have resulted in fires.

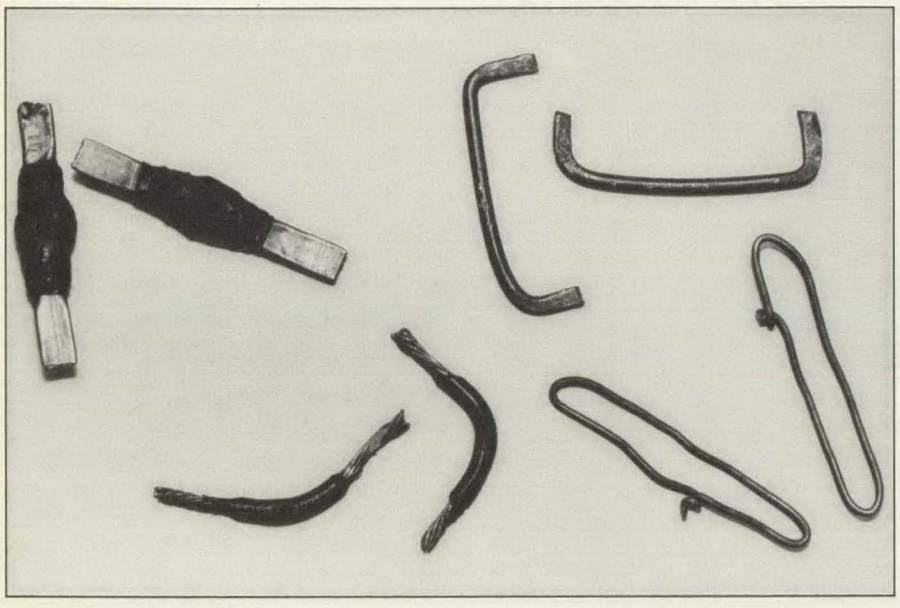
Some enterprising thieves steal an extra meter and place the spare meter in their socket for 10 to 15 days each month. Then, before the meter reader is scheduled to read their meter again, they put the meter provided by the utility back in the socket. Meter readers usually catch these people when they make random checks of the meters between meter reading cycles.

Other offenders drill or shoot a hole in the meter. They then use a piece of wire or coat hanger to put a drag on the wheel. They remove the wire and cover the hole with duct cement and a splash of paint before the meter reader returns.

Sophisticated power thieves either use elaborate bypass systems or tamper with internal mechanisms of the meter. Usually, they will install a bypass system at the weatherhead where the entrance cable attaches to the house and then runs to the other side of the meter. By placing a switch on the bypass, customers can decide when they want electricity to run through the meter and when they want it to run through the bypass.

Customers tampering with the internal mechanisms of the meter can simply bend the wheel to create a drag, or they can tamper with the meter's polarity to accomplish a similar objective. They also can modify registration of electricity by placing resistors in the meter.

"Power theft affects all consumers because it results in increased rates."



An assortment of various metal items used for jumping electrical meter sockets.

Combating the Problem

The first step in combating the power theft problem is for utilities to develop and maintain system integrity. Law enforcement agencies should encourage utilities to seal *all* meters and then inspect the seals regularly.[9] For this program to be effective, utilities must securely maintain the seals. Some utilities use plastic seals with serial numbers and require employees to sign for them by number. Others have lead seals and use crimping devices with distinctive patterns to close those seals. The utility will know that someone has tampered with the seal if they find the wrong serial number or crimping pattern on a seal at a customer's house.

Some older homes have meters located in basements or back rooms where the utility company cannot readily access them. Many companies move these meters to outside areas where they can visually inspect the meter when it is read. In areas where power theft has become a major problem, utilities can place these meters on utility poles high enough to be beyond the reach of the customer, but still easily readable by meter readers.

Utilities that closely monitor the amount of electricity used by customers can often detect a theft without looking at the meter. They can accomplish this task by having their data processing department conduct a comparison analysis of a current month's usage with the same month of the previous year. If they detect a decrease of more than 33 percent, they should inspect the metering system at that account.[10]

Law enforcement agencies should encourage utility firms in their areas to monitor all disconnected accounts, especially if they disconnected a consumer for nonpayment. Utility personnel should drive past the house at night several days after the utility has disconnected the service. If they see lights, they may then suspect that the customer is stealing. If a police officer sees electricity being used where it has been legally disconnected, he or she is witnessing either the theft of electricity or the receipt of stolen property, depending on the applicable legal statutes in his or her jurisdiction.

Investigating the Crime

Some utility systems have developed an in-house capability by using former police officers to detect and investigate power thieves. Most utilities, however, rely on their local law enforcement agency to assist them with the investigation and prosecution.

Utilities often initiate probable cause investigations after a meter reader detects a broken seal or other indications of tampering. The meter reader reports the condition to a supervisor or power theft investigator, who then conducts the investigation. At this point, some utilities will contact their local law enforcement agency, and an officer will accompany the utility investigator during the initial investigation.

If the investigator finds evidence of tampering, the area around the meter is treated like any other crime scene.[11] The investigator often prepares reports, takes photographs, and collects evidence. The handling and eventual disposition of the photographs and evidence will depend on any agreements between the law enforcement agency and the utility.

If the primary objective of the utility's power theft program is revenue recovery, the utility will collect and maintain the evidence. The law enforcement officer's role, in this case, is that of a witness to what was found at the scene. If the investigation results in prosecution or litigation, the utility will call the officer as a material witness. In these cases, the customer usually decides to reimburse the utility for the loss to avoid court proceedings.

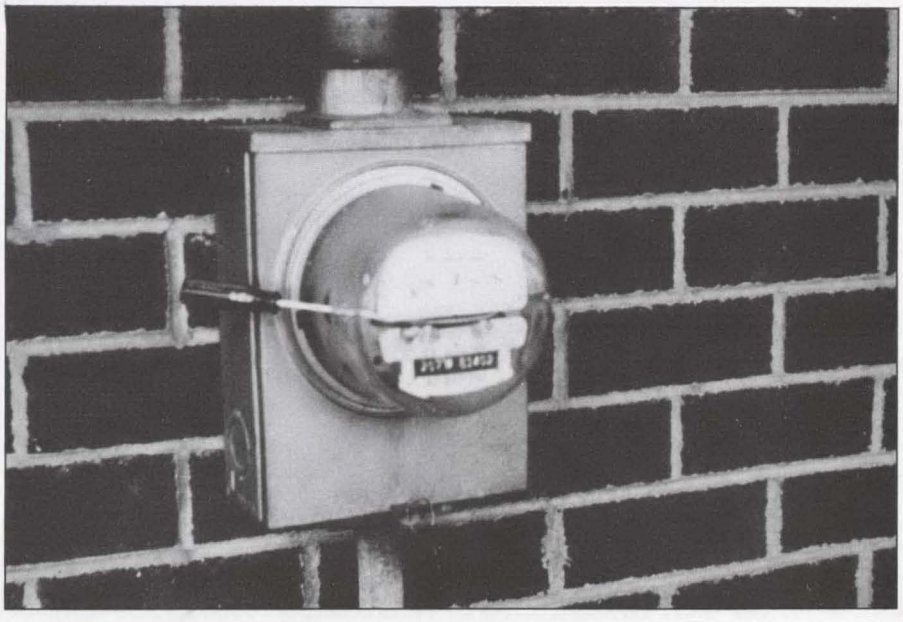
In jurisdictions where the utility and the police agency have decided to prosecute power thieves, the officer at the scene of the initial investigation usually will collect the photographs and evidence. The utility investigator serves as a material witness. In these cases, the utilities want to try to prove the customer's guilt. They hope the judge will require guilty customers to make restitution to the utility as part of the sentence.

A number of utility systems conduct their own investigation, and when warranted, take certain cases to their local police department. Other systems avoid criminal prosecution entirely. They prefer to use the civil judicial system, when needed, to deal with their power theft problems.

Prosecuting Power Thieves

Law enforcement agencies are not always aware of the extent of power theft and its economic impact, because when a utility catches a thief, it prefers to give the customer the opportunity to pay for the amount of electricity stolen to avoid criminal prosecution. This often is an effective approach when dealing with first-time offenders. On the other hand, dealing with repeat offenders necessitates criminal investigation and prosecution to combat the problem.[12]

Many States have laws that make meter tampering and power theft crimes punishable by a combination of a fine, imprisonment, or civil restitution.[13] Most power theft cases are investigated and prosecuted under two general sets of statutes. Meter tampering laws deal only with evidence indicating that someone tampered with the meter or metering system.[14] Investigation under these statutes tries to establish that the meter was tampered with and that the consumer charged with the crime did the tampering. Since



An example of one utility thief's method for slowing down an electric meter by using a screw driver inserted through a predrilled hole in the meter glass.

". . . the theft of utility services costs the United States over $3 billion every year . . . ."

it seldom is easy to prove who was responsible, some State statutes include a prima facie provision that assigns the presumption of guilt to the person(s) who benefited from the tampering.

The other set of statutes addresses the total power theft problem, including the dollar loss suffered by the utility.[15] These statutes apply when someone has tampered with the meter system and actually stolen electricity or other utility services. Again, some State statutes include an assumptive provision that assigns responsibility for the tampering and theft to the person(s) who benefited as a result of the action.

Some States provide for awarding treble damages if a utility wins a suit against a thief. For example, if a customer stole $1,000 in services, the court could award the utility $3,000 in damages.

Before a utility can file charges against a potential suspect, it should gather the following as evidence, documents, and appropriate statements:

Witnesses—These include the meter reader who initially detected the possible diversion, the utility investigator, and the police officer who conducted the investigation.

Tampering devices—These could include straps behind the meter, wires used in a bypass system, or other tampering devices or equipment relevant to the case.

Meter report—This would show that the meter was operating correctly when installed and demonstrate how the particular tampering method used would have affected the metering of electricity. Most utilities have laboratories where the meters can be tested and technicians who will provide the necessary testimony in court.

Account billing history—This would illustrate the time the theft began and the amount and cost of the stolen electricity. Most utilities have the ability to review each account's consumption and billing records on a month-by-month basis to provide this information.

Some utilities prefer to use civil litigation when they have questions such as: Did meter tampering or power theft occur? How much electricity was not metered as a result of this tampering/theft? Was the defendant responsible for the electricity used at this location? In a civil process, the utility does not accuse anyone of stealing. They simply state that the meter did not operate correctly and that the defendant is responsible for the electricity used at the location where the loss occurred.

Problems in Prosecution

In many States, a conviction for meter tampering or power theft can be based solely on a utility being able to demonstrate motive, opportunity, and that the accused benefited as a result of the tampering, regardless of who actually did it. Utilities establish motive through the customer's billing records and the cost of the diverted power. They demonstrate that the accused had opportunity and benefited from the diversion by showing that the accused lived in the residence or owned the business where the theft occurred.

States having statutes that include the presumptive clause assume that the person "who benefited as a result of the tampering" is criminally responsible. The prima facie clause has been challenged in a number of States.[16] Some States have upheld the clause in the face of challenges, while others have ruled it unconstitutional. As a result, many utilities have decided to avoid criminal prosecution when the question of who actually tampered with the meter becomes an important point.

Another problem in the criminal prosecution of utility theft arises in some State statutes that require the prosecution to prove the defendant intended to injure or defraud the utility.[17] This can make prosecution difficult. For example, a customer moves into a vacant house or apartment where no service is connected and then jumps the socket to get power. Did this customer intend to call the utility, report the action, and pay for the electricity used, or did he intend to steal?

Recent Cases

The New York State Supreme Court recently affirmed a conviction of theft of services by a corporation based on evidence of a damaged electrical meter that recorded a substantially reduced power consumption.[18] The court concluded that since only the corporation's employees had access to the room housing the damaged meter, there was sufficient evidence for a conviction.

The Sixth Circuit of the U.S. Court of Appeals held in a Tennessee case that electrical service is a property right and cannot be discontinued to a customer without prior notice or a predetermination hearing.[19] Even though a city found that its meter had been removed and replaced by another one,

the court held that the customer had sufficient due process rights to prevent termination of electrical service without notice.

An investigation into the literature also found two cases in which electrical power diversion resulted in the loss of professional employee status. A board of education in Alaska dismissed a tenured school teacher after his conviction for diverting electricity. The Alaska Supreme Court upheld the board's decision to dismiss the teacher based on their finding that the act constituted a crime of moral turpitude.[20] Another case involved the disbarment of an attorney convicted of theft of services by meter tampering or receiving unmetered electrical service, as well as attempted criminal possession of a weapon.[21]

Courts hearing appeals on utility power service thefts generally found the terminology describing this offense to be clear (i.e., not unconstitutionally vague). A Louisiana Supreme Court case found no problems in the terms "diverting," "preventing," and "interfering," which described how utility service was obtained by a defendant.[22] The Supreme Court of Delaware also upheld that their State's theft of services statute also was not unconstitutionally vague.[23]

Summary

The economic crimes of meter tampering and power theft have grown to alarming proportions in many parts of the world. Power theft affects all consumers because it results in increased rates.

A coordinated effort between utilities and law enforcement agencies can help to combat this problem. Utilities have the responsibility to assess the extent of the crime in their service area and to establish methods and procedures for identifying thieves. They must also determine what their objectives will be once they detect potential thefts. Some utilities conduct all of their investigations and followup actions, while other systems call upon their local law enforcement agency to assist them in investigations.

Since many utilities do not have personnel with the experience or qualifications necessary to conduct a criminal investigation, the potential role of the police agency becomes very important. If utilities elect to conduct their own investigations, they will still need advice, assistance, and training from their local police agency. If they decide to work with the agency to combat the problem, they must establish procedures for the coordinated effort.

Though the theft of utility services costs the United States over $3 billion every year, by working together utilities and police agencies can combat this crime and help control the future cost of energy to the consumers in our country.

FBI

Footnotes

[1]E. F. Gorzelnik, "Theft of Service Poses Major Problems," *Electrical World*, May 1982, pp. 101-103.

[2]A. J. Donsiger, "The Underground Economy and the Theft of Utility Services," *Public Utilities Fortnightly*, November 22, 1979, pp. 23-27.

[3]"Utilities Say 1 Percent of Users are Stealing Power," *The New York Times*, March 26, 1984.

[4]"Con Edison Reports $7 Million in Power Stolen in 1981, But Sees Improvement," *The New York Times*, August 24, 1982.

[5]"PEPCO Adds Investigators, Catches Many More Thieves," *The Washington Post*, February 6, 1981.

[6]*1982 National Energy Theft Survey* (Boston: New England Power Service, July 2, 1982).

[7]Supra note 5.

[8]J. J. Williams, *Iron Gonads* (Alamogordo: Consumertronics Company, 1970).

[9]K. A. Seger,"Systems Approach Limits Power Theft," *TVPPA News*, November-December 1982, pp. 10-13.

[10]Supra note 1.

[11]Supra note 9.

[12]J. J. Gray, ed., "Theft of Utility Services," *Criminal and Civil Investigation Handbook* (New York: McGraw Hill Book Company, 1981), p. 7-126-8.

[13]*Ala. Code* §13-2-80 et seq.; *Alaska Stat.* §42.20.030; *Ariz. Rev. Stat.* §13-1601; *Cal. Penal Code* §499a; *D.C. Code* §22-3115; *Fla. Stat. Ann.* §812.14; *Ga. Code* §26-1507; *Haw. Rev. Stat.* §708-825 et seq.; *Idaho Code* §18-4621 et seq. *Ill. Rev. Stat.* tit. 111 2/3 §381,382; *Kan. Crim. Code §17-1921; La. Rev. Stat. §14.67.6; Ohio Rev. Code Ann.* §4933.19; *Pa. Stat. Ann.* tit. 18 §3926(e); *Tn. Code Ann.* (TCA) §39-3-938; and *Utah Code Ann.* §76-6-409(1)(a) and (1)(b); paper presented by S. R. Grubbs, "Legal Remedies for Theft of Electricity," American Power Association Legal Seminar, November 12, 1980.

[14]See, for example, Virginia §18.2-163, *Tampering with Metering Device; Diverting Service.* The Virginia statute does include a prima facie provision.

[15]See, for example, Tennessee §39-3-938, *Diversion of Electric Power - Presumption of Intent to Defraud - Civil Action by Utility.* The Tennessee statute does include a provision whereby the utility can recover treble damages.

[16]Paper presented by M. Banks, *Current Diversion Training Manual*, University of Florida and the Southeastern Metermen's Association, March 1979.

[17]Paper presented by F. M. Bryant, *Meter Tampering, Power Diversion and Underbilling*, American Public Power Association, June 11, 1984.

[18]*People* v. *San Roc Restaurants, Inc.*, 498 N.Y.S. 2d 481 (1986).

[19]*Myers* v. *City of Alcoa*, 752 F.2d 196 (6th Cir. 1985).

[20]*Kenai Peninsula Borough Board of Education* v. *Brown*, 691 P.2d 1034 (Alaska 1984).

[21]*Richard DeCesare* v. *Departmental Disciplinary Committee*, 443 N.Y.S. 2d 375, 82 A.D. 2d 716 (1981).

[22]*State* v. McCoy, 395 So. 2d 319 (La. 1980).

[23]*Wright* v. *State*, 405 A.2d 685 (Del. Supr. 1979).

The Electronic Communications Privacy Act

Addressing Today's Technology

(Part II)

By
ROBERT A. FIATAL, J.D.
Special Agent
Legal Counsel Division
FBI Academy
Quantico, VA

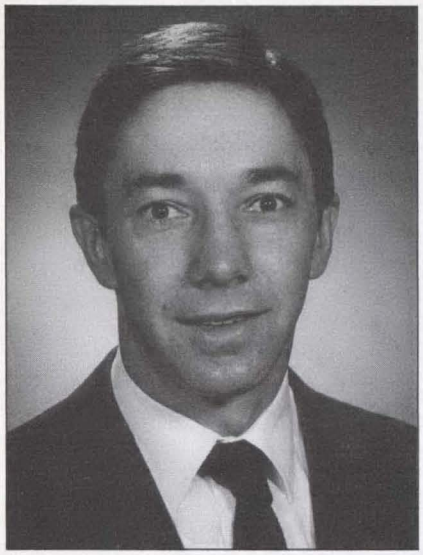
Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

Part one of this article identified the problem areas which provoked Congress to pass the Electronic Communications Privacy Act of 1986[24] (the ECPA). Parts two and three of this article will address those three provisions of the ECPA which commonly impact Federal, State, and local investigative procedures. Part two will address that portion of the ECPA which now requires law enforcement officers to obtain extraordinary, or wiretap-type, orders when planning to nonconsensually intercept electronic communications, such as messages sent to digital display pagers or messages sent from one computer to another. Part three will discuss the two remaining provisions of the ECPA: (1) That portion which sets forth the procedure law enforcement officers must follow to use pen registers, which record the phone numbers dialed from a telephone, and trap and trace devices, which determine the origin of a phone call; and (2) the section of the ECPA which proscribes the procedure police officers must observe when obtaining stored electronic communications, such as computerized messages kept in an electronic mailbox, and transactional records of communications services, to include telephone toll records and nonpublic telephone subscriber information.

THE ECPA

When considering these three separate provisions of the ECPA, State and local law enforcement officers must first understand two significant points that affect their work in this area. First, the ECPA is not intended to preempt existing State law, whether of statutory or judicial origin.[25] For example, if the State standard or procedure for obtaining toll records or using pen registers is more restrictive than that provided for by the ECPA, police officers within that State must comply with the stricter State law.

Second, although all three sections of the ECPA have been applicable to Federal investigations since the ECPA's effective date, January 20, 1987, they affect State and local investigations at varying times. The third section of the ECPA to be discussed in this article, involving government access to stored communications, toll records, and unlisted subscriber information, had universal effect on



Special Agent Fiatal

January 20, 1987. State and local officers must therefore understand and comply with this portion of the act immediately.

Congress determined, however, that the first section of the ECPA, requiring the acquisition of a wiretap-type order to intercept electronic communications during their transmission, and the second section to be discussed, setting forth the procedure law enforcement must follow to use pen registers and trap and trace devices, were significant changes in traditional law. Therefore, States will have 2 years from the date of enactment of the act to bring their own law into conformity with those two provisions of the ECPA.[26] As Congress passed the act on October 2, 1986, State and local officers have to comply with these two sections of the ECPA by October 2, 1988, unless, of course, their respective States adopt procedures in these areas at least as restrictive as the Federal mandates before October 1988.

Interception of Electronic Communications

As discussed in part one of this article, prior to the enactment of the ECPA, Title III of the Omnibus Crime Control and Safe Streets Act [27] (title III) and its analogous State statutes required law enforcement officers to obtain extraordinary judicial orders when they planned to aurally intercept wire communications (wiretaps) or oral communications where there exists a reasonable expectation of privacy (bugs), in the absence of the consent of a party to the communication. An aural interception was the interception of a communication involving the transmission of the human voice. Title III therefore provided no protection to communications that did not involve the spoken word, such as telegraph or facsimile-type communications, which involve the electronic transmission of a written message, photograph, drawing, or document.

The first portion of the ECPA significantly expanded the traditional wiretapping and bugging law by also affording the same protections previously supplied to wire and oral communications to electronic communications. The ECPA provides that in order to intercept an electronic communication during the course of its transmission, without the consent of one of the parties to that communication, the police officer must obtain an extraordinary order, just as if he were intercepting a wire communication or an oral communication involving a reasonable expectation of privacy.[28] Although this portion of the ECPA immediately affected Federal wiretapping procedure, State and local officers are not required to conform with this change in the law until October 2, 1988.

In effecting the expansion of the traditional wiretapping and bugging law, Congress provided a very broad definition of what is an electronic communication. It basically includes any type of communication transmitted by some electronic means, unless it involves the transmission, at least in part, of a human voice, which would instead be a wire communication. This broad definition of an electronic communication encompasses those written messages, documents, and photographs transmitted by telegraph and facsimile-type communications services. It also includes those communications electronically transmitted from one computer

". . . States will have 2 years from the date of enactment of the act to bring their own law into conformity with . . . two provisions of the ECPA."

terminal to another and those numerically coded messages transmitted to digital display paging devices. If a law enforcement officer intends to intercept any of these types of communications during the course of their transmission and does not have the consent of one of the parties to the communication, he must first obtain an interception, or wiretap-type, order. He must of course fulfill the same procedural requirements in the application for such an order as if it were an application for the interception of wire or oral communications.[29] These include the traditional probable cause and particularity requirements, as well as an explanation of exhaustion of traditional investigative techniques and a record of prior interceptions and interception efforts.

When constructing such an all-inclusive definition of electronic communications, Congress realized that there were several types of communications that, although technically falling within the definition of an "electronic" or "wire communication," did not deserve those protections afforded by title III. Congress therefore created several exceptions to what might otherwise be deemed an "electronic" or "wire communication," and each is noted in turn.

Communications Not Protected by the ECPA

The ECPA expressly denotes six types of communications for which a law enforcement officer is not required to obtain a wiretap-type order to intercept. Some fourth amendment consideration may, however, be applicable in limited circumstances, as the interception may involve the government's intrusion into a reasonable expectation of privacy. If so, the law enforcement officer must obtain a search warrant in the absence of consent or emergency. While analyzing the ECPA's six exceptions to electronic and wire communications, this article will also address any possible fourth amendment considerations applicable to those exceptions.

Publicly accessible radio communications

Law enforcement officers and others can receive, or intercept, radio transmissions which are "readily accessible to the general public"[30] without obtaining a wiretap order. This would include interception of AM-FM radio broadcasts and those ham radio broadcasts, CB broadcasts, walkie-talkie broadcasts, and marine or aeronautical, or ship to shore, broadcasts, which are not scrambled or encrypted in such a manner as to thwart their public accessibility.

Tracking devices

Police officers can also monitor tracking devices, sometimes referred to as beacons, or beepers, without obtaining a wiretap order.[31] Tracking devices emit periodic radio signals which enable the receiver to ascertain the movement of the device. Law enforcement agencies commonly attach these devices to a motor vehicle, airplane, or boat or place them in a package containing narcotics or chemicals or equipment used to manufacture narcotics, so that they may monitor the movements of the vehicle or package.

Although the police officer is not required to obtain a wiretap order to monitor the transmissions of these types of devices, he may, under certain circumstances, infringe upon an individual's reasonable expectation of privacy by monitoring such a device. In *United States* v. *Knotts*,[32] the Supreme Court determined that when a law enforcement officer monitors the movements of a tracking device while it is upon the highway, or within public view, he does not infringe upon an individual's reasonable expectation of privacy, as the individual has no such expectation of privacy in his movements in publicly visible areas. The police officer therefore does not need a search warrant when confining his monitoring of the tracking device to such circumstances.

In the subsequent case of *United States* v. *Karo*,[33] however, the Supreme Court recognized that if a law enforcement officer continued to monitor the tracking device once it moved into an area where it was no longer within public view, such as inside a residential premises, and obtained information which he could not have obtained by lawful visual surveillance, he was intruding into a justifiable expectation of privacy. In this situation, the police officer needed a search warrant to continue to monitor the device, in the absence of an emergency, to comply with fourth amendment requirements.[34]

Radio portion of cordless telephones

As previously mentioned, handheld cordless telephones have become overwhelmingly popular with the public. When purchased, a warning on the packaging of such a device advises the buyer that other individuals can easily intercept the conversations made over the device. They may accomplish this by using a similar device, and in some

instances, a standard AM-FM radio receiver. Congress duly recognized that there was little, if any, privacy interest in that portion of a communication which travels over radio waves between the cordless phone and the base unit. The law enforcement officer, therefore, is not required to obtain judicial approval to intercept the radio portion of a communication made over a handheld cordless telephone.[35] Likewise, the officer does not have to obtain a search warrant to overhear the radio portion of a cordless phone, as such activity does not intrude into a reasonable expectation of privacy.

It should be pointed out in this context that unlike the radio portions of cordless phone communications, those communications made through cellular phones are wire communications. The law enforcement officer must therefore obtain a wiretap order to intercept this type of communication in the absence of consent of one of the parties to the cellular phone call. This even includes calls made from one cellular phone to another cellular phone.[36]

Although portions of the cellular phone call, like portions of the cordless phone call, travel over the airwaves, there are valid reasons for this distinction. Cellular phones have a far greater range — sometimes hundreds of square miles, due to the number of radio receivers and transmitters arranged in adjacent geographical areas — than the range of cordless phones, commonly limited to a few hundred feet. Additionally, the type of equipment needed to intercept a cellular phone call is much more sophisticated and expensive than that needed to intercept the radio portion of a cordless phone, due to the range capabilities of the cellular phone and the varying radio frequencies used in such transmissions. Persons therefore possess a much higher expectation of privacy in calls made over a cellular phone than in those made over a cordless phone.

Tone-only paging devices

A police officer may intercept the transmission made to a tone-only paging device without obtaining a wiretap order.[37] As previously noted, there is no expectation of privacy in the beep made through such a device that merely notifies the possessor of this type of pager that someone is attempting to reach him. The officer therefore also need not acquire a search warrant to conduct such an interception as this activity does not involve an infringement upon any legitimate expectation of privacy.

The criminal who relies upon paging services to facilitate his illegal activities, however, seldom uses a tone-only pager. Instead, he will use a voice pager, or more frequently, a digital display paging device. Those involved in the illicit transfer of narcotics often contact their buyers and providers through digital display pagers. As discussed elsewhere, in contrast to the tone-only pager, those communications transmitted to a voice pager are wire communications as they involve the spoken word. Also, those communications sent to a digital display pager fall within the definition of electronic communications. Therefore, the law enforcement officer must obtain proper judicial authority by obtaining a wiretap-type order before intercepting messages sent to a voice or display paging device, in the absence of consent of a party to the communication.

Surreptitious video surveillance

If law enforcement officers desire to intercept a closed-circuit television broadcast during its transmission, for example, a video teleconference between two suspected criminals, they must first obtain an interception order. The intercepted television transmission would be an electronic communication, now entitled to the protections afforded by title III. If the officers merely survey a suspected criminal through the use of a video camera, however, they do not have to comply with wiretap procedure. They are not tapping, or intercepting, any type of electronic, wire, or oral communication.

If the officers use the video equipment to watch an area or activity where the person or persons observed have a reasonable expectation of privacy, they will, however, need to obtain a fourth amendment search warrant, unless they have the consent of one of the parties and that party is present while the officers conduct the surveillance. Two U.S. circuit courts of appeal, recognizing this type of video surveillance to be unusually intrusive, have recommended that the applications for video surveillance search warrants and the search warrants themselves satisfy certain procedural requirements also found in title III.[38] For example, these circuit courts stated that applications for video surveillance warrants should explain that less-intrusive investigative techniques, like the use of informants, undercover officers, or traditional search warrants, have been tried and failed or why they would be unlikely to succeed or be unnecessarily dangerous. Additionally, these courts require

". . . the ECPA is not intended to prempt existing State law . . . if the State standard or procedure . . . is more restrictive than that provided for by the ECPA, police officers within that State must comply with the stricter State law."

video surveillance warrants to be effective for no more than 30 days. The orders must also, like a wiretap order, particularly describe the people, place, and type of criminal activity to be observed and instruct the executing officers to minimize their interception of innocent, or noncriminal, activities. If the officers, in conjunction with nonconsensual video surveillance into an area where there exists a reasonable expectation of privacy, also intercept the oral communications of those viewed by a hidden microphone, they must, of course, obtain a "bug" order pursuant to title III or analogous State law to lawfully intercept the oral communication, in addition to the video surveillance warrant.

Pen registers and trap and trace devices

The ECPA specifically states that law enforcement officers are not required to obtain a wiretap-type order to use pen registers, which record the numbers dialed from a telephone, and trap and trace devices, which determine the point of origin of a telephone call.[39] As previously discussed, the Supreme Court also determined that there is no reasonable expectation of privacy in the numbers dialed from a telephone.[40] Therefore, police are also not required to obtain a search warrant to use a pen register or trap and trace device.[41]

Although police are not required to obtain a wiretap order or a search warrant to use either pen registers or trap and trace devices, phone companies, who provide necessary technical assistance in using these types of investigative techniques, commonly insist in nonemergency situations upon some type of court authorization before providing their assistance. Congress, in order to set forth a standardized procedure for obtaining court authorization for the use of pen registers and trap and trace devices and to provide limited judicial monitoring of the use of these devices by law enforcement, set forth specific procedures that police officers must follow to obtain authorization for their use.

They must either obtain a court order, to be issued upon the applicant's assurance or affirmation, that the information to be gained from the pen register or trap and trace device is relevant to a legitimate criminal investigation or consent from the user of the telephone to which the device is to be attached.

Part three of this article will discuss in detail this portion of the ECPA which proscribes procedures for using pen registers and trap and trace devices. It will also examine that portion governing the acquisition of stored communication, such as those in electronic mailbox systems, and information pertaining to the subscriber of a communication service, such as telephone toll records and nonpublic telephone listing information.

FBI

(Continued next month)

Footnotes

[24]*Supra* note 1.

[25]18 U.S.C. 2703 and 3122(a)(2).

[26]Senate Bill 2575, 99th Congress, 2d Session, Electronic Communications Privacy Act, Sections 111 and 362.

[27]*Supra* note 3.

[28]18 U.S.C. 2511(1).

[29]The ECPA does, however, somewhat relax the procedure a Federal law enforcement officer must follow to apply for a court order authorizing the interception of an electronic, rather than a wire or oral, communication. The application for such an order can be predicated upon the investigation of any Federal felony and can be authorized for transmittal to a Federal judge by any U.S. attorney. 18 U.S.C. 2516(3). Nonetheless, the Department of Justice, as a matter of policy, will continue to require departmental application approval for electronic communication interception orders for 3 years from the effective date of the act.

[30]18 U.S.C. 2510(16) and 2511(2)(g).

[31]18 U.S.C. 2510(12).

[32]460 U.S. 276 (1983).

[33]468 U.S. 705 (1984).

[34]For a more detailed discussion of the fourth amendment's application to the monitoring of tracking devices, see John C. Hall, "Electronic Tracking Devices: Following the Fourth Amendment," *FBI Law Enforcement Bulletin*, vol. 54, No. 3, (Part I) February 1985, pp. 26-31; No. 4, (Conclusion) March 1985, pp. 21-31. The ECPA does provide for the potential extraterritorial jurisdiction of a search warrant issued to monitor a tracking device. If obtained, the warrant can be effective even if the device moves out of the jurisdiction in which the warrant was issued, as long as the device was installed within the issuing jurisdiction. 18 U.S.C. 3117.

[35]18 U.S.C. 2510(1) and (12).

[36]18 U.S.C. 2510(1) defines a wire communication to include those voice communications that are transmitted through switching stations.

[37]18 U.S.C. 2510(12).

[38]*See United States* v. *Biasucci*, 786 F.2d 506 (2d Cir. 1986); *United States* v. *Torres*, 751 F.2d 875 (7th Cir. 1984).

[39]18 U.S.C. 2511 (2)(h).

[40]*Supra* note 19.

[41]The Supreme Courts of the States of Colorado and Pennsylvania have determined the use of a pen register to be a search under their respective State constitutions and therefore require that officers obtain a search warrant prior to their using such a device, in the absence of consent or emergency. *Commonwealth* v. *Beuford*, 475 A.2d 783 (Pa. Sup. Ct. 1984); *People* v. *Sporleder*, 666 P.2d 135 (Col. Sup. Ct. 1983).

WANTED BY THE FBI

Any person having information which might assist in locating these fugitives is requested to notify immediately the Director of the Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC 20535, or the Special Agent in Charge of the nearest FBI field office, the telephone number of which appears on the first page of most local directories.

Because of the time factor in printing the FBI Law Enforcement Bulletin, *there is the possibility that these fugitives have already been apprehended. The nearest office of the FBI will have current information on the fugitives' status.*

Photograph taken 1984

Jay Thomas Burlison,

also known as Lester Brown, Jay Burlinson, Jay Thomas Burlinson, J. T. Burlison, Jay Burlison, Jay T. Burlison, "Blue Jay."
W; born 1-25-43; Waynesboro, TN; 5'8"; 135 lbs; med bld; blk (graying) hair; green eyes; ruddy comp; occ-laborer, lumberyard worker, truck driver; remarks: Reportedly missing teeth; scars and marks: Scars on face, appendectomy scar.
Wanted by FBI for INTERSTATE FLIGHT-MURDER; AGGRAVATED ASSAULT

NCIC Classification:

COTT1617111112141706

Fingerprint Classification:

16 O 1 T OO 11 Ref: 5
S 17 U OOO 17

I.O. 5022

Social Security Numbers Used: 408-68-8373; 408-68-3273; 408-68-3373

FBI No. 926 536 F

Caution

Burlison is being sought in connection with the shooting murder of one individual and the aggravated assult of another. He is reportedly in possession of several handguns and should be considered armed and extremely dangerous.

Right index fingerprint

Photograph taken 1975

Ronald Harland Saurman,

also known as Ron Lydell, Ronald McDonald, Ronald H. Saurman, Mr. Snow.
W; born 1-28-46 (true date of birth); 1-1-46; 1-26-46; New York, NY (true place of birth); Grand Rapids, MI; 6'; 160 lbs; med bld; brn (may be dyed blonde) hair; blue eyes; med comp; occ-musician, pilot, ranger, self-employed retailer; remarks: Saurman is an alleged buyer of expensive Indian artifacts. He may be in possession of high quality false passports and other fictitious identification.
Wanted by the FBI for RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS; CONTROLLED SUBSTANCE ACT

NCIC Classification:

16520413091355111106

Fingerprint Classification:

16 M 1 R III 9 Ref: T
M 1 R IOI R

I.O. 5039

Social Security Number Used: 385-46-3336

FBI No. 702 556 F

Caution

Saurman, a convicted cocaine trafficker, is believed to be armed with weapons and should be considered armed and dangerous.

Right thumbprint

Photographs taken 1982 and 1986

Joseph John Kindler,

also known as Joseph John Kidler, Joseph Kindler, Joseph J. Kindler, Scott M. McGill, Scott Michael McGill.
W; born 9-11-60 (true date of birth); 8-11-60; Philadelphia, PA; 5'8"; 159 lbs, med bld; light brn hair; brn eyes; light comp; occ-electronic equipment repairman; remarks: He allegedly has an extensive knowledge of all electronic equipment, including security devices; scars and marks: Burn scar on left inner forearm.
Wanted by the FBI for INTERSTATE FLIGHT-MURDER

NCIC Classification:

AAAAAA0404AA02AATT02

Fingerprint Classification:

4 1 aAa 4 Ref: A
1 aUat T

I.O. 5036

Social Security Number Used: 211-48-3191

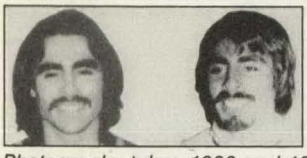
FBI No. 409 012 W4

Caution

Kindler, an escapee from custody, is being sought in connection with a murder wherein the victim was bludgeoned to death with a baseball bat. The body was subsequently disposed of by dumping the weighted body into the Delaware River. Kindler has been armed with a handgun in the past and has stated he will never be taken alive. Consider armed, dangerous, and an escape risk.

Right thumbprint

WANTED BY THE FBI



Photographs taken 1980 and 1984

Kenneth Bernard Candelaria,

also known as Michael Andreas-Villa, Michael Andres-Villas, Kenner B. Candelaria, Kennith Bernard Candolaria, Kenny Kennard, Kenneth Rameriz, "Dogfood," "Kenner Dogfoot," "Indian," "Kenner," and others.

W; born 7-20-49 (true date of birth); 7-20-50; Roswell, NM; 5′2″; 120 lbs; med bld; blk hair; brn eyes; fair comp; occ-painter, leather worker, jewelry craftsman, construction and landscape laborer, cuts firewood; remarks: Often passes himself off as an American Indian and has been known to wear feathers and Indian jewelry. He is allegedly an acomplished surfer. Candelaria may be accompanied by his wife, Sherry Constance Candelaria, nee Gracia, White female, born 11-27-57, Los Angeles, CA, 5′, brn hair, hazel eyes, Social Security Number Used: 553-04-5581. SHE IS NOT WANTED BY LAW ENFORCEMENT AUTHORITIES.

Wanted by FBI for AIDING AND ABETTING; POSSESSION WITH INTENT TO DISTRIBUTE MARIJUANA; DISTRIBUTION OF MARIJUANA; CONSPIRACY WITH INTENT TO DISTRIBUTE MARIJUANA; IMPORTATION OF MARIJUANA; CONSPIRACY TO IMPORT MARIJUANA.

NCIC Classification:

POPIDMPM20DIPOPIPIDI

Fingerprint Classification:

O 32 W IMM 20
I 28 W OII

I.O. 5030

Social Security Numbers Used: 463-86-4974; 463-86-4973; 582-60-9334

FBI No. 224 804 Y11

Caution

Candelaria, who is allegedly involved in drug trafficking, has been previously convicted of carrying a concealed weapon. He is reportedly armed with an AK-47 rifle, hand grenades, and has vowed not to be taken alive. Candelaria should be considered armed and dangerous.

Left thumbprint

Photographs taken 1985

Claude Daniel Marks,

also known as Claudio Daniel Makowski (true name), John Chester Clark, Edward Cole, Charles Everett, Michael Hamlin, C. Henley, Dale Allen Martin, Tony McCormick, Michael Prentiss, Brian Wilcox, and others.

W; born 12-31-49 (true date of birth); 2-11-44; 11-1-45; 6-8-50; 2-6-51; 6-26-51; 3-26-55; Buenos Aires, Argentina; 6′; 190 lbs. hvy bld; brn hair; brn eyes; med comp; occ-fast food cook, radio announcer, auto mechanic, printer; scars and marks: mole on neck; remarks: Marks is a martial arts enthusiast and allegedly is knowledgeable of electronics and automobile maintenance, weapons, explosives, and reloading procedures. Reportedly speaks fluent Spanish. Wears contact lenses or glasses. Marks may be accompanied by Donna Jean Willmott, FBI Identification Order 5035, WHO IS ALSO WANTED BY LAW ENFORCEMENT AUTHORITIES.

Wanted by the FBI for CONSPIRACY TO VIOLATE PRISON ESCAPE, DAMAGE AND DESTRUCTION OF GOVERNMENT PROPERTY, RECEIPT AND TRANSPORTATION OF EXPLOSIVES, INTERSTATE TRAVEL TO PROMOTE CRIMINAL ACTIVITY, POSSESSION OF UNREGISTERED FIREARMS

I.O. 5034

Social Security Numbers Used: 551-80-8393; 129-62-4064; 287-03-2916; 299-05-3771; 520-82-1220; 568-75-8212; 601-34-2858; 120-68-4648; 547-67-2897; 608-98-2730; 561-67-2823; 692-42-9631;556-31-3362; 015-65-0510; 525-36-4427

FBI No. 83 249 FA4

Caution

Marks has been trained in the martial arts and has been known to be in possession of explosives. He should be considered armed and dangerous.

FBI TOP TEN FUGITIVE

Right thumbprint

Photographs taken 1985

Donna Jean Willmott,

also known as J. Billings. Marcie Garber, Marcia Gardner, Jean Gill, Dona J. Krupnick, Donna J. Willmott, Donna Jean Willmot, Donna Wilmiet, Donna Jean Wilmott, Terry Young, and others.

W; born 6-30-50 (true date of birth); 12-15-56; Akron, OH; 5′; 105 lbs; small bld; brn hair (dyed blonde); brn eyes, ruddy comp; occ-hospital technician, nurse, lab technician, acupuncturist, housekeeper; remarks: Willmott is known to use false identification and change appearance using wigs and/or dyed hair. Wears corrective lenses. Willmott has reportedly taken martial arts courses. Willmott may be accompanied by Claude Daniel Marks, FBI Identification Order 5034, WHO IS ALSO WANTED BY LAW ENFORCEMENT AUTHORITIES.

Wanted by the FBI for CONSPIRACY TO VIOLATE PRISON ESCAPE, DAMAGE AND DESTRUCTION OF GOVERNMENT PROPERTY, RECEIPT AND TRANSPORTATION OF EXPLOSIVES, INTERSTATE TRAVEL TO PROMOTE CRIMINAL ACTIVITY, POSSESSION OF UNREGISTERED FIREARMS

NCIC Classification:

121109PM12AA1009CI10

Fingerprint Classification:

12 9 U OIM 12
2aU OII

I.O. 5035

Social Security Numbers Used: 270-50-0840; 360-42-8763; 360-42-8736; 567-67-9133; 390-18-4818

FBI No. 867 585 EA5

Caution

Willmott has reportedly taken martial arts lessons and has been known to possess explosives and a wide array of weapons. She should be considered armed and dangerous.

FBI TOP TEN FUGITIVE

Right index fingerprint

☆U.S. Government Printing Office: 1988—202-051/80002

Interesting Pattern

A combination of a loop and a tented arch formation must have the loop formation appearing over the tented arch to be classified as an accidental whorl. Any loop and tented arch formation not in this position shall have the loop formation as the preferred classification. This month's presentation is classified as an accidental whorl with an inner tracing. The loop formation appears over the upthrust tented arch.

Change of Address

Not an order form

FBI
Law Enforcement Bulletin

Complete this form and return to:

Director
Federal Bureau of
Investigation
Washington, DC 20535

Name

Title

Address

City State Zip

U.S. Department of Justice
Federal Bureau of Investigation

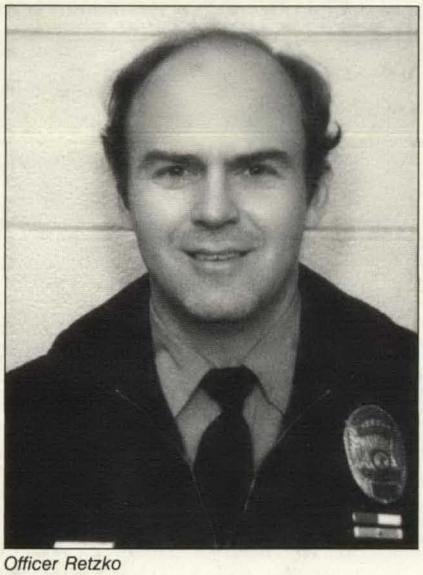
Second Class Mail
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Washington, D.C. 20535

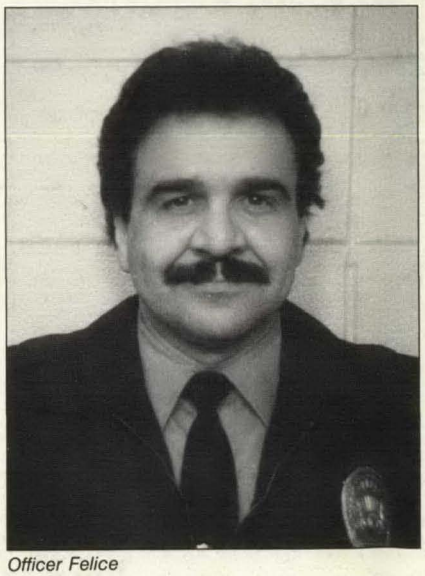
Official Business
Penalty for Private Use $300
Address Correction Requested

The Bulletin Notes

On February 11, 1987, Police Officers David Retzko and James Felice of the Willingboro Township, NJ, Police Department, while on routine patrol, were dispatched to a house fire. At the scene, they encountered an elderly woman holding an infant, who had escaped from the burning house. Without regard for their own safety, these officers entered the burning dwelling and recovered two lifeless children. The officers immediately administered CPR and revived the children. The Bulletin joins these officers' superiors in commending their heroism.



Officer Retzko



Officer Felice