USABulletin

SEPTEMBER 1997 VOL. 45, NO. 5

ELECTRONIC INVESTIGATIVE TECHNIQUES

In This Issue

Letter from the Editor-in-Chief

The next two issues of the *Bulletin* focus on the working relationships among the United States Attorneys' offices, the Criminal Division's Office of Enforcement Operations (OEO) and Computer Crime & Intellectual Property Section, and the Assistant Attorney General or Deputy Assistant Attorney General in the area of Title III, and other electronic surveillance techniques. We have included articles, checklists, and interviews covering the approval process for, and use of, Title III intercepts and related electronic surveillance methods in the investigation and prosecution of a variety of criminal cases.

The interview of OEO Director Frederick D. Hess is terrific. He provides us with insight into the history of OEO, its inner workings, and the need to have OEO lawyers review applications to allow us to use these effective and powerful investigative tools. Through the collective efforts of several OEO lawyers, we have a great article on the "nuts and bolts" of OEO's Title III approval process and highlights of several major Title III cases. You'll also find that the articles submitted by Michael R. Sklaire of the Narcotic and Dangerous Drug Section are invaluable references when faced with "what do we need to do to get . . . [electronic surveillance order]" questions. AUSA Jeffrey W. Johnson has written a very common sense article regarding his approach to wiretaps. We also included an interview with DEA Special Agent Mark Styron regarding his perspective on working relationships between AUSAs and Agents in wiretap cases. AUSAs Melissa J. Annis, Monica Bachner, and Patricia Diaz share their experiences with wiretap investigations, including some of the obstacles AUSAs face when supervising wiretaps. Each author offers terrific suggestions and "things to think about."

Please take time to review the inside back cover of the magazine for our publication schedule over the next several months. If you are interested in writing an article on any of these topics, please contact me. Finally, if you have any comments or constructive criticisms regarding past issues, call me at (809) 773-3920 or Email me at AVISC01(DNISSMAN). Our intent is to make the *Bulletin* a practical and useful resource; our method of doing so is through your continued contributions, comments, and suggestions.

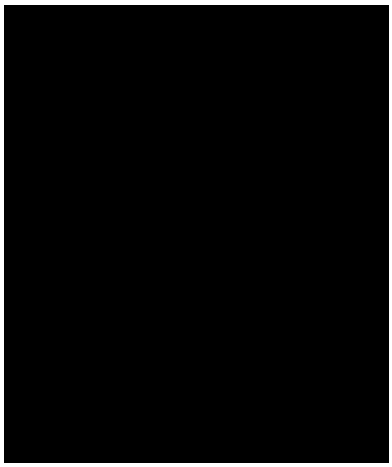
DAVID MARSHALL NISSMAN

Published by
Executive Office for United States Attorneys
Washington, D.C.
Carol DiBattiste, Director
United States Attorneys' Bulletin Staff, (202) 616-1681
David Marshall Nissman, Editor-in-Chief
Wanda J. Morat, Editor
Barbara J. Jackson, Editor
Patrice A. Floria, Editor
Susan Dye Bartley, Graphic Designer
Nina M. Ingram, Student Assistant

Send distribution address and quantity corrections to:
Barbara Jackson, Executive Office for United States Attorneys, Bicentennial Building, Room 6011, 600 E Street, N.W., Washington, D.C. 20530-0001
(202) 616-8407 or fax (202) 616-6653

Contents

Interview with Director Frederick D. Hess Office of Enforcement Operations



Director Frederick D. Hess
Office of Enforcement Operations

Frederick D. Hess has served as Director of the Office of Enforcement Operations (OEO) for more than 15 years. He received his Bachelor of Arts degree from Columbia College and Juris Doctor degree from Brooklyn Law School. In August 1967, he was appointed an attorney in the Criminal Division as part of the Attorney General's Honors Program. Mr. Hess began his career in the Department of Justice in the Legislation and Special Projects Section, where he served as Deputy Chief from January 1974 until becoming Associate Director of the Office of Legal Support Services (OLSS) in February 1979. He was Acting Director of OLSS from January 1980 to June 1982, when OLSS was merged with OEO and he was named Director.

As Director of OEO, Mr. Hess oversees the use of the most sophisticated investigative tools in the Federal Government. Beyond reviewing United States Attorneys' offices' requests for authorization to apply for court orders approving the interception of wire, oral, and most electronic communications, OEO—with a staff of approximately 100 attorneys, analysts, paralegals, and secretaries—provides the United States Attorneys' offices and the Federal law enforcement agencies with a wide range of prosecutorial and investigative support services. OEO authorizes or denies the entry of all applicants into the Federal Witness Security Program (WSP), and oversees matters relating to all aspects of the WSP; administers the International Prisoner Transfer and S Visa programs; supervises the mechanism by which Federal law enforcement officers or agents employed by the Offices of the Inspectors General may become Special Deputy United States Marshals; and coordinates requests to immunize witnesses, subpoena attorneys, issue subpoenas to the press, close court proceedings, or search the offices of attorneys who are suspects or targets of an investigation. In addition, OEO provides legal advice to Federal, state, and local law enforcement agencies on the use of the Federal electronic surveillance statutes; assists in developing Department policy on emerging technologies and telecommunications issues; and responds to requests made to the Criminal Division for disclosure of information pursuant to the Freedom of Information Act and the Privacy Act. Upon request, OEO also assists in the drafting of reply briefs involving electronic surveillance issues.

OEO Director Fred Hess (FH) was interviewed by Assistant United States Attorneys (AUSAs) David Nissman (DN), Editor-in-Chief of the *United States Attorneys' Bulletin*, and Jennifer Bolen (JB), Northern District of Texas. OEO Senior Associate Director Maureen Killion (MK) also participated in the interview.

DN: How do you view the working relationship between OEO and the United States Attorneys' offices?

FH: When we get a call from the field, the attorney's attitude is not, "What do you want?" but, rather, to ask what they can do to help. We have hardworking people, particularly in the Electronic Surveillance Unit. When D. Lowell Jensen, now a Federal district judge in San Francisco, was Assistant Attorney General of the Criminal Division, he coined a phrase for our office: "The office that never sleeps."

DN: Do you personally review each affidavit?

FH: We are now in a situation where there are just too many. Fifteen years ago, during the first year that I was here, there were 227 affidavits for review. The next year there were 360. Last year there were 1367. For seven or eight years, I read every affidavit, but it's

just not possible anymore. Also, the office is larger and has many more functions that require my attention. While I no longer have time to read the incoming affidavits, I do review the Electronic Surveillance Unit's action memoranda that summarize each electronic surveillance request for the Assistant Attorney General or Deputy Assistant Attorney General that must approve the request before a court order may be sought.

On the incoming end, we like a senior person in the United States Attorney's office to sign off on the affidavit and let us know that this is a case that the United States Attorney wants to do. A Title III is a three-legged stool: the legs are the investigative agency, the United States Attorney's office, and our office. Like any three-legged stool, if one leg falls off, the stool falls over—so all three participants have to approve. So when an affidavit is sent to this office, the agents—primarily from DEA, FBI, and the Customs Service—should also send a copy to their headquarters. The agency headquarters then does an independent review. We don't go forward on new Title III applications without a written request from the agency's headquarters telling us they want to do it. Wiretaps are expensive. We've always used the ballpark figure of $50,000 for the cost of running a 30-day wiretap, because wiretaps are so agent time-intensive.

"We don't go forward on new Title III applications without a written request from the agency's headquarters telling us they want to do it."

Frederick D. Hess

When we get an affidavit, we log it in and assign it to a reviewing attorney and a senior attorney. The senior attorney reads it quickly to make sure that there are no major problems with it, and then turns it over to the reviewing attorney. If there are problems with the affidavit—and we find them a good percentage of the time—the reviewing attorney contacts the Assistant United States Attorney who will be applying for the Title III order. We raise the problems we've seen in the affidavit, and discuss how the Assistant can get the affidavit in shape so we can move it forward.

Once changes we request are made, the reviewing attorney writes a synopsis of the affidavit—a five or six page action memorandum. A case file is started that contains the application, affidavit, and any prior action memoranda (from previously handled, related Title III requests). These documents, along with the OEO attorney's action memo, are then given to the Unit Chief, Julie Wuslich, or her deputy, Janet Webb. One of them reviews the case file and may request additional information or changes. Then this file comes to me or one of the OEO Associate Directors. I read as many of them as I can. We then review it, and put a buckslip on it to the Assistant Attorney General or one of the Deputy Assistant Attorneys General. One of these high-level Department officials reviews the Title III request and, almost invariably, will sign it. They have problems with the requests once in a while, but major problems are rare after the extensive review process in OEO.

DN: Who reviews the request when it goes to Main Justice?

FH: When I started here, Title III allowed for the Attorney General's authority to be delegated only to the Assistant Attorney General's level, which created a great burden on the Assistant Attorney General especially as our numbers began to go up. We finally got that amended in 1986 so that the authority can now be delegated to the Assistant Attorney General **or** the Deputy Assistant Attorneys General for the Criminal Division. A request can now be handled by any one of the five Deputy Assistant Attorneys General unless, for some reason, I need to direct it to a specific Deputy— such as when it's related to a previous request handled by one of the Deputies. Otherwise, whoever is available can get it. The only exception to this is a roving oral or wire interception request which, by statute, must be reviewed (and approved) by the Assistant Attorney General or higher.

DN: What happens when the application comes back from the Deputy Assistant Attorney General?

Hess Receives Attorney General Award

On June 13, 1997, Director Frederick D. Hess, Office of Enforcement Operations (OEO), received the Attorney General's Mary C. Lawton Lifetime Service Award in recognition of high standards of excellence and dedication exhibited during his 30-year career with the Department of Justice, and especially during his 15-year tenure as head of OEO. He supervised the implementation of a variety of sensitive and sophisticated investigative or prosecutive programs, and handled inquiries pursuant to the Freedom of Information and Privacy Act. ❖

FH: When the authorization is signed by the Deputy Assistant Attorney General, it is faxed back to us. The authorization memo, along with a letter from me to the United States Attorney, is faxed to the Assistant, and the Assistant then makes the actual application to the court.

JB: Does that process change depending on the type of wiretap case; for example, narcotics, public corruption, or computer? Do different people get involved or is it basically the same process?

FH: We send a copy of an original affidavit to the section of the Criminal Division that has the substantive responsibility for that subject area and ask them to review it, not for the existence of probable cause, but, rather, to determine if it is a significant case. Electronic surveillance is a very sensitive and important investigative tool, and we want it used where it is most advantageous. The section submits their comments at the same time we're cleaning up other matters with the Assistant. When the request is ready to go to the Assistant Attorney General or Deputy Assistant Attorney General for review, we also need to get a memorandum from the headquarters of the investigative agency requesting that the application be reviewed and approved. This sometimes delays the approval process for several hours or a day.

The Electronic Surveillance Unit is a collegial group. We assign the same attorney to any extensions and spinoffs, but if that person is on vacation or travel, another attorney can usually pick up the case without a problem, and there's not too much of a lag. Extensions are reviewed basically the same way as originals, except that we don't go to the substantive Criminal Division section for comments or to the investigative agency for a requesting memo. As such, we can usually get these done more quickly than the original request.

I see two problems with extensions. The first problem is that sometimes the Assistant doesn't oversee the agent when the affidavit is being prepared. Everyone is in a hurry, that's a given. For example, in a drug case the agent will often throw together a train of conversations that is in code. These drug codes are not exactly sophisticated. I read them and know exactly what they're talking about, when they're talking about half a truck, half a shirt, or a car with three tires, but we need a document that a judge can read. So we request that these conversations be characterized or briefly interpreted. We can't expect every judge to know drug codes, or be willing to interpret the codes if the agent, who is trained as an expert in these matters, is not willing to do so. The agent knows that when these people are talking about "cassettes" they're really talking about kilograms of cocaine. That's what this conversation means in the agent's opinion, which is based on his experience in the current investigation as well as previous investigations. It should be described that way. That's all we need. We're not talking about guilt beyond a reasonable doubt here. We're dealing with probabilities.

The second problem with an extension is timing. I know everybody is busy, and we're busy here too. If extensions are submitted on the 29th day of the 30-day interception period, it's a burden on everybody to get it approved in time. Giving priority to a last-day extension means some other AUSA's wiretap has to wait. We try to meet the demand, but we usually need two or three days lead time. While we don't need it on the 15th or 20th day, if the affidavit comes in on the 25th, 26th, or 27th day with the conversations characterized, recent investigative leads summarized, and the continuing need for interception set out, then we can almost certainly get it signed before the interception period expires.

"Whether for an original or extension request, each affidavit has to establish probable cause for three things: that a predicate crime as set forth in the statute [18 U.S.C. 2516(1)], has been or will be committed; that the people you're naming as violators are indeed committing these offenses; and that the people you are naming are using not just any phone but THAT phone or, if it's a request for a bug, THOSE premises to commit these specific offenses."

Frederick D. Hess

Whether for an original or extension request, each affidavit has to establish probable cause for three things: that a predicate crime, as set forth in the statute [18 U.S.C. 2516(1)], has been or will be committed; that the people you're naming as violators are indeed committing these offenses; and that the people you are naming are using not just any phone but THAT phone or, if it's a request for a bug, THOSE premises to commit the specific offenses.

We apply a standard to determine if there is probable cause. Sometimes it's difficult to meet, but if the two main things we look for are there, everything else usually falls into place and our review can be done quickly.

First, you have to have independent evidence (that is, evidence other than pen register information) within the past six months that illegal activity was discussed on

the target phone, or inside the target premises. For example, an informant in a drug case says, "I called him at this number [the target phone number] two months ago and tried to buy drugs," or within the last few months an undercover agent called the target phone to buy drugs, or the agent or informant was standing in the room where the phone is located when they overheard someone using it for a drug-related conversation. There are a number of other ways of doing it. For example, somebody's courier is arrested and he says, "Yes, I've done this before and every time I get there this is the number I call." At the same time, you have to have a pen register running on the target phone that shows when the phone was used and what numbers were called, which may be able to confirm the calls identified by the informant. In a pen register analysis, you can't just list a lot of phone numbers. You have to identify the number called and who uses it, and whether there's evidence that this person is involved in the criminal activity. This type of analysis also helps you determine which persons are likely to be intercepted in criminal conversations during the interception period.

Second, you have to establish that at least one pertinent phone call was made over the target phone within the last 21 days—and that can be by the use of pen register information. For example, the pen register shows that the target phone has been used recently to contact a known coconspirator. There's a problem when you can't get the independent evidence that the target phone has been used in furtherance of the crime, and all you have are pen registers that show that alleged drug traffickers are calling other alleged drug traffickers, with nothing to show what these conversations may be about.

I know that OEO's pen register policy has occasionally been a big bone of contention in the field. The policy is in place because we have a responsibility to the American people and to Congress to be very careful in how we apply the statute. We are engaged in extraordinary invasions of personal privacy and we have to be as certain as possible that these people are indeed doing what the affidavit alleges they're doing.

"I know that OEO's pen register policy has occasionally been a big bone of contention in the field. The policy is in place because we have a responsibility to the American people and to Congress to be very careful in how we apply the statute."

Frederick D. Hess

We have developed ways of making pen registers work without what some have called the "dirty" call. To do that you have to establish a pattern of phone use that supports other information in the affidavit. For example, your informant tells you that a truck is driven from Chicago to Texas every three weeks to pick up drugs. The informant says that the subjects always stop in St. Louis on the way back from Texas and call the target phone to report that they're almost home. Physical surveillance confirms that the subjects have stopped their truck in St. Louis, and a pen register/trap and trace reveals that a call was received over the target phone from St. Louis at this same time. The subjects are later surveilled as they park the truck at the location where the target phone is located. Around this time, the pen register goes wild indicating calls over the target phone to persons who have drug records and/or are suspected of distributing narcotics. Surveillance may then show that there is an increase in visits to the premises that are consistent with drug trafficking.

Now you've established a pattern that tracks what your informant told you. You don't have any traditional, direct evidence of phone use, but showing this kind of pattern between identifiable phone calls and the resulting drug activity makes it go. There may be other ways of doing this as well, and our attorneys work with the Assistants in setting out the facts in order to establish patterns where possible.

On the other hand, if all you have is that the informant says that a subject is a drug dealer, and the subject makes 100 or 200-plus calls a month to people who have drug records, and that's it, that is not enough. I don't know whether that might be enough to stand up in court, but that's not the standard we apply. We apply a higher standard because we understand that Congress enacted this statute, and Congress can take it away if it perceives that we are not exercising our supervisory role properly. It should not be easy to tap a phone, and we should not accept the very lowest

common denominator that a court might accept for probable cause. We need a little more than that. We don't ever want to jeopardize the existence of the wiretap laws, and the way we do this is to have a track record of judicious and careful application of the statute and a record of not getting suppressed in court based on a lack of probable cause.

"It should not be easy to tap a phone, and we should not accept the very lowest common denominator that a court might accept for probable cause. . . . We don't ever want to jeopardize the existence of the wiretap laws, and the way we do this is to have a track record of judicious and careful application of the statute and a record of not getting suppressed in court based on a lack of probable cause."

Frederick D. Hess

DN: Have you succeeded in this?

FH: In every case except for one time. I remember the first time that I met Steve Trott, who, at the time, was the Assistant Attorney General for the Criminal Division (and who is now a court of appeals judge on the Ninth Circuit). He came to the Department in the early '80s from the United States Attorney's office in Los Angeles and, before that, he was in the district attorney's office in Los Angeles. The first question he asked me was, "What is your rate of reversal on probable cause grounds?" At the time, I was able to say that it had never happened. Since then, we have been reversed once on probable cause grounds, but this record is still quite extraordinary. By the way, that's just once in many thousands of cases.

DN: What happens in emergency situations?

FH: We have two concepts for an emergency situation. One is the statutory concept, which is a 48-hour emergency, in which you get the Attorney General's oral permission to intercept wire or oral communications for 48 hours without a court order. We don't like these, because 48 hours go by so fast that there's a panic at the end to get it to court. The agents, who should be writing their affidavit because they're going to have to file everything within 48 hours, no matter what, are in the middle of the case. The problem is getting around to writing it. Usually, it's well past the 40th hour before we receive something, and we have to do the whole review process with the clock ticking because the statute mandates suppression of the evidence if the application is not made within the 48 hours. Because of this, we prefer to avoid them, so we limit them to life-threatening emergencies, usually a kidnapping or where a murder is believed to be imminent. There still has to be probable cause for the phone in all of this, and you have to show need. If all you can show are phone calls to the house of the kidnapped victim's family, then you don't have a need for the tap because you're listening to these calls with the family's permission, and you can identify the calling phone (through a trap and trace). Instead, you have to be able to show, usually through a pen register, that after the first call was made to the family over the target phone, this same phone was used to call somewhere else—maybe to an accomplice. These later calls are the ones that have to exist in order to justify the wiretap.

We can't worry too much about establishing patterns or a strict application of the pen register policy when a life is in danger—that's a whole different atmosphere. We'll do it, but those situations create enormous problems because agents and Assistants are not disciplined to start writing right away. Instead of this avenue to handle emergencies, we prefer a second course—that someone writes a bare-bones affidavit as rapidly as possible, and then we move very quickly and expedite the process as much as possible. When we get an affidavit that is in a shape that the Deputy Assistant Attorney General can read it (because we don't have time to write an action memo), we send it forward with the authorizing memo—this is assuming that the facts are there. Obviously, this is done only rarely, and not where there's just going to be a couple-pound load of cocaine coming in tomorrow, because a load probably came in last week and one is likely to come in again next week. Using just the affidavit and authorizing memo won't fly for that kind of thing. If something huge happens, like a person is in danger of being killed and we believe phone calls are going to be made to hit men, we're going to be up on that phone as soon as possible. Still, as you can see, it makes sense to do most emergencies as an "expedited review" with an affidavit wherever possible, rather than as a statutory, 48-hour emergency.

DN: What do you do with this bare-bones affidavit when you receive it? Where does it go when it reaches you? How is this procedure different?

FH: It's got to meet all of the statutory requirements. The difference is that we call the Terrorism and Violent Crime Section (or whatever section supervises the

underlying offenses) and get a 1-2-3 okay. We tell people in the field to notify FBI headquarters to get them to sign off on this because, until they do, it's not going to happen. We take the affidavit, call one of the five Deputy Assistant Attorneys General, and explain that we cannot write an action memorandum and that we will fax them the affidavit as soon as we get it. We review it here quickly, advise the Assistant what changes or additions are needed, and then we fax or hand carry it to Main Justice.

DN: Does this affidavit ever see its way into court?

FH: Yes; from the court's point of view it is just like any other affidavit. The point is that there **is** an affidavit—that's the difference between the 48-hour emergency and this expedited one. With the 48-hour emergency, you have nothing, no paper at all. You have a conversation between the Director of the FBI and the Attorney General, after everyone underneath says "okay, let's do this," and then within 48 hours you need an application, order, and affidavit for us to review, and all three have to be presented to the court within 48 hours from the time the Attorney General orally authorizes it. Forty-eight hours go by fast, and it's invariably a weekend. Whereas, if you write an affidavit that you can give to a judge prior to the tap, you're authorized for up to 30 days. The affidavit in a 48-hour emergency has to be based solely on what the Attorney General knew when she approved the emergency tap. When you go to court after the emergency authorization, you can only tell the judge as much as the Attorney General knew at the time she approved it, because the court has to validate the emergency interception. Now, if you've had some pertinent calls over the tapped phone in between, and you want to keep up on the tap after 48 hours, you need a separate extension request. The information in the extension request will be different than in the 48-hour emergency affidavit. You have to be careful to keep the documents separate because the first area of attack later on is going to be that the 48-hour affidavit contained something that the Attorney General didn't know at the time of her okay. If you have the bare-bones affidavit presented to court to start with, you can intercept for up to 30 days and won't have to worry about the 48-hour paperwork **and** an immediate extension request.

MK: We lost one where a judge decided it wasn't a true emergency. We went up on a wiretap pursuant to the emergency provision and, when we applied for the follow-up order, the judge ruled that it wasn't an emergency because we had time to file an affidavit in the first place. Some cases are true emergencies. A child is kidnapped and you've got to move fast. Most cases do not fall into that category. What I've discovered is that the agencies often think it's easier to get an emergency wiretap than it is to do the paperwork up front. They think an emergency wiretap requires no paperwork from the agents. But a 48-hour emergency means more paperwork and in a much shorter time frame.

FH: I want to make a point also about the *Electronic Surveillance Manual*. We published the manual originally in 1991 and sent it to every office. It contains draft forms for every conceivable pleading in a wiretap, pen register, you name it. It has been updated, and will soon be available on disk and on USABook. If an Assistant has read this and has tailored the affidavit to meet the requirements in the manual, then it can go through our office very quickly.

DN: Do you have any final message for Assistants?

FH: I've been through this for 15 years and every so often a great case comes along that you'll look back on for years. I'm thinking of the Pizza Connection case in which we worked with Rudy Giuliani when he was United States Attorney in the Southern District of New York. Louis Freeh was the AUSA in charge of the case. Several of these cases have been summarized elsewhere in this publication. (See pages 10 and 11.) These cases are memorable and you know that the wiretap was the thing that made the case. The wiretap is a great investigative tool and it can make your case for you. Cherish it, preserve it, and protect it. Don't ask us to push it beyond where it is supposed to go. Live with our pen register policy, because it has made the judges, Congress, and others happy. We will work with you to try to make it work in your case. This investigative tool is too important to play games with.

DN: How do you think the AUSAs are doing on wiretaps?

FH: They're doing great! ❖

The information concerning provisions or applications of Title III in the articles by Assistant United States Attorneys in this issue of the *United States Attorneys' Bulletin* are the opinion of the authors and not necessarily those of the Office of Enforcement Operations, Criminal Division, or the Department.

The Office of Enforcement Operations—Its Role in the Area of Electronic Surveillance

Prepared by the Staff of the Electronic Surveillance Unit
Office of Enforcement Operations
Criminal Division

The Office of Enforcement Operations (OEO) is the Criminal Division office responsible for overseeing the use of the most sophisticated investigative tools at the Federal Government's disposal in furtherance of domestic criminal investigations, including the interception of wire, oral, and electronic communications under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. As provided for in 18 U.S.C. § 2516 and Department of Justice (DOJ) regulations, the Department's approval must be obtained before applying to a Federal court for an order authorizing such surveillance.* OEO also has a supervisory role in the use of court-authorized video surveillance, as well as the consensual monitoring of non-telephonic communications in certain sensitive circumstances.

In FY 1996, OEO's Electronic Surveillance Unit (ESU) reviewed over 1,300 electronic surveillance requests—a figure almost 30 percent greater than that for FY 1995. The ESU's efforts in supervising the use of electronic surveillance also include providing legal advice to investigators and Assistant United States Attorneys (AUSAs), assisting with trial/appellate briefs and motions when requested, providing training, and assisting and commenting on all electronic surveillance matters that come through the Division. Julie P. Wuslich is the head of ESU and Janet D. Webb is the deputy chief. Nancy Brinkac, Gina DiGiuseppe, Robert Gerardi, Joan Holmes, Paul Joseph, Andrew Simonson, Natalie Thornton, and Steven Wasserman support the Unit and are directly involved in the review of wiretap requests. OEO Senior Counsel Stephen Harwood assists ESU in answering Title III-related questions from the field. Once recommended by ESU, requests for Title III approval go to either Associate Director Carla H. Raney, Senior Associate Director Maureen H. Killion, or Director Frederick D. Hess for final review and recommendation by OEO. (See accompanying interview and sidebar.) Then the requests are sent to the Assistant Attorney General's (AAG) office for review and possible approval by a Criminal Division Deputy Assistant Attorney General, or by the AAG or Acting AAG. The application **must** be reviewed and approved by the AAG or Acting AAG if a roving interception is involved. (An in-depth description of this approval process appears elsewhere in this issue.)

OEO's ability to keep pace with the demands of the United States Attorneys' offices (USAOs) and the Federal investigative agencies in their use of electronic surveillance is constantly being challenged by shifting investigative priorities. An increase in funding for the Drug Enforcement Administration (DEA) or the Organized Crime Drug Enforcement Task Forces, or a policy decision to increase the FBI's involvement in drug investigations, clearly results in more work for OEO's ESU. This is because Federal drug investigations—which target major drug importation and distribution organizations—draw upon wiretaps, because of investigative necessity, as one of their primary investigatory tools. The use of electronic surveillance is likely to increase substantially with the expected creation of dedicated wiretap units in a number of DEA field offices. From ESU's experience, it is clear that even relatively minor changes in electronic surveillance laws can increase substantially the workload of that unit.

AUSAs should be aware that the growing number of Title III requests received in OEO has forced the ESU's reviewers to prioritize their caseload to ensure expeditious review of the most time-sensitive Title III pleadings. As such, it is imperative that pleadings be submitted to OEO as soon as practicable. This is especially true in the case of requests for extensions of

*While 18 U.S.C. 2516(3) allows United States Attorneys to apply for a court order authorizing the interception of electronic communications without the need for prior Criminal Division approval, the *United States Attorneys' Manual*, at 9-7.000, et seq., requires prior Division approval for all applications to intercept electronic communications except those involving the interception of alpha-numeric pager communications.

interceptions of wire, oral, and/or electronic communications.

Criminal Division's Review of Title III Electronic Surveillance Requests

Pursuant to 18 U.S.C. § 2510, et seq., the Attorney General has delegated her authority to authorize applications for Title III electronic surveillance to the Assistant Attorney General, Acting Assistant Attorney General, Deputy Assistant Attorneys General, and Acting Deputy Assistant Attorneys General of the Criminal Division. The Division has established the following authorization process for applications for Title III court orders authorizing the interception of wire and/or oral communications:

1. A USAO and/or Federal criminal investigative agency submits an affidavit and related pleadings to the ESU.

2. The ESU refers the pleadings to the substantive office or section of the Criminal Division for a determination of the significance of the investigation. Concurrently, the investigative agency's headquarters personnel review the affidavit to determine whether the pleadings are legally sufficient and to make certain that the objectives of the investigation are within the general mandates and budgetary constraints of the agency.

3. Also, concurrent to 2, an ESU attorney reviews the pleadings to ensure legal sufficiency, significance, and compliance with the procedural requirements of Title III and with Department policies.

4. Then the ESU prepares an authorization memo for the signature of a Criminal Division official who is designated by the Attorney General to authorize requests. In a separate memo, OEO's Director recommends to the reviewing official that the request for interception be authorized or rejected. The official may then accept or reject this recommendation.

5. If approval is granted, a copy of the authorization memo, the Attorney General's Order of Special Designation, and a letter from the Director of OEO are sent to the USAO advising the United States Attorney of the approval. The first two documents are to be filed with the court as part of the court authorization process.

6. The USAO then files the respective pleadings and authorization memorandum with the district court and, if the judge agrees with the request to intercept, he/she will sign the court order authorizing the interception.

Although not statutorily mandated by Title III or the Electronic Communications Privacy Act of 1986 (ECPA), a similar review procedure is in place in OEO to handle USAO requests for court orders authorizing the interception of electronic communications (e.g., computers and facsimile machines), except those being placed to digital display paging devices. (For digital display paging devices, authorization by a supervisory attorney in the USAO is required.) ECPA requirements that must be complied with prior to the interception of pager communications, including the need for a court order, are believed sufficient to address applicable privacy concerns without the need for prior Criminal Division authorization.

Government Use of Electronic Surveillance— Extremely Important Cases

The following are just a sample of the major law enforcement investigations where electronic surveillance was critical to a successful resolution of the matter, whether obtaining the conviction of drug traffickers and the forfeiture of millions of dollars in drug assets or preventing the destruction of Government property and the loss of innocent lives. Generally, what distinguishes these investigations is the extremely secretive and sophisticated nature of the targeted individuals, whose knowledge of law enforcement techniques and intense fear of being detected and arrested leads them to be highly cautious in dealing with persons they don't know. These characteristics make traditional investigative methods less likely to be successful. These cases also involve complex offenses and/or a large number of defendants. In each of these Title III cases, wiretaps and bugs were essential to the

arrests and prosecutions of the defendants, and the seizure of millions of dollars in narcotics proceeds or other forfeitable assets.

The Commission Case—Organized Crime Convictions in Southern District of New York

In September 1983, the FBI began the first in a series of wiretaps and bugs targeting "the Commission"—the bosses of organized crime's five leading families. The Title III electronic surveillance in this investigation, employed continuously for 18 months, was extremely productive, providing the FBI with details of organized-crime-related activities that were well beyond the knowledge of any FBI informant. The information obtained from the Title III surveillance was used to put together an airtight case against the defendants.

Based in large part on the electronic surveillance information, the defendants were charged in the Southern District of New York with racketeering activities, including murders, loansharking, labor pay-offs, and extortion in the concrete industry. The prosecution presented more than 100 taped conversations at trial to bolster the informant information, other witnesses' testimony, and surveillance photographs. Eight defendants were convicted, including the heads of the Genovese, Lucchese, and Colombo organized-crime families.

Paul Castellano/John Gotti—Organized Crime Convictions in Eastern District of New York

In the early 1980s, the FBI commenced a Title III investigation of Paul Castellano, the reputed boss of the Gambino organized crime family. Agents installed bugs in Castellano's residence, and the intercepted conversations revealed that Castellano's organization was involved in numerous racketeering activities, including international car theft and conspiracy to murder. In February 1986, six of Castellano's associates were convicted of running the car theft ring.

In December 1985, Castellano was murdered by associates of John Gotti in a power struggle for control of the Gambino organization. To obtain evidence of the murder, FBI agents installed bugs and wiretaps in a social club frequented by Gotti. Based on intercepted conversations, Gotti was convicted in April 1992 of racketeering and conspiring to murder Castellano. Gotti's efforts to challenge his Federal conviction were rebuffed by the United States Supreme Court, and his conviction was upheld. He is currently serving a sentence of multiple terms of life imprisonment without the possibility of parole.

Herrera-Buitraga Organization—Cali Cartel Investigation in Eastern District of New York

One of the most successful uses of wiretaps in a narcotics investigation occurred in connection with the DEA's investigation of the Herrera-Buitraga organization. The investigation, which targeted New York City-based operatives for the Cali, Colombia, cocaine cartel, was largely dependent upon approximately 18 months of continuous court-authorized wiretaps of cellular telephones used by members of various New York cells reporting to major drug lords in Cali. During the investigation, the DEA was able to identify and tap over 100 cellular phones. The conversations led directly to millions of dollars' in cocaine and cash, which were seized by the DEA at various points in the investigation. At the conclusion of the taps in December 1991, the DEA arrested more than 100 individuals and seized $14.6 million in cash. Records seized during the arrests indicated that this group had been shipping $50 million a month in cocaine profits from New York to Cali.

The wiretaps were of critical importance in this investigation because the sophisticated and compartmentalized method of operation of the organization made the limited informant information of little importance. No one informant was in a position to provide more than the barest details on any area of the operation. Without the wiretaps, the DEA would not have successfully tied the operation to the Cali Cartel, or identified the participants and their method of operation.

Operation Illwind—Defense Procurement Fraud Convictions in Eastern District of Virginia

Between January 1987 and July 1988, the United States Attorney for the Eastern District of Virginia and the FBI conducted a series of court-authorized interceptions of wire and oral communications of several defense procurement consultants in the District of Columbia, the Eastern District of Virginia, the Middle District of Florida, and the Eastern District of New York. The investigation, known as "Operation Illwind," focused on allegations of bribery and fraud being committed by Department of Defense employees, contractors, and consultants in the award of massive procurement contracts for the military.

After 18 months of court-approved Title III interceptions, including approximately 30 "spinoff" wiretaps, the FBI executed approximately 45 search warrants and seized massive amounts of personal and corporate records. The investigation resulted in 64 convictions and $622 million in fines, including a $190 million fine against the Unisys Corporation.

Walter Moody—Murder of a Federal Judge Conviction in the Northern District of Georgia

In December 1989, Robert Vance, a judge on the United States Court of Appeals for the Eleventh Circuit, was killed by a bomb that was mailed to his residence. In April 1990, Federal agents targeted Walter Moody as a suspect in the bombing and, pursuant to a Title III court order, placed bugs in Moody's residence. Agents learned that Moody talked to himself about the bombing. In June 1990, Moody was arrested on an unrelated charge, and agents placed a bug in his prison cell. In June 1991, Walter Moody was convicted of first degree murder for killing Judge Vance. Prosecutors used evidence obtained from the bug in the prison cell to prove that Moody had created and sent the bomb.

Chinese Organized Crime—Gang Kidnapping Southern District of New York

On March 18, 1994, four Chinese nationals were kidnapped from a location in New York City by six men. This case, like several others recently, concerned illegal alien smuggling. Over the following day and a half, the kidnappers made 15 to 20 telephone calls to an associate of the victims, demanding money in exchange for their safe release. The kidnappers provided the associate with the number of a cellular phone and instructed him to contact them on that telephone. During this period of time, a pen register installed on the cellular phone revealed numerous telephone calls from the cellular phone to other phones.

On March 19, 1994, the Attorney General authorized the emergency interception of communications over the cellular telephone used by the kidnappers. The wiretap was credited with leading to a successful resolution of the situation: the four victims were recovered, relatively unharmed, and 12 people were arrested.

RUKBOM—Domestic Terrorism Northern District of Illinois

In RUKBOM, a domestic terrorism case, the El Rukn street gang in Chicago, attempting to act as a surrogate for the Libyan Government, proposed to shoot down a commercial airliner with a stolen military rocket, in return for financial remuneration. Electronic surveillance enabled law enforcement agents to prevent this attack, thereby saving over 100 lives (and possibly more) by averting a domestic disaster similar to the terrorist bombing of Pan Am Flight 103 over Scotland.

Zorro II—Cali Cartel's Operations in the United States Central District of California and nine other United States Attorneys' Offices

An extremely successful use of wiretaps in a narcotics investigation, code-named Zorro II, occurred in DEA's investigation of the Cali Cartel's operations in the United States. This investigation was concluded in the spring of 1996 and used over 90 court-authorized wiretaps (including extensions) that were conducted over nine months in ten judicial districts. Based on information produced by the taps, over 130 persons were arrested and 5,598 kilograms of cocaine and approximately $9 million in cash from drug proceeds were seized. (Commendations issued to AUSAs in connection with this matter were previously detailed in the July 1997 issue of the *USAB*.)

Use of Electronic Surveillance—Questions and Answers

Q: Why does OEO have a 21-day current probable cause requirement in wire, oral, and electronic interceptions?

A: Intertwined with the probable cause requirement of the Fourth Amendment and the provisions of Title III is the requirement that the information of criminal conduct and facility/premises usage—even if clearly established—not be stale; i.e., is not just historical in nature but is also such that a judge could reasonably conclude that the information is still current and the criminal activity is ongoing. Over the years, OEO has established a "21-day rule" to show that the probable cause is still "fresh." This means that when the Assistant Attorney General's office receives the request to authorize a Title III application, the latest use of the targeted facility or premises in connection with the crime must be within 21 days of that review. This time frame allows a few days to transpire before the application is presented to the district judge, thus ensuring that the information establishing probable cause will not become stale in the intervening period. While the 21-day rule may seem arbitrary, it has served the Government well. The various agency headquarters understand the basis for the rule and do their best to ensure that the affidavits meet this requirement before they are sent to OEO for review.

Q: What is the Criminal Division's pen register policy for wire interceptions?

A: The Criminal Division's pen register policy (instigated and supported by Acting Assistant Attorney General John C. Keeney) is that pen register information **alone** is not sufficient to establish probable cause for a wiretap.[**] Pen register records only show that one phone is being used to call another phone. They do not show that the phones are being used to discuss criminal matters. Therefore, there must be a showing (independent of pen register records) from which a judge may conclude that the phone to be tapped has been used in furtherance of specified criminal activities within the six-month period preceding the application. Obviously, the easiest way to do this is for an informant to have a consensually recorded conversation about criminal activities with a subject using the target phone. There are, however, other ways to show that the phone is being used to further criminal activities of the subjects. For example, an informant may see or overhear a subject using the target phone in connection with the criminal activities.

Finally, a detailed analysis of pen register activity showing **a pattern of calls** from the target phone at or around the time of known criminal activity may often be sufficient to establish probable cause for a wiretap. For example, probable cause will be established if, after each payment of a bribe to a representative of a public official, the pen register analysis shows that there is a call to the phone of the targeted official. Alternatively, if pen register analysis shows consistently that, before the delivery of a drug shipment, there were calls to the source of drugs in Mexico or Colombia or to contacts in each of the places where the drugs will be transiting, followed by a flurry of calls to known drug customers when the drug shipment is delivered, such a pattern is usually sufficient to establish probable case that the phone is being used in connection with the specified criminal activity. Each of those instances, coupled with pen register analysis showing calls from the target phone to known criminal associates within the preceding 21 days, should be sufficient to obtain Criminal Division authorization to apply for a wiretap. It is important to stress that raw pen register data, showing calls to suspected criminal associates, without an extensive analysis to establish patterns of activity such as described above, will normally not be sufficient to establish probable cause for a wiretap.

Q: Do the requirements differ regarding the use of Title III to intercept electronic and wire communications generated via computer or PC? Who in OEO handles these types of Title IIIs?

A: If a communication is neither "wire" (which requires an "aural," or voice transfer) or "oral," then it is electronic, and there is no distinction in Title III as to the interception of different facilities that are used in connection with sending and receiving electronic communications (e.g., computers, fax machines). If investigators wish to intercept a computer-to-computer transmission, then this is a purely electronic communication, and is intercepted as provided for in 18 U.S.C. §§ 2516(3) and 2518. If the communication has been sent and becomes a "stored electronic communication," it may be retrieved as provided for in 18 U.S.C. § 2703 (whether it is stored with a service provider or in a remote computing service). ESU attorneys who review Title III requests can provide assistance with these computer transmissions.

In situations where a computer has been seized and investigators wish to gain access to its contents, this planned seizure of information is not a Title III interception. Questions in this area should be directed to the Computer Crimes and Intellectual Property Section of the Criminal Division. Note, however, that if the computer user can be considered a "publisher," then any attempt to retrieve information stored in the computer may implicate provisions of the Privacy Protection Act of 1980 (42 U.S.C. 2000aa), and an approval process relating to conducting such a search would be handled by OEO's Policy and Statutory Enforcement Unit.

Q: Does OEO have a role in coordinating multi-district investigations that use Title IIIs?

A: Yes. Generally, in a multi-jurisdictional investigation, OEO assigns one attorney to review all the Title III applications. This attorney ensures that the applications submitted by the various districts are consistent with each other as to probable cause, the identification of subjects, and investigative objectives, and that each application correctly refers to the other applications filed, and establishes the investigative need for each wiretap, addressing specifically how each wiretap interrelates with the others. Moreover, the OEO attorney may help identify potential conflicts in the investigation that might be caused by the planned takedown of a case in one jurisdiction while the

[**] OEO Director Frederick Hess provides additional commentary regarding OEO's pen register policy in his interview.

investigation continues elsewhere. Finally, the OEO attorney attends investigation strategy sessions where such strategies are discussed and plans are formulated to initiate additional wiretap cases.

Q: Under what circumstances does the Government need to obtain a Title III order to intercept electronic communications to a pager? When will a search warrant suffice? Are there any exceptions?

A: Three types of pagers are addressed specifically in Title III: (1) tone-only pagers, (2) digital display pagers, and (3) tone-and-voice pagers. Tone-only pagers simply beep when a call is received, digital display pagers exhibit messages in letters and numbers on a small screen, and tone-and-voice pagers receive the spoken message sent by the caller. Only digital display and tone-and-voice pagers require Title III authorization before interception. Because digital display pagers receive electronic communications for which an expectation of privacy exists, the Government must obtain an order to intercept **electronic** communications pursuant to 18 U.S.C. § 2516(3) and § 2518, when it seeks to use a clone of the targeted pager to intercept the electronic communications being transmitted to the targeted pager. Interception orders for digital display pagers may be sought for **any Federal felony**. On the other hand, tone-and-voice pagers require an authorization to intercept **wire** communications and, thus, the application must specify one of the Federal offenses listed in 18 U.S.C. § 2516(1), and **must** be authorized by a specified Department of Justice official.

While pager applications are not reviewed by OEO, and authorization by Criminal Division officials is not required, they **must** be authorized by a supervisory attorney in the USAO. It is important to remember that the affidavit, application, and order must meet all requirements of 18 U.S.C. § 2518, including probable cause, statements of prior application, and duration. Progress reports must be filed if requested by the court, and extensions also must be approved by a supervisory attorney in the USAO. Additionally, pager Title IIIs may be signed only by district court judges, **not by magistrates** [18 U.S.C. §§ 2516(1) and 2516(3)].

It is important to distinguish between using a clone pager to intercept electronic communications as they are transmitted, for which a Title III order is required, and obtaining stored paged messages directly from a pager after it has been lawfully seized incident to an arrest. When agents arrest an individual and lawfully seize the individual's pager, the agents are in lawful possession of the pager, but may they retrieve the stored messages without obtaining a search warrant? While no expectation of privacy exists for those persons who sent messages to the seized pager, [see *United States v. Meriwether*, 917 F.2d 955 (6th Cir. 1990) (where defendant could not claim an expectation of privacy in the phone number he input into a pager that was seized by agents)], an expectation of privacy **does** exist for the person in possession of the pager at the time of the seizure. This expectation may be overcome, however, by one of the exceptions to the warrant requirement, especially where agents are aware that pager messages could be lost if not retrieved, and thus exigent circumstances may exist. [See also *United States v. Chan*, 830 F.Supp. 531 (N.D. Cal. 1993) (pager seized incident to arrest); *United States v. Lynch*, 908 F.Supp. 284 (D. V.I. 1995) (same); *United States v. Ortiz*, 84 F.3d 977 (7th Cir. 1996) (same); *United States v. Reyes*, 922 F.Supp. 818 (S.D.N.Y. 1996).] These courts upheld the warrantless retrieval of numbers from the memories of pagers seized incident to a lawful arrest and during consensual searches of cars.

Q: Why do we need a Title III application to intercept a pager? Isn't the privacy right in wire communications entirely different in nature than electronic communications?

A: While telephone calls and communications over a digital display pager are different in nature, they are still "communications" protected both by Title III and the Fourth Amendment. While some argue that pager intercepts provide similar information to that obtained from pen registers, this is not totally true. What a pen register records— and which the Supreme Court has held is **not** protected by the Fourth Amendment—are the numbers dialed from a telephone in order to reach another party and carry on a conversation. The numbers dialed **were not** the intended communication. In contrast, the numbers a pager intercept records are the numbers the caller punches into his or her phone after making contact with the pager company. These numbers—often the phone number to be called to return the incoming call, or codes like "911" for emergencies or types of access numbers—are, in fact, the intended communication. This is a distinction that makes all the difference, both statutorily and constitutionally.

Q: What are digital analyzers and cell site simulators, and is a court order required to use them?

A: It is now possible for agents to capture electronically the unknown electronic serial number (ESN) or telephone number of a cellular telephone through the use of a device known as a **digital analyzer**. It can be

programmed to identify the telephone number assigned to the subject cellular telephone and telephone numbers dialed from this phone, as well as its ESN; i.e., a number assigned by the cellular telephone manufacturer and programmed into the telephone. Although this device is also capable of intercepting both the numbers dialed from the cellular phones and the voice (wire) communications to and from cellular telephones, the digital analyzer is programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone's number.

Similarly, a **cell site simulator** (CSS) can provide agents with a cellular telephone's ESN and mobile identification number ("MIN," which contains the cellular telephone number and other information related to the operation of the phone). The CSS simulates some of the activities of a cellular service provider's cell site transmitter, albeit in a much smaller area, and allows agents to query cellular phones for their ESNs and MINs through "autonomous registration," an activity a cell site transmitter normally conducts to identify cellular phones operating within its cell or area. Like a real cell site transmitter, the CSS can determine ESNs and MINs of cellular phones that are "powered up" or turned on. (The phone need **not** be in a "use" mode; the information can be obtained unbeknownst to the cellular phone user.)

In addition to capturing ESNs and MINs of cellular telephones, digital analyzers/CSSs can capture the cell site codes identifying the cell location and geographical sub-sector from which the cellular telephone is transmitting; the call's incoming or outgoing status; the telephone numbers dialed (pen register order required); and the date, time, and duration of the call. This cell site data is transmitted continuously from a cellular telephone (not by the user) as a necessary part of call direction and processing. The service provider uses this information to connect with the account in order to direct calls, and constantly reports to the customer's telephone a readout regarding the signal power, status, and mode of the telephone.

If a Government agent, without involving the cellular telephone service provider, uses a digital analyzer or CSS either to obtain from a cellular phone its MIN and ESN, it does not appear that there are constitutional or statutory constraints on the warrantless use of such a device by the Government. See *In The Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995), and *Smith v. Maryland*, 442 U.S. 735 (1979) (the Fourth Amendment provides no privacy protection for numbers dialed on a telephone). With regard to 18 U.S.C. §§ 3121-3127 (pen register/ trap and trace statutes), the Department's policy is that, to the extent CSSs and digital analyzers are used as pen registers or trap and trace devices, they should only be used pursuant to a court order issued pursuant to these statutes.

Specifically, Title III's provisions (18 U.S.C. §§ 2510-2522) would not apply to the use of a digital analyzer or a CSS when they are used to capture call processing information (MIN, ESN, cell site location, status of call, etc.) because they do not intercept the contents of any wire, oral, or electronic communication as the term "contents" is defined by Title III. Currently, Section 2510(8) states, "'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that information." ESNs/MINs and other automatic call processing information that are technologically necessary for the service provider to process cellular calls are not the types of transmissions Congress included within Section 2510(8)'s definition of "contents" when it was amended in 1986. [See S. Rep. No. 541, 99th Cong., 2d Sess. 13 (1986).]

In addition, there is no "electronic communication" [as defined by 18 U.S.C. § 2510(12)] unless the MIN or ESN is "transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce." A transmission normally contemplates a sender and a receiver. The ECPA legislative history regarding the definition of wire communication warns against an improper mechanical reading of the phrase "in whole or in part. . . by the aid of wire. . . ," and states that the phrase "is intended to refer to wire that carries the communication to a significant extent from the point of origin to the point of reception, even in the same building. It does not refer to wire that is found inside the terminal equipment at either end of the communication." [S. Rep. 99-541, 12.] Thus, it does not appear that MINs and ESNs "forced" from the cellular telephone by the CSS or obtained by a digital analyzer are "electronic communications" within the contemplation of 18 U.S.C. § 2510(12).

If cell site information is treated as a subscriber record or other information rather than a contemporaneous electronic communication covered by Title III, then 18 U.S.C. § 2703 (regarding stored electronic communications) might apply. It should be noted, however, that Section 2703 controls disclosures by service providers to Government entities and does not prohibit the Government from obtaining such information on its own without involving the service provider. Additionally, because CSSs and digital analyzers do not access communications in electronic storage in a facility

with electronic communication service, Section 2703 does not apply.

Q: Are cordless telephones covered by Title III?

A: Sections 2510(1), 2510(12), and 2511(4)(b) of Title 18, U.S.C., were amended in 1994 to include the radio portion of cordless telephone communications as protected wire or electronic communications. Consequently, there is no longer an exception to the Title III requirements for the radio portion of a cordless phone. Now a Title III order is required to intercept **all** wire communications over a cordless, cellular, or landline telephone. Illegal interception of the radio portion of cordless telephone communications is subject to the same criminal penalty scheme that is applied to the illegal interception of cellular telephone communications. The penalty for a first offense is a fine of not more than $5,000 if the interception was not for a tortious or illegal purpose, or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication is not scrambled or encrypted.

Two practical effects of this provision are that agents may no longer use a scanner to monitor **any** telephone conversations without obtaining court authorization [18 U.S.C. § 2510(1)], and second, the provision applies not only to law enforcement but to private citizens monitoring cordless phone conversations on their scanners. Citizens may not monitor scanners and then give that information to law enforcement. Existing case law states clearly that only **inadvertent** interceptions can be used by law enforcement. If a citizen is **intentionally** monitoring cordless or cellular phone conversations, that information is not admissible and the person could be in violation of Title III [*Thompson v. Dulaney*, 970 F.2d 744 (10th Cir. 1992); *Bess v. Bess* 929 F.2d 1332 (8th Cir. 1991); and *Shaver v. Shaver* 799 F. Supp. 576 (E.D.N.C. 1992)].

Q: What process can the Government take to seize information contained in an electronic notebook?

A: Electronic notebooks are small, electronic address books used to store names, numbers, and other information often found in drug ledgers. When an agent seizes one of these items, a Title III order is not needed to search the information contained in the notebook because the retrieval of the data is not an "intercept" as defined in 18 U.S.C. § 2510(4). However, a search warrant may be needed depending on the circumstances described below.

There is a protected expectation of privacy in the memory of an electronic data notebook. [*United States v. David*, 756 F.Supp. 1385, 1390 (D. Nev. 1991); *United States v. Chan*, 830 F.Supp. 531, 534 (N.D. Cal. 1993)] An electronic address book is "indistinguishable from any other closed container and is entitled to the same Fourth Amendment protection." [*David*, 756 F.Supp. at 1390. See also *United States v. Blas*, 1990 WL 265179 (E.D. Wis. 1990)]

The expectation of privacy exists regardless of whether the notebook has password protection or not. A password to an electronic address book is analogous to a key to a locked container. [*David*, 756 F.Supp. at 1391]

Because closed containers are accorded Fourth Amendment protection, an exception must exist to justify a warrantless search of an electronic data notebook. For example, as with other closed containers, police may examine the contents of containers found on or near an arrestee during a search without a search warrant. [*New York v. Belton*, 453 U.S. 454, 461 (1981)]

In *David*, an agent seized the defendant's address book based on the agent's belief that the defendant was deleting information from it. [*David*, 756 F.Supp at 1392] Once the address book was seized, however, the exigency that justified the seizure evaporated, and the warrantless search of the contents of the book was unjustified. [*Id*] Fear that the device's batteries would die and, therefore, the information would be lost, was not sufficient to justify a search. [*Id*. at 1392 n.1.]

As noted in *David*, the data contained in electronic data notebooks can be deleted easily and, therefore, exigencies may arise that justify seizure of the devices to prevent loss of evidence. [*Id*. at 1389] However, the "difference between possessory interests and privacy interests may justify a warrantless seizure of a container for the time necessary to secure a warrant, where a warrantless search of the contents would not be permissible." [*Id*. at 1392]

Q: What is required to seize stored wire communications in a voice mail system?

A: There has been much debate about whether a Title III order or a search warrant is needed to seize wire communications stored in a voice mail system. The confusion exists because the statutory definition of wire communications—the body of case law defining the meaning of an interception—and the legislative history do not give a succinct and cohesive answer. It is Department policy that if the Government is seeking to seize wire communications stored in a voice mail system, a search warrant is required. If the Government seeks to capture wire communications contemporaneously as they are left on a voice mail system, then a Title III order is required. Recently, in *United States v. Moriarty*, ___ F.Supp. ___ (D. Mass. 1997) (1997 WL 249206, May 7,

1997), the court accepted the magistrate's report and recommendations concerning a motion to dismiss a count of an indictment. Specifically, the Government indicted the defendant on charges of illegal wiretapping, under 18 U.S.C. § 2511(1)(a), and unlawful access to voice mail, in violation of 18 U.S.C. § 2701. Pursuant to the Double Jeopardy Clause of the Fifth Amendment, the defendant sought dismissal of the wiretapping count, arguing that the wire tapping counts and voice mail counts were duplicitous. The Government argued that Section 2511(a)(1) requires the defendant to actually acquire the content of a communication, and Section 2701 only requires access to it which, by implication, does not necessitate the acquisition of the communication. In other words, when the defendant listened to the voice mail messages, he did more than just access them, he intercepted them. The court's analysis, too, focused on the differences between the terms "intercept" in Section 2511(a)(1) and "access" in Section 2701. The court, however, determined that the term "'intercept' requires the contemporaneous acquisition of the information, whereas 'access' could apply to both contemporaneous and stored transmissions." Under the facts of this case, the court found that the defendant's listening to the voice mail messages did not make it an intercept within the meaning of 18 U.S.C. § 2511(a)(1) because "[o]nly the interception of voice mail while in transmission, like a wiretap on a telephone in use, can amount to a violation of Section 2511 [of Title 18, United States Code]." Accordingly, the wiretap count was dismissed.

Based on this court decision, it appears that only a search warrant would be needed to obtain stored wire communications on a voice mail system, because accessing the communications after transmission would not be a contemporaneous interception for which a Title III order would be needed.

Conclusion

On the opposite page is a chart that shows for each type of communication, the applicable section in the U.S.C., who approves the order, and other steps to take when court orders are necessary to obtain access to wire, oral, and electronic communications.

For further information, please contact Electronic Surveillance Unit attorneys during work hours at (202) 514-6809 or, for after-hour emergencies, through the Justice Command Center at (202) 514-5000. ❖

Mechanisms by Which the Government Can Obtain Wire, Oral, and Electronic Communications and Related Information[***]

Type of Communication	Court Order	Search Warrant	Subpoena (Admin., grand jury, trial)
Wire, electronic, or oral communications (e.g., telephone calls, pager messages, faxes, Emails, computer transmissions, and face-to-face communications)	Pursuant to 18 U.S.C. § 2510, et seq. (Title III); must be signed by a Federal district court judge	N/A	N/A
Stored electronic communications (e.g., Emails, pager messages, and voice mails in storage 180 days or less); see 18 U.S.C. § 2703(a)	N/A	As provided for in 18 U.S.C. § 2703(a); no prior notice to customer or subscriber	N/A
Stored electronic communications in electronic storage more than 180 days; see 18 U.S.C. § 2703(a)	Drafted pursuant to 18 U.S.C. § 2703(d); prior notice to customer or subscriber unless notice is delayed pursuant to § 2705; magistrate may sign	As provided for in 18 U.S.C. § 2703(a), (b); no prior notice	As provided for in 18 U.S.C. § 2703(a), (b); prior notice to customer or subscriber unless notice is delayed under § 2705
Material held or maintained on a remote computing service (e.g., Email, business records, credit records, payroll records); see 18 U.S.C. § 2703(b)	Drafted pursuant to 18 U.S.C. § 2703(d); prior notice to customer or subscriber unless notice is delayed under § 2705; magistrate may sign	As provided for in 18 U.S.C. § 2703(b); no prior notice	As provided for in 18 U.S.C. § 2703(b); prior notice to customer or subscriber unless notice is delayed under § 2705

Continued

[***] This table does not address prison monitoring, consensual monitoring, or the use of video surveillance. Questions regarding the use of these investigative techniques should be referred to the Office of Enforcement Operations' Electronic Surveillance Unit.

Type of Communication	Court Order	Search Warrant	Subpoena (Admin., grand jury, trial)
To install or use a pen register or a trap and trace device	Pursuant to 18 U.S.C. § 3121, et seq.; magistrate may sign; order sealed until otherwise ordered by court	N/A	N/A
Government use of a digital analyzer, Trigger-fish, cell site simulator, or other device to capture cellular phone ESNs, MINs, and cell site locale, without the aid of the service provider	N/A	N/A	N/A
A record or other information about a subscriber or customer of a communications service provider or remote computing service (not including the contents of communications); see 18 U.S.C. § 2703(c)(1)(B)	Drafted pursuant to 18 U.S.C. § 2703(d); magistrate may sign; notice to customer or subscriber is not required	As provided for in 18 U.S.C. § 2703(c)(1)(B); notice to customer or subscriber is not required	N/A
Name, address, local and long distance toll records, telephone numbers, or other subscriber numbers or identities, and types of service; see 18 U.S.C. § 2703(c)(1)(C)	Drafted pursuant to 18 U.S.C. § 2703(d); magistrate may sign; notice to customer or subscriber is not required	As provided for in 18 U.S.C. § 2703(c)(1)(C); notice to customer or subscriber is not required	As provided for in 18 U.S.C. § 2703(c)(1)(C); notice to customer or subscriber is not required

Electronic Surveillance Guide

Michael R. Sklaire, Trial Attorney
Narcotic and Dangerous Drug Section
Criminal Division

"We just arrested the main target of our investigation and he had a pager on him. Is a search warrant required to look at the stored messages?"

"I have a case involving fraud over the Internet, and I want the subscriber information for a target subject's account. Do I need a court order or will a subpoena be sufficient?"

"I know I need a Title III to record the bad guy's conversations. What if I want to put a video camera in his residence. Do I need a Title III? Do I have to send the affidavit to Washington for approval?"

Every Assistant United States Attorney (AUSA) working with agents on ongoing criminal investigations will be asked these types of questions. Specifically, the agents want to know what type of court order, if any, is needed to obtain electronic information such as phone records, dialed numbers, and computer files. Attached is a chart of the most commonly requested searches conducted in a criminal investigation, from real-time interceptions to stored computer records. Please note that there are many issues involved in doing electronic searches that are not covered here. Specifically, the statutes and case law dictate different notice, disclosure, minimization, and reporting requirements for each type of search. Please contact the Electronic Surveillance Branch of the Office of Enforcement Operations (OEO), at (202) 514-6809, or the Computer Crimes Section at (202) 514-1206, with any questions concerning these requirements. The chart is broken down into the following headings:

1. **Information Sought**: Set forth below are general categories of requested information, ranging from the numbers dialed from a subject's phone to the subscriber's name, to the actual intercepted conversations. As defined in 18 U.S.C. 2510, a "wire communication" is any communication involving a phone (cordless, residential, business, even cloned). An "oral communication" is any conversation intercepted through the use of a bug or listening device placed in the room. An "electronic communication" is anything intercepted over a pager, computer, or facsimile machine. **Under Federal law, if one party to a wire, oral, or electronic communication consents to the recording or monitoring of that communication, then no order, warrant, or Title III is required.** The categories set forth in this chart apply to situations when **no** party consents to the interception of the communication.

2. **Device**: This category provides common terms for interception or access devices. Some agencies may refer to a pen register as a "DNR" (Dialed Number Recorder). A Caller ID device is the same thing as a "trap and trace."* A "cell site simulator" or "digital analyzer" is a device that captures the electronic serial number and phone number of a cellular phone. A "cloned cellular phone" is a device that is programmed to copy and capture the billing information of another phone so that any calls made by or to the cloned cellular phone are billed to the legitimate subscriber.

3. **Paper Needed**: A general rule is that if your agents want to intercept a conversation or message "real-time," while the communication is occurring, then a Title III warrant is needed. If they desire communications in storage, such as stored pager or computer messages, then a search warrant is needed. If the desired information is toll records or transactional data (subscriber names and addresses), then a subpoena is required. A Title III affidavit must contain much more information than just a showing of probable cause. Also, the probable cause section of a Title III is much more extensive than in an affidavit for a search warrant. Contact OEO for samples. For stored communications and data, be sure to check the case law and contact the Department's Computer Crimes Section.

4. **Statute:** Sections 2510-2520 of Title 18 should be referred to when doing real-time interceptions of wire, oral, and electronic communications. Sections 3121-3123 should be referred to when conducting pen registers and trap and trace devices (real-time interception of dialed digits). Sections 2701-2710 should be referred to when dealing with "stored electronic communications," otherwise known as computer files off a network, toll records from the phone company, historical

*United States v. Fregoso, 60 F.3d 1314 (8th Cir. 1995)

pager communications, etc. Section 2703 sets forth whether you need a search warrant, court order, or subpoena for the stored information. Finally, Rule 41 of the Federal Rules of Criminal Procedure (FRCP) governs any search warrant.

5. **Authorizing Official(s):** Only district court judges may authorize Title III interceptions (real-time communications). Magistrates may authorize search warrants, pen registers, and court orders for stored communications. In addition, before you get district court authorization for a Title III, remember the statute requires that the Assistant Attorney General of the Criminal Division, or one of the Deputy Assistant Attorneys General (DAAG) authorize the interception. That is accomplished by contacting OEO's Electronic Surveillance Branch. All Title III paperwork **must** be sent to OEO for approval, with the exception of clone pagers, which can be approved in the respective United States Attorneys' offices. In addition, the use of a Closed Circuit Television (CCTV) needs to be approved by OEO before getting a warrant signed.

6. **Duration:** The general rule is that you have 30 days to conduct a Title III and 60 days to conduct a pen register, before you must go back to court (and OEO in the case of Title III) for new authorization. However, if the objectives of the investigation have been met prior to the end of the 30-day period, then interception must be terminated. For a Title III, the 30-day interception period begins either when the interception is first conducted pursuant to the court order, or 10 days after the judge signs the order, whichever comes first.

7. **Standard of Review**: For pen registers, trap and trace devices, and Caller ID devices, you must show the magistrate simply that the information is "relevant and material to an ongoing criminal investigation." For court-authorized disclosure of phone records, subscriber information, and other "transactional data," as defined in 18 U.S.C. 2703(c), you must show "specific and articulable facts" that reflect why this information is relevant and material. For a Title III search warrant, your affidavit must reflect more than probable cause for a search warrant, "probable cause plus." The probable cause standard for a Title III is higher than for a normal search warrant. In essence, you must show the court that the particular phone (fax, computer, pager . . .) is **clearly** being used for illegal purposes. Mere inferences that the phone is being used based on pen registers and toll records are not usually sufficient. Common ways to achieve "probable cause plus" are through the use of consensual calls made to the target facility, combined with pen register or toll record analysis reflecting that the facility has been and is still being used for illegal purposes.

A Title III order differs from a normal search warrant also in the statutory requirements of necessity and alternative investigative techniques contained in 18 U.S.C. 2518. The Government must show the court why normal investigative procedures have not succeeded in obtaining the required evidence concerning criminal activity. Further, in a Title III affidavit, minimization provisions must be set forth.

In addition, for a "roving" wiretap where the targets change phones every few days, the court must make a specific finding that the phones are being dropped so often to thwart interception by law enforcement [18 U.S.C. 2518(11)(b)]. Note that there is also a provision for "roving" oral interception, whereby it is not possible (or practical) to identify the location of the interception prior to the communication occurring [18 U.S.C. 2518(11)(a)].

For a CCTV that is installed surreptitiously by the agents, the standard of review is probable cause, the same as a search warrant. However, many circuits have now adopted the standard set forth in the Ninth Circuit in *United States v. Koyomejian*,** whereby the CCTV search warrant must resemble a Title III warrant in terms of including such Title III requirements as minimization, alternative investigative techniques, and duration. Often, a request for CCTV is filed at the same time as a request for Title III interception of oral communications (bug). Contact OEO for further details. ❖

**970 F.2d 536 (5th Cir. 1992)

Commonly Requested Searches

Info Sought	Device	Paper Needed	Statute	Authorizing Official(s)	Duration	Standard of Review
Phone Number Dialed— Real Time (outgoing)	Pen Register	Court Order	18 USC 3121	Magistrate	60 Days	Relevance
Phone Number Dialed— Real Time (incoming)	Trap and Trace/ Caller ID	Court Order	18 USC 3121	Magistrate	60 Days	Relevance
Incoming and Outgoing Phone Numbers Dialed and Subscriber Info—in Storage	Toll Records	Grand Jury Subpoena Admin Subpoena Court Order	18 USC 2703(c)	Grand Jury/ Agency/ Magistrate		Specific and Articulable Facts (Relevant and material to an ongoing investigation)
Oral Communications	Bug	Title III	18 USC 2518	District Court Judge and DOJ - DAAG/ OEO	30 Days (from 1st interception, or 10 days from signing)	Probable Cause+
Wire Communications (Real Time)	Cellular Phone Hardline Phone (business or residential) Cordless Phone	Title III	18 U.S.C. 2518	District Court Judge and DOJ - DAAG/ OEO	30 Days	Probable Cause+
Faxed Documents (Real Time)	FAX Machine (electronic communica-tions)	Title III	18 U.S.C. 2518	District Court Judge and DOJ- DAAG/OEO	30 Days	Probable Cause+
Computer Files/ Stored or Down-loaded	Computer Stand-alone	Search Warrant (if info in storage 180 days or less)***	18 USC 2703(a) and Rule 41 FRCP	Magistrate		Probable Cause

Continued

*** For information in storage more than 180 days, a subpoena or court order may be sufficient.

Info Sought	Device	Paper Needed	Statute	Authorizing Official	Duration	Standard of Review
Computer Messages Sent via Email, Internet, Network System (Real Time Interception)	Computer Network (America Online, DOJ Phoenix, for example)	Title III (if real-time interception)	18 U.SC 2518	District Court Judge/and DOJ- DAAG/ OEO	30 Days	Probable Cause+
Wire Communications over Fraudulent Phone	Cloned Cellular Phone (wire com-munications)†	Title III	18 USC 2518	District Court Judge and DOJ-DAAG/OEO	30 Days	Probable Cause+
Use of Multiple Cellular Phones (changing so often that the numbers cannot be identified)	Roving (wire communica-tions-Changing phones every 2-5 days)	Title III	18 USC 2518(11) (b)	District Court Judge and AAG- Contact OEO	30 Days	Probable Cause & Changing Facilities with purpose to thwart interception
Video (Installed by Agents in Residence/ Business)	Video-CCTV (Closed Circuit Television)	Rule 41 Search Warrant + Title III Requirements	Rule 41 FRCP	District Court Judge and OEO (DOJ policy)	No More than 30 Days	Probable Cause with Title III Requirements (Duration, Minimization, alternative techniques, etc.)
Video Camera Already on Premises	Security Camera-(already in place—need interception equipment to monitor	Title III (electronic communication)	18 USC 2518	District Court Judge and DOJ-DAAG/OEO	30 Days	Probable Cause+
Video (Outside Premises—Public Area)	Pole Camera	No Warrant Needed (unless viewing protected area, then search warrant required)††				

†A Title III is needed even if the phone is fraudulent or stolen because the "communication" is protected under Title III, regardless of the facility used.

††Examples of protected areas include the installation of a fence, closed curtains, or closed garage door. When the subjects exhibit an EXPECTATION OF PRIVACY, then a search warrant is required.

Info Sought	Device	Paper Needed	Statute	Authorizing Official	Duration	Standard of Review
Names and Numbers from Electronic Address Book	Elec. Data Notebook	Search Warrant	Rule 41 FRCP	Magistrate		Probable Cause
Tracking Device	Transponder, Bumper Beeper, GPS (global positioning system)	Search Warrant[†††] (To install or monitor signal in 4th Amendment protected area.)	Rule 41 FRCP	Magistrate		Probable Cause
Identify Cell Phone by Electronic Serial Number (ESN) or Phone Number (MIN)	Cell Site Simulator, Digital Analyzer (reads Electronic Serial Number and Phone number of cellular phone)	1. 2703 Court order if only ESN/phone number requested and search requires phone company's cooperation[‡] 2. Pen Register order if dialed numbers requested 3. Title III if conversation intercepted	1. 18 USC 2703(d) 2. 18 USC 3121 3. TITLE III	1. Magistrate 2. Magistrate 3. District Court Judge and DOJ - DAAG/OEO		1. Specific and Articulable Facts 2. Relevance 3. Probable Cause +
Info from Seized Pager	Pager-seized	Search Warrant (unless incident to arrest–then no paper needed)[‡‡]	Rule 41 FRCP	Magistrate		Probable Cause
Realtime Intercept-Messages Sent to Pager (Clone)	Pager-cloned (electronic communication)	Title III	18 USC 2518	District Court Judge and DOJ-US Attorney Approval Needed	30 Days	Probable Cause+
Voice Messages in Storage	Voice Mail Answering Machine	Search Warrant	Rule 41[‡‡‡]	Magistrate (Contact OEO!)		Probable Cause+

Don't Forget To . . .

[†††]In those rare instances when you know that the car will remain in public view at all times, then a search warrant is not required.

[‡]No paper is needed if the agent is using this device to find this information without the phone company's assistance.

[‡‡]The case law suggests that if a pager is searched **immediately** following the legitimate arrest, then no warrant is necessary pursuant to an exigent circumstances argument. However, any delay removes the exigency and a search warrant would be required.

[‡‡‡]The legislative history of Title III suggests that voice messages in storage are covered by Title III. However the case law pertaining to answering machine tapes suggests that a search warrant is sufficient. Contact OEO for further details.

Michael R. Sklaire, Trial Attorney
Narcotic and Dangerous Drug Section
Criminal Division

So you have completed a successful Title III investigation. The subjects used the phone to talk about their illegal activity, the interceptions led to the identification and eventual arrest of numerous co-conspirators, and you were able to seize drugs and money from the organization. The takedown went smoothly, the grand jury had no doubts, and the case is proceeding to trial.

And then THE MOTION arrives. Defense counsel has conveniently pointed out to you and the court that you forgot to seal up the tapes at the end of the investigation. Result: Wire interceptions suppressed. So much for the successful investigation!

Every Assistant United States Attorney (AUSA) who has conducted wiretap investigations wakes up in the middle of the night with the same nightmare involving one of those annoying statutory requirements that, if not done, will sink the investigation. Title III requires certain ministerial tasks that force an AUSA to get involved in an investigation more than with any other investigative technique. From the drafting of the wiretap, to the monitoring of conversations, to the termination of interceptions, suppression lurks for the AUSA who forgets these tasks.

Section 2518 of Title 18, United States Code, sets forth the procedures for obtaining Title III authorization and for conducting the interceptions. Among those procedures are requirements for (1) including prior applications of all target subjects and facilities, (2) conducting the investigation within a 30-day period, (3) minimization, and (4) sealing. If not done, each of these requirements could result in suppression, regardless of the quality of the interceptions. Below are some tips to guarantee that the wiretap evidence will be presented to the jury.

Prior Applications

Section 2518(1)(e) of Title 18, United States Code, requires that a Title III affidavit **must** include,

> "a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application."

In each affidavit, whether an original, extension, or a spinoff, the agent must list every prior interception for each of the target subjects named, the location (if the application is for a bug), and the target facility (for a phone, pager, computer, or fax machine). Each investigative agency has an electronic surveillance unit ("ELSUR") that keeps computer records of all Federal prior interceptions for each of these categories. The agent must state in the affidavit that those indices have been searched. That search must be conducted within 45 days of the court's order. Note that this only applies to Federal interceptions. The case law has reflected that the agent need not check every state's indices, only those of which the agent (or AUSA) has personal knowledge. See *U.S. v. Persico*, 1994 WL 36367 (E.D.N.Y. January 28, 1994).

Several courts have held that if the failure to include the prior applications was inadvertent or a good faith error, then suppression is not the remedy. [*U.S. v. Bianco*, 998 F.2d 1112 (2d Cir. 1993); *U.S. v. Lujan*, 936 F.2d 406 (9th Cir. 1991).] However, the Court of Appeals for the D.C. Circuit has suppressed a wiretap for not including those prior applications that were known to the affiant at the time the affidavit was filed. [*U.S. v. Bellosi*, 501 F.2d 833 (D.C. Cir. 1974).]

Query the agents before filing an affidavit to ensure that they have checked with the ELSUR units as well as their fellow agents, for any prior interceptions of all persons named in the affidavit, not just the principal interceptees. [*Bianco*, 998 F.2d at 1128.]

Period of Interception

Section 2518(5) of Title 18, specifies that once a judge signs a Title III order, the agents have 30 days to conduct the interception, or no "longer than is necessary to achieve the objective of the authorization." At the end of the 30-day period, if the investigation has not been completed and the objectives have not been met, then the interception **must** be terminated. If an extension is sought, the judge must sign the extension order before the expiration of the 30-day period. Any interceptions conducted **after** the 30-day period will not only be suppressed but considered illegal, in violation of 18 U.S.C. § 2511.

The statute provides that the 30-day period begins at the time and date of the first interception (i.e., when the interception device is turned on for the first time), or ten days after the judge signs the order. The 10-day grace period was created for situations where technical

problems and interceptions cannot begin immediately.

The 30-day period should then be computed as thirty 24-hour periods from the date and time of the first interception, or forty 24-hour periods from the date and time the judge signed the order. For example, if the first interception takes place on August 2 at 4:00 p.m., then the wiretap order expires at 4:00 p.m. on September 1.

Section 2518(5) does not clarify whether the 10-day grace period applies to extensions. To avoid scrutiny, measure the 30-day period for extensions from the date and time of the judge's extension order.

Minimization

Before every Title III investigation begins, an AUSA must sit down with all monitors, agents, and contract employees conducting the wiretap to discuss the procedures for minimizing non-criminal conversations. Section 2518(5) states, in part, that "[e]very order and extension thereof shall contain a provision that the interception shall be . . . conducted in such a way as to minimize the interception of communications not otherwise subject to interception." Minimization means that the agents can only listen to criminal conversations, and must turn off interception devices when the subjects engage in non-criminal conversations. In *U.S. v. Scott*, the Supreme Court stated that the determination of whether or not to minimize a conversation should be viewed as "objectively reasonable" based on the circumstances confronted by the monitor at the time of interception. [436 U.S. 128, 140 (1978).]

Agents and monitors must determine what constitutes a criminal conversation before determining whether the conversation needs to be minimized. The AUSA must define the alleged criminal activity for all of the monitors, and describe the statutory violations and give them an indication of what types of conversations will be expected. Especially in white collar cases, it is difficult to distinguish a criminal from a non-criminal conversation. Therefore, AUSAs need to carefully discuss the alleged violations and must feel comfortable that everyone in the wire room understands the need to minimize non-criminal calls.

In addition, the AUSA needs to explain the privileges to the agents and monitors before each wiretap begins. Agents need to know that generally attorney-client, husband-wife, priest-penitent, and doctor-patient conversations should not be intercepted, unless the privilege has been waived or there is evidence that the participants will be discussing ongoing criminal activity. The AUSA needs to be available throughout the interception to address questions as they arise.

Agents should understand the concept of "spot monitoring," whereby they may check non-criminal conversations every few minutes to see if they have

turned criminal. AUSAs should also discuss "after-the-fact minimization" of conversations that are in a code or foreign language where no translator is "reasonably available." [18 U.S.C. 2518(5).] When the translator becomes available, they need to minimize as if monitoring the conversation real-time.

Each United States Attorney's office should have sample minimization instructions that can be used to conduct minimization conferences with the agents and monitors, and each participant must read and sign them. Maintaining close supervision of the Title III interceptions and making sure that the agents understand the law and privileges will ensure that the wiretap will not be suppressed as an "unnecessary intrusion" on the privacy rights of the target subjects. [See *U.S. v. Ozar*, 50 F.3d 1440 (8th Cir. 1995), and *U.S. v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1990).]

Sealing

At the end of every wiretap investigation, the tapes or recordings of the communications must be sealed, as stated in 18 U.S.C. § 2518(8)(a). This includes pager messages, faxed transmissions, and computer records. Sealing involves placing the recorded tapes into evidence envelopes and packages that are brought to the issuing judge by the agent and AUSA. The judge observes the sealing of the boxes and then issues an order stating that the tapes have been sealed. Sealing protects the tapes from tampering and ensures that the interceptions are not disclosed. It must occur "**[i]mmediately** upon the expiration of the period of the order." [18 U.S.C. 2518(8)(a) (emphasis added).] Any delay in bringing the tapes to the judge will result in scrutiny of the AUSA's actions, and may result in the suppression of the wiretap evidence. [See

U.S. v. Ojeda-Rios, 495 U.S. 257 (1990). (The Government must explain why a delay occurred and why the delay was objectively reasonable), and *U.S. v. Feiste*, 961 F.2d 1349 (8th Cir. 1992).]

Excuses such as the termination of the wire over a weekend or the unavailability of a judge will be considered reasonable. [*U.S. v. Pitera*, 5 F.3d 624 (2d Cir. 1993).] Other excuses will require the AUSA to justify reasons for the delay. [*U.S. v. Vastola*, 989 F.2d 1318 (3d Cir. 1993), and *U.S. v. Carson*, 969 F.2d 1480 (3d Cir. 1992).] Seal up the tapes after every 30-day period, even if you are requesting an extension, to avoid having to provide an explanation to the court. ❖

Defending Wiretaps: "Think in the Beginning What the End Will Bring"

Assistant United States Attorney Jeffrey W. Johnson
Deputy Chief, Narcotics Section
Central District of California

As prosecutors, we frequently evaluate wiretaps and oral interceptions on the basis of the number of targets against whom courtroom-quality evidence is gathered and the quantity of contraband seized as a consequence of intercepted conversations. However, there is another important and more accurate barometer of the success of court-authorized interceptions—that is, how the wiretap or oral interception weathers the suppression motions that are inevitably filed when a case is initiated. The primary focus of any prosecutor supervising wiretaps, oral interceptions, or other electronic surveillance should be how each step taken by the investigative team before and during the electronic surveillance will be considered by the district court judge who ultimately decides whether a given interception complied with statutory requirements. Far too often, prosecutors find themselves in the unenviable position of having to explain to a court why an interception should not be suppressed as a consequence of some newly exposed error or omission, when a few precautionary steps before and during the interception would have eliminated the problem.

Moreover, we must not forget the zeal with which defense counsel attack electronic interception. Some criminal defense lawyers have told me that they view wiretaps and interceptions of oral communications as a form of "investigative cheating." In short, they believe that such techniques destroy the "level-playing field" that affords a defendant the opportunity to pit his word against the word of the investigators. Thus, in cases that are built primarily upon court-authorized wiretaps or interception of oral communications, defense lawyers can be counted upon to launch full-scale attacks against every aspect of the interception. Obviously, when defense lawyers succeed in excluding intercepted conversations from trial, in many instances, they have cut off the Government's case at the neck. Frequently, these attacks are of the shotgun variety, intended to uncover any chink—major or minor—in the conduct of the court-authorized interception. Usually, a defendant's attack is double-edged: on one hand, a defendant will allege failure by the Government to establish probable cause within the four corners of the affidavit, as required by 18 U.S.C. § 2518(1)(b), (3)(a) and(3)(b); on the other hand, the defendant will allege that the affiant recklessly or intentionally made material misstatements or omissions. See *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978); *United States v. Tham*, 960 F.2d 1391, 1395-96 (9th Cir. 1992). At other times, these attacks may take the form of surgical attempts to discredit the affidavit supporting the interception application or to claim that the Government misled the authorizing judge with false progress reports; these attacks can be based upon perceived inconsistencies within the affidavit, suspected misstatements, or omissions stemming from the defense's own investigation and/or speculation, as well as defendant affidavits which contradict the Government's account of specific events that underlie the Government's probable cause and/or necessity showings.

In this process, the prosecutor is truly the captain of his own destiny. By enforcing just a few common sense standards, the prosecutor can usually guarantee that the inevitable suppression hearing will end with those wonderful words, "MOTION DENIED."

Probable Cause

In the vast majority of cases, most reasonable judges and prosecutors would agree when there is or is not probable cause that a particular crime is being committed by a particular target over a particular telephone facility; those are the easy cases. However, there are occasions when the existence of probable cause is a "close call"; i.e., when reasonable prosecutors and/or judges might differ over the question of whether there is sufficient probable cause to justify use of a wiretap or bugging device. In light of the statutory and practical requirement that wire or oral interception applications pass muster with the Office of Enforcement Operations and, subsequently, with the Attorney General or one of her statutorily-authorized designees, some prosecutors advocate being as aggressive as the Department will permit in seeking authorization where the probable cause is a "close call." This approach can backfire. As much as we hate to admit it, one judge's probable cause can sometimes be another judge's mere suspicion.

No one knows the judicial preferences and tendencies of Federal judges better than the attorneys who appear before them regularly. Therefore, it is incumbent on prosecutors to exercise their own good judgment **in the first instance** as to whether or not to pursue interception based on "arguable" probable cause. After all, it is those same prosecutors who ultimately will have to defend that interception in a suppression hearing. In larger Federal districts, prosecutors obviously cannot anticipate what judge will be scrutinizing an affidavit in some future suppression hearing. However, even in those districts, institutional experience gives a prosecutor a sense of whether a particular affidavit would face more than a minimal risk of being found inadequate by a significant minority of the bench. In the United States Attorney's office for the Central District of California, we take great care to submit for approval only those interception affidavits that we would be comfortable defending in the courts of our district. In keeping with this philosophy, we are sometimes forced to decline interception affidavits that are likely to be unsatisfactory to at least a significant minority of our Federal bench. This approach minimizes the possibility that time and resources will be wasted gathering evidence that we can not use—at least not until after an appeal.[*]

[*] If an interception were suppressed, the district court's conclusion would be subject to de novo review; however, any factual determinations that the district court made in conjunction with the suppression would be subject to a clear error review. *United States v. Hill*, 953 F.2d 452, 456 (9th Cir. 1991).

Dotting the i's and Crossing the t's

All prosecutors should be from Missouri.[**] With electronic surveillance, and all other aspects of our work for that matter, we should personally verify all facts in a wiretap affidavit that can be verified.[***] An investigative agent will not be offended when we ask to see copies of the pen register or trap and trace data, or toll records which constitute part of the probable cause for an application. This personal review not only affords the prosecutor an opportunity to verify the accuracy of such information in the affidavit, it also gives him or her an opportunity to identify other information that might be pertinent immediately or at some future point in an investigation. Likewise, the prosecutor should review any and all surveillance and interview reports that are connected to events described in an affidavit.[†] Such review not only enables a prosecutor to confirm the accuracy of accounts set forth in the affidavit, it also permits the prosecutor to identify any information that a defense lawyer may later claim was improperly misstated or omitted from the affidavit. Armed with such information, the prosecutor stands a much better chance of diffusing potential bases of suppression.

Clarifying Necessity Issues in Camera

In the context of interception applications, prosecutors often face the problem of how much information should be disclosed to the issuing judge in order to comply with the statutory requirement that we provide a "full and complete statement as to whether or not other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." Most often, this problem occurs where the investigative agency is seeking to protect the identity of an informant for security reasons. Frequently, it is necessary to give the issuing judge a little more detail to avoid defense claims that the judge was misled by the circumspect way in which certain facts or events were described in the application affidavit. An

[**] Missouri is the "Show Me" state.

[***] The prosecutor should be aware of, and the Government should disclose to the authorizing judge **all** investigative techniques that have been, are being, or will be used.

[†] Naturally, this approach has limitations. Occasionally, such reports are not even generated until some time after an interception affidavit has been submitted. And, of course, some events are never documented in a report.

alternative that should be considered in such instances is the filing of a supplemental in camera affidavit, concurrent with the interception application, which elaborates on necessity-related details that the Government might hope to avoid disseminating when the interception is disclosed to the defendants. Such affidavits should contain express language that the Government is providing the information only to clarify a necessity issue, and not for consideration by the issuing judge in determining whether or not there is probable cause or necessity for the contemplated interception. See *United States v. Falls*, 34 F.3d 674, 682 (8th Cir. 1994), wherein the court of appeals emphasized that the Government should use sworn testimony before the issuing judge to disclose fully "the fact of and the reason for masking the [confidential] witness's identity in [an] affidavit" seeking silent video surveillance authorization. Cf . *United States v. Danovaro*, 877 F.2d 583, 587-88 (7th Cir. 1989) (Government may redact information released under 18 U.S.C. § 2518(9) if both dangerous to informants and unnecessary to sustain order).

While trial judges sometimes order disclosure of supplemental affidavits over Government objection, the mechanism at least gives the Government a fighting chance. Additionally, the separate filing approach gives the Government the opportunity to highlight the information that is pertinent to the issuing judge's decision to authorize the interception, and the portion that was not. At the same time, at a suppression hearing, such filings can bolster the Government's contention that it did not mislead the issuing judge as to the information contained in the supplemental affidavit.††

Conclusion

Good defense lawyers will always find ways to attack the Government's interception affidavits. Therefore, suppression hearings will remain a regular part of the electronic interception process. At least if we follow the simple guidelines discussed above, suppression hearings will rarely result in premature termination of our prosecutions. ❖

_____

†† Of course, if security considerations change at some point after the interception, the Government can then seek court authorization to disclose the supplemental affidavit as well.

Wiretaps: A DEA Agent's Perspective Interview with Special Agent Mark Styron

Since 1987, Special Agent Mark Styron has worked for the Drug Enforcement Administration (DEA).

He is currently assigned to DEA's office in Dallas, Texas, as acting Group II Supervisor. Prior to going to work for DEA, Mark Styron served as a Dallas Police Officer. He has an extensive background in the use of wiretaps in drug investigations. He has participated in numerous foreign language wiretaps, as well as wiretaps involving multi-drug and multi-jurisdictional trafficking. Agent Styron serves alongside agents from Miami, Los Angeles, and New York, as an instructor for DEA's in-house training program on the administration and use of wiretaps. Agent Styron also provides instruction to DEA personnel on the identification of cellular phones and pagers being used by drug traffickers; how to use "trigger-fish" technology; how to use pen registers and trap and traces; and how to organize this information for use in a wiretap affidavit and/or at trial.

Agent Mark Styron (MS) was interviewed by Assistant United States Attorney Jennifer E. Bolen (JB), Northern District of Texas, Dallas Division. AUSAs St. Clair Theodore and Rose Romero, Northern District of Texas, assisted with this article.

JB: What is DEA's current policy regarding the use of wiretaps in drug investigations?

MS: DEA has recently taken a more aggressive stance on the use of wiretaps in its drug investigations. One of the reasons for this is that wiretaps have proven to be an effective tool in dismantling entire drug organizations. A wiretap can expose the entire conspiracy— across city limits, state lines, and even the country. Also, DEA has recently relaxed its funding restrictions so that case agents are more likely to commit to a wiretap in an investigation that merits the use of the same. In the past, DEA relied on other agencies for monitors and support personnel to run wiretaps. Now, DEA has obtained more technical equipment to outfit in-house wire rooms. DEA also uses these budget funds to pay for contract monitors and transcription services. This change in position has increased the effectiveness of DEA wiretap operations.

JB: Obviously, a wiretap is an expensive investigative tool, both in terms of equipment and personnel. What type of budget considerations do you as a case agent have to consider when seeking to use a wiretap during a drug investigation?

MS: The agency has to consider the cost of leasing the lines to implement the wire; monitor services (including overtime amounts); transcription services; and supplies such as tapes, monitoring equipment, etc.

JB: Within DEA, what steps does an agent have to take to use a wiretap in an investigation?

MS: The first thing a case agent must do is determine whether the investigation merits a wiretap. This step necessarily involves a detailed analysis of the targets of the investigation; the evidence gathered to date; and a determination as to whether the goals of the agency can be met without a wire; in other words, whether there can be a successful and complete prosecution of the drug organization based on all evidence short of a wiretap. Because one of DEA's major goals is to identify and prosecute large-scale drug importers and major distribution organizations, traditional law enforcement techniques are usually not sufficient to do this and a wiretap becomes an automatic consideration. However, the agent must be able to articulate to his or her boss precisely the reasons a particular investigation merits a wiretap. Second, the agent must determine where the money will come from to actually administer the wiretap. Wiretaps are personnel intensive, requiring the complete dedication of numerous individuals to perform a variety of tasks. The agent must be able to tell his or her boss the expected time frame for the wire (how long it will run) and the number and type of telephone lines to be targeted (single or multiple, ground or cellular), and to provide an estimate of the number of people needed and their proposed schedules in order to work the wire (including monitors, translators, transcribers). Often it is difficult to provide this information with any certainty because the evidence gathered during a large-scale investigation usually results in "spin-off" investigations which may also merit wiretaps. Obviously, these factors make it difficult to accurately estimate the time frame and extent of a wiretap.

JB: Where does DEA get its money to finance a wiretap?

MS: Funding might come through the DEA case agent's Divisional Office or through DEA Headquarters, depending on the cost of the wire and the magnitude of the targeted organization. The larger the investigation, the more likely funding will come from DEA Headquarters. Alternatively, funding for a wire might be tied into another investigation; i.e., the wiretap is the result of a "spin-off" from a case that already has wiretap funding. So, for example, if Los Angeles is conducting a wiretap on an organization and has intercepted calls that reveal that the organization has ties to Dallas, then, based on these intercepted calls, DEA-Dallas would initiate a wiretap on the local telephone lines. Again, the purpose of the "spin-off" or extended wiretap would be to dismantle the entire drug trafficking organization.

JB: What other issues arise when an agent is considering the use of a wiretap in an investigation?

MS: The agent must continuously evaluate the evidence gathered during the investigation and attempt to identify the most important telephone(s) to be targeted for wiretap consideration. Sometimes this issue and those we have already discussed are affected by the number of other wiretaps going on in a particular Division. Consequently, the question becomes: Can the investigative group handle the burden of yet another wire—both physically and financially? Finally, the agent must consider what impact, if any, the use of a wiretap might have on the investigation. In other words: Will the wiretap result in fewer or more seizures of narcotics? Will the investigation be compromised as a consequence of having to use more surveillance teams to back up the conversations on the wire or to follow a shipment of drugs? Can the wiretap be effectively completed if there are time or budget constraints? Will other offices conduct "spin-off" investigations if sources of supply or distribution cells are identified within their jurisdiction? Basically, questions of this nature are considered by the case agent for the purpose of evaluating the benefits and cost of using a wiretap.

JB: In summary, give us your best laundry list of a case agent's responsibilities in securing and administering a wiretap.

MS: A case agent has the ultimate responsibility for an investigation "numbered" under his or her name. When an investigation merits the use of a wiretap, the case

agent has, *at a minimum*, the following responsibilities: (1) prepares the wiretap affidavit; (2) coordinates with state and local law enforcement agencies regarding investigative intelligence and support resources; (3) coordinates and schedules surveillance; (4) coordinates and schedules monitors, translators (if necessary), and transcribers; (5) makes recommendations regarding overtime funding (number of people and amount of overtime); (6) makes decisions regarding the use of contract monitors (how many and where from); (7) obtains supplies for wire room (tapes, pen register equipment, wiretap equipment, call logs, etc.); (8) coordinates and schedules undercover transactions and/or use of informants, which may or may not be tied to activity on the wire; (9) coordinates decisions regarding the use and timing of search warrants during the wiretap process; (10) prepares 10-day reports; (11) reviews pertinent telephone calls and transcripts for accuracy (or reviews the same with the translator); (12) updates the AUSA regularly about the wire and the ongoing investigation; (13) prepares agency reports tracking the progress of the investigation; (14) secures pen registers/trap and traces for new telephones identified during the investigation; (15) secures pager intercept orders; (16) administers activities relating to the use of informants and document meetings and debriefings; (17) serves as overseer of all wire room activities, and often sits on the wire for a shift; (18) communicates intelligence gathered during the wiretap and related investigation to other DEA Divisions; (19) prepares criminal complaint affidavits if merited during the investigation; (20) debriefs individuals arrested during the investigation; and (21) whatever else needs to be done.

JB: Have you developed a checklist that you and your fellow agents use during the administration of a wiretap case?

MS: Yes. DEA-Dallas uses a basic checklist that can be modified and adapted as a particular case demands. The checklist is basically a time-line or chronology of the administrative and legal aspects of the investigation, and consists of several lists within itself. For example, one purpose of the checklist is to record the dates that pen registers, trap and traces, pager intercepts, and wiretaps are initiated or extended, and to record the minimization meeting and the due dates for 10-day reports. Another purpose of the list is to keep track of the supplies necessary to conduct the wire. Similarly, the checklist is used to keep track of the necessary OCDETF paperwork and teletypes to DEA Headquarters regarding funding of the investigation and identification of the investigative goals. The checklist is also used to establish and maintain monitor schedules, the supervising agent's schedules, and surveillance schedules. There is no magic to the content of a checklist; my only comment is that a case agent should definitely use one.

JB: Obviously the role of a case agent during a wiretap operation is extensive and very important. What are your thoughts on the role of an Assistant United States Attorney in a case involving a wiretap?

MS: Overall, the role of an AUSA depends on the nature of the case—its size, expected number of defendants, time frame, reactive status (meaning whether it will involve few or many criminal complaints, search warrants, pen registers, trap and traces, tracker applications, trigger-fish operation, pager intercepts, etc.). It has been my experience that AUSAs are typically very involved in the large-scale drug investigations, whether a wiretap is used or not. When a case merits a wiretap, the agent usually spends a great deal of time advising the AUSA of the investigative history. This process usually results in the preparation and review of a wiretap affidavit. The agent prepares the affidavit, and the AUSA reviews it. As an agent with all of the above-described responsibilities, I expect the AUSA to review the wiretap affidavit in a "timely" manner. The timeliness of an AUSA's review is critical because much of the information contained in a wiretap affidavit relates to dated events; e.g., we often use confidential informant information, controlled purchase transactions, or consensually monitored telephone calls to establish probable cause for a target telephone. When the wiretap affidavit documents "hot calls" to a target telephone, the clock starts running. If an AUSA sits on a wiretap affidavit for too long, the subjects of the investigation may not even be using the same telephone by the time the wiretap is approved.

JB: Is it fair to say that timing is critical in wiretap cases, and that more than just the authorization to listen depends on the AUSA's timeliness?

MS: Absolutely. Not only is the agent concerned about getting authorization to listen on the right telephones, but he or she is also concerned with the coordination of the schedules of dozens of other people. It becomes a logistical nightmare to reschedule all of the monitors, translators, transcribers, surveillance teams, etc., when a delay occurs in a wiretap investigation. Oftentimes, we are not able to simply call on other resources to fill the holes for scheduling conflicts that arise as a consequence of a delay. Therefore, we depend on the AUSA for his or her timely and involved participation in the wiretap process.

JB: With regard to the wiretap affidavit specifically, what's your perception of the steps an AUSA should take to finalize it and send it to Washington, D.C.?

MS: That's a tough question, and the answer depends on the experience of the agent and AUSA involved. In my experience, I have seen agents submit wiretap affidavits that require a great deal of "editing" in order to make them presentable to the people in Washington who provide Department of Justice authorization to seek a wiretap order from a judge. I have also seen AUSAs completely re-write a wiretap affidavit because of a style conflict with that of the agent's. Obviously, the AUSAs have the legal training and background to make judgments necessary to protect the Government's representatives and case throughout the criminal process. However, I strongly urge AUSAs to "edit" wiretap affidavits with an eye toward preserving the agent's "verbiage." In other words, the affidavit should not become the words of the AUSA. I feel strongly about this because, as an agent, I know it is much easier to defend my own words in court rather than someone else's.

JB: What other expectations do you have of an AUSA in a wiretap case?

MS: I think it's fair to expect the AUSA responsible for the wiretap to keep track of what's going on—on a daily basis. Before going up on a wire, the agent and the AUSA should discuss what is expected of each other and reach an agreement as to the "who, what, where, when, and how's" of keeping each other up-to-date on the daily events during the wire. For example, the agent and the AUSA should come up with a procedure to ensure that the AUSA receives the wire logs and transcripts. There must also be a meeting of the minds on the issue of what calls should be transcribed and when in relation to the event of the call. If these matters are not discussed prior to the interception of the first call, misunderstanding and miscommunication are inevitable.

JB: What recommendations would you make regarding communication and organization to agents and AUSAs who have not yet handled a wiretap case?

MS: I think that communication, organization, and flexibility (in that order) are the keys to a successful wiretap—regardless of the experience of the agent or AUSA. For first-timers, I would suggest the use of a check list and regular meetings between the AUSA and the investigative team.

JB: What technical things can go wrong with a wiretap?

MS: Perhaps the most common technical problem related to a wiretap is that the tapes do not properly record a conversation. Other technical problems include: (1) poor quality of a target line, (2) failure to conduct a test call and then monitoring the wrong telephone (big problem), (3) tape duplicating machine "eats" the original duplicate tape, and (4) power outages which interfere with the ability to monitor the target lines.

JB: What guidance do you expect from an AUSA regarding the right way to handle the correction and documentation of technical problems?

MS: When a technical problem occurs with the wiretap, it is imperative that the AUSA provide the agent with immediate and timely guidance. Of course, this means that the agent has the responsibility of immediately notifying the AUSA of the problem. Sometimes problems arise because of the telephone company's refusal to cooperate. If this is the case, the AUSA should be prepared to pursue the telephone company's refusal to comply with the court's order.

JB: How can an AUSA be most helpful to agents in understanding the importance and necessity of minimization of actual telephone call intercepts?

MS: The AUSA should provide monitoring agents and personnel with a comprehensive minimization memo. In addition, the AUSA should attempt to give real examples of calls that should be minimized during the minimization meeting. If an AUSA has never "minimized" a wiretap team, then he or she might consider asking a more experienced AUSA for a "go-by" memo and may ask that person to actively participate in the meeting by giving specific examples of the minimization requirements.

JB: How can an AUSA be helpful regarding the transcription of wiretap calls?

MS: Let me answer that question by stating the obvious: the transcripts of wiretap calls are important throughout the investigation and prosecution of a case. I believe it is imperative for the AUSA and the agent to reach an agreement as to which calls need to be transcribed immediately and which calls can wait. Likewise, I believe that the AUSA should make it his or her practice to conduct a daily review of the "pertinent call" log so that he or she can advise the agent as to whether there is a need to transcribe fewer or more calls as the wiretap progresses. Many schedules and resources depend on this decision. Once the agent and the AUSA reach an agreement on the issue of transcription, it is the agent's responsibility to accurately communicate the agreement to his or her investigative team, and to ensure that it is

carried out. Finally, I believe it is imperative for the AUSA and the agent to reach an agreement as to the format or physical layout of the call transcripts. Such an agreement will save time in the long run and allow for a more concentrated study on the accuracy of the transcription's substance (the content of the call itself). This agreement will also minimize the chances of having to redo all exhibited wiretap transcripts during the week or two before trial.

JB: In your opinion, what is the most important thing an AUSA can do during the trial of a wiretap case?

MS: Perhaps the most important thing an AUSA can do during the trial of a wiretap case is to put on testimony of an agent at the beginning of a trial to explain to the jury what a wiretap is and how it is conducted; i.e., the procedures the Government must (and did) follow to get authorization to listen to somebody's conversations. Through this testimony, the AUSA/agent can familiarize the jury with wiretap "jargon" and the concept of "coded language." Most importantly, this type of testimony helps jurors understand the rigorous process of a wiretap; helps minimize a jury's concern that someone's privacy has been invaded; and shows that the Government really does have to account for its actions and actually goes a long way to protect the rights of citizens. ❖

Electronic Surveillance: Does it Bug You?

Assistant United States Attorney Melissa J. Annis
Southern District of Texas

Who would have thought that after completing at least seven years of higher education, practicing law for a few years (perhaps in a high paying yet less than fulfilling position in private practice), that you would one day spend endless (and perhaps painful) hours applying for, listening to, and defending a BUG?!?!? Now it might not be a long-antennaed, hairy, multi-legged kind of bug but it is a bug all the same. That's right, you now engage, albeit vicariously from the safety of your Government office, in the kind of activity that you read about in spy novels and watch on "movies of the week." The evidence that you gather off of your "bug" can be just as fascinating as that depicted in fiction, but what they failed to warn you of are the frustration and problems that often come with the absolutist nature and requirements of dotting your "i's" and crossing your "t's" in complying with the statutes.

When you venture into the world of electronic surveillance, there are many, many questions you have to ask and some you don't even know you should ask. I generally turn to the Office of Enforcement Operations' Electronic Surveillance Unit, a.k.a. OEO, for the answers to my questions. OEO has a "how to" manual (which also clears up how **not** to), with answers to the questions most commonly asked by Assistant United States Attorneys (AUSAs). Since OEO is the expert on this topic, the following is an attempt to point out perhaps the elementary but practical application of these statutes and issues for which AUSAs should prepare.

What is "Title III?"

Although wire, oral, and electronic interceptions are generally referred to as "Title IIIs" you will not find what you are looking for under Title 3 of the United States Code. Strangely enough, we do not refer to the wire and electronic surveillance statute by the title or chapter where this law is actually found in your code book (see Title 18, U.S.C. §§ 2510-2522) but, rather, by the Title number in the legislation creating this statute; i.e., Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Title III provides law enforcement with the ability to execute what really constitutes a "super search warrant." It is not an ordinary search warrant because it

allows the search to be conducted over a particular instrument, no matter where that instrument may be in the United States (and even outside the jurisdiction of the court), and the search is allowed to span a 30-day period with the approval of the court.

Communication

Just exactly what **is** a wire, oral, or electronic (one in which the human voice is not used) communication covered by this chapter? Certainly, it must be a communication that is surrounded by a legitimate expectation of privacy, one that is intercepted by law enforcement or someone otherwise not excluded by Title III scrutiny (like the service provider acting in the normal course of business, or a switchboard operator) , and the interception is not consented to by at least one party to the communication.

The word "interception" is defined in § 2510(4) as the acquisition of the contents of any wire, oral, or electronic communication "through the use of any electronic, mechanical, or other device." What about a device used simply to enhance the ear's natural ability to hear; is that considered an intercept covered by Title III? How about a glass used to listen through the wall, or a hearing aid? As long as the device, like a hearing aid, is used to correct subnormal hearing and not to increase hearing to better than normal, it is exempt from this statute [§ 2510(5)(b)].

Search Warrants v. Interception Orders

Like the search warrants we most frequently litigate under Rule 41, Federal Rules of Criminal Procedure, you must have intercept applications approved by a judge of "competent jurisdiction"; i.e., a judge of a United States district court, United States court of appeals, or an authorized state judge. For Rule 41 search warrants, you must have the approval of a Federal magistrate judge or a state judge in a court of record. An application for either of these searches must be based on probable cause as alleged in the affidavit (which may be based on hearsay evidence), and the affiant for either type of affidavit can be subject to a *Franks v. Delaware*, 438 U.S. 154 (1978), challenge. The warrant or order for these searches must identify specifically the place to be searched. Each warrant or order authorizes the seizure of **only** those specific items or communications approved by the court; however, the plain view or plain hearing doctrine applies to both types of searches. Whether a communications order interception or a search warrant, the issuing judge must be notified of what was intercepted or found. The wire/electronic intercept statutes and Rule 41 both require an inventory notifying the party(s) intercepted or whose premises were searched, of the interception or search. (Note that this notice may be postponed in certain instances—more on that later.) The last common denominator is that each of these searches is subject to a variety of statutory and common law challenges in a motion to suppress.

Despite all the similarities between Rule 41 searches and court authorized interceptions, there are some significant differences. One of the more significant differences between the statutes is jurisdictional. Under Rule 41, a judge within the district must issue the warrant to search property within the district. A Federal judge, however, has jurisdiction to issue an order authorizing the interception of wire, oral, and electronic communications within the jurisdiction where the interception will take place. This means that a telephone located in one district could be intercepted in another district with the permission of the court where the interception will take place. Even a cellular telephone physically located in another country may be intercepted lawfully in the United States as long as that cellular telephone is using a cell site in the United States. For example, a judge in the Southern District of Texas may authorize the interception of a cellular telephone physically located just across the border in Matamoros, Mexico, if that telephone is using a cell site on the United States side of the border in the Southern District of Texas where the interception will take place.

Congress has outlined very strenuous requirements for the lawful application, interception, and use of electronic surveillance, given the nature of the intrusion in wire, oral, and electronic interceptions. For example, applications to intercept communications under Title III must be authorized by the Attorney General, Associate Attorney General, Deputy Attorney General, Assistant Attorney General, or a Deputy Assistant Attorney General in the Criminal Division of the Department of Justice [§ 2516(1)]. Without the proper authorizations, the evidence will be suppressed.

The Application

Search warrants require some specificity, but Title III requires that an application to intercept communications include:

(1) the identity of the investigative or law enforcement officer submitting the application and the officer authorizing the application [§ 2518(1)(a)];

(2) a full and complete statement of the facts relied upon to conclude there is probable cause [§ 2518(1)(d)];

(3) details as to the alleged offenses [§ 2518(1)(b)];

(4) details as to the nature and location of the facilities from which or where the communications are to be intercepted [§ 2518(1)(b)];

(5) a particular description of the type of communications to be intercepted [§ 2518(1)(b)];

(6) the identity of the persons (if known) committing the offense(s) and the persons whose communications are to be intercepted ("named interceptees") [§ 2518(1)(b)];

(7) a full and complete statement of whether other investigative procedures have been tried and failed, or why they appear unlikely to succeed or are too dangerous to employ [§ 2518(1)(c)];

(8) a statement of the period of time for which the interception is to be conducted, not to exceed 30 days and terminating earlier if the objectives of the investigation are accomplished. [§ 2518(1)(d)]; and

(9) a statement of prior applications to intercept the same person, place, or facility, including the action taken by the court for each application [§ 2518(1)(e)].

If an application for extension is necessary to continue to monitor the communications of your named interceptees for an additional 30 days, the application must also include the interception results thus far and an explanation of the reasons why the desired results have not been achieved [§ 2518(1)(f)].

Probable Cause

The probable cause standard used in ordinary search warrants is the same standard used in applications for interception. There are three separate probable cause findings in an interception application: (1) probable cause to believe that persons have committed, are committing, or are about to commit one of the crimes enumerated in § 2516; (2) probable cause to believe that particular communications concerning such offenses will be obtained through interception; and (3) probable cause to believe that the facility from which the communications are to be intercepted has been, is being, or is about to be used in connection with the commission of those offenses (except, of course, in the circumstance of a roving interception, which applies to the named individual, not just a particular facility or premises). Once the concept of three layers of probable cause is understood, it makes outlining the probable cause in the affidavit much easier.

Probable cause can be developed in part through pen registers, traps and traces, caller ID, toll and billing records, and through the assistance of informants, undercover agents, and cooperating defendants. A pen register and/or trap and trace section is an important part of the affidavit that develops probable cause. Once subscriber information provides names for the numbers being called by—or calling into—the target phone, such informants assist in identifying individuals who may be intercepted over the subject telephone, and it is an easy way to "freshen" the probable cause. This can also be accomplished through billing records or a "daily dump" from the cellular company. Installing and using a pen register and a trap and trace device requires a court order, although the requirements of Title III do not apply. Billing records and toll records can be obtained through the agency's administrative subpoena power. The only drawback to this type of record is the time lag between the request and the time the company actually provides the records. Toll and billing records can, however, certainly provide a historical call analysis for the period prior to the installation of the pen register and/or trap and trace which, in turn, can aid in building your probable cause foundation.

Necessity

Not only must the court find probable cause but there must be a finding to execute this super search warrant since the other investigative techniques **must** have proven to be unsuccessful or appear unlikely to succeed, or are just too dangerous. Clearly, every conceivable investigative technique need not be exhausted before the necessity requirement is met. However, the necessity requirement seems to be one of the areas of concentrated effort in the defense bar's attempts to suppress the results of super search warrants. Sometimes, the affidavit writer spends too little time writing the affidavit and uses boilerplate language that does not explain exactly why the affidavit is necessary and why surveillance, pens, search warrants, toll records, etc., have not and will not work. In some instances, relying on exhaustion of some investigative techniques may not be sufficient if the agents have, to that point, identified only one or two named interceptees with whom a reliable, confidential informant has made consensual recordings of a criminal nature, and the informant can make a prosecutable case without the interceptions. If

there is no basis in the affidavit for the court to find that additional violators (co-conspirators) will be identified and evidence of their guilt will be established, at least in part, through interceptions, the court may conclude that this intrusive investigative technique is (or was) not necessary, leading to denial (or later suppression) of the application/interception.

Post-authorization Duties—Role of the AUSA

The prosecutor plays a central role in the application process. Reviewing the affidavit and applying for the intercept order puts AUSAs in the middle of the process. Perhaps the most significant role prosecutors play with regard to the interception of wire, oral, and electronic communications is handling post-authorization duties. While many of these duties are shared with the agents, the prosecutor is responsible for ensuring that they are conducted timely and correctly.

Minimization

Minimization is an issue that the defense has used historically as a major challenge to the manner in which the court's order was executed. Prosecutors should play a very active role in determining conversations that should be recorded and minimized, by giving agents and monitors very explicit instructions regarding what they can and cannot listen to, and by always being available during the intercepts.

During the minimization conference with the agents and monitors, the AUSA should review the various privileges that might be at issue if certain conversations are intercepted and the crimes listed in the order as authorized offenses to intercept. It is very important to ensure that each monitor and supervising agent in the monitoring room read the application, affidavit, and order to become familiar with the authorized offenses and other minimization instructions in the order. The prosecutor should advise the monitors that any criminal communication may be intercepted even if it is not one of the offenses listed in the order—since a "plain hearing" doctrine has developed through case law. [See also U.S.C. § 2517(5).]

It is also helpful to the monitors to describe code words that might be used during the criminal conversations. Agents generally are aware of potential code words that may be used by a particular group of targets from informant or undercover officer information. This becomes increasingly important during the interception. At the beginning of the overhears, the monitors can listen to more of the conversation than they can later in the 30-day period. This is appropriate because the monitors need more leeway at the beginning of the intercept to determine if the conversation is criminal in nature. Remember to include in your applications and orders, a provision to allow the monitors to "spot check" the conversation to ensure that an earlier nonpertinent (i.e., non-criminal) conversation has not turned to criminal matters.

Progress Reports

The issuing judge may order that the court be provided progress reports from the AUSA during the period of interception [§ 2518(6)]. These reports usually are submitted every 10 days to inform the court of the progress made toward achieving the authorized goals and of the need for continued interception. The AUSA should take this opportunity to inform the court of newly-identified targets and the interception of communications relative to other crimes not specified in the order. These reports also may include unusual or arguably sensitive conversations and events; for example, conversations presumed to be privileged. Keeping the issuing judge informed of the progress of the interception and the content of pertinent communications in the "10-day reports" may prove helpful in defeating the defense's minimization arguments.

Sealing

To protect confidentiality and prevent tampering, § 2518(8)(a) mandates that wire, oral, or electronic communication be recorded, if possible, so the recording is protected from editing or alteration. This subsection also mandates that "immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions."

Sealing is a simple procedure but can result in fatal evidentiary problems for the prosecutor. The recordings must be sealed or the prosecutor must provide an explanation for not sealing before the use or disclosure of intercepted communications or even evidence derived from such communication. So, not only does the AUSA have to explain why the recordings were not sealed or why there was a delay in sealing, but the court will have to be convinced that it was excusable. Although § 2518(8)(a) allows for sealing after the conclusion of all extensions, OEO recommends that recordings be sealed at the conclusion of each 30-day period of interception, pointing out that "the definition of an extension order is construed very narrowly." This is a

very important point and good advice. If recordings are sealed after every period of interception, the inevitable problems that occur immediately after an interception do not threaten the previous 30-day periods. Thus, subsequent defense assertions and claims—or court findings—of a taint can be effectively contained and eliminated.

For example, § 2518(8)(a) requires that sealing be done at the direction of the issuing judge, and take place immediately upon expiration of the period of interception. Now in the real world, the issuing judge is not always available immediately upon expiration of the order. Likewise, agents are not always available at that juncture, as they are often busy executing search warrants; arresting defendants; or testifying at the detention hearings of the defendants intercepted. Each day that passes before the recordings are sealed gives a little more credence to the motion to suppress for failure to seal or seal timely. In short, you are building problems into your own case. Clearly this is a practice to be avoided at all costs—there are enough **un**avoidable ones lurking out there.

The statute also requires that the recordings be maintained for at least 10 years in the custody of whomever is directed by the issuing judge, usually the agency responsible for the interceptions. Occasionally the prosecutor is faced with solving the problem of a court-ordered, sealed box of wire tapes that has been opened by an unsuspecting agent who may have been looking for something else. To avoid this, the best practice is to have the agents place a copy of the order on the outside of the box so, years from now, everyone knows that the box is under seal. As for the accidental unsealing of the box, one course of action would be to explain the circumstances to the judge, making a record that the tapes were not altered or changed and that all tapes are present and accounted for, and request that the court reseal the tapes.

"Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge." [§ 2518(8)(c).]

Inventory

An inventory disclosing: (1) the fact of the entry of an order or application; (2) the date of the entry and the authorization period approved or disapproved, or the denial of the application; and (3) the fact that during that period communications were or were not intercepted, must be served on the parties named in the order and other parties to intercepted communications as the issuing or denying judge requires [§ 2518(8)(d)]. This inventory must be completed no later than 90 days after the end of the last extension. If the AUSA makes a showing of good cause (i.e., the investigation is continuing), the inventory may be postponed. Any portion of the intercepted communications, applications, and orders that the court determines is in the interest of justice be made available upon motion, to a person who has received an inventory.

However, it is not necessary to give an inventory to each and every person intercepted during the period of interception, if the court agrees. Generally, if individuals have never been fully identified, or certain people were intercepted in noncriminal conversations (e.g., the Pizza Hut delivery man) and were not otherwise listed as a named interceptee, prosecutors should request from the court that inventories not be served on those persons.

Disclosure and Use of Intercepted Communications

Title 18, U.S.C. § 2517(1)-(5) outlines the "cans" and "cannots" concerning disclosures of the contents of intercepted communications without a court order. When in doubt, get a court order for the disclosure, as it is obviously the safest course [§ 2518(8)(b)]. Wire and electronic communications can be damaging and powerful evidence at trial but if the mandates of Title III are not followed carefully, you may be in a great deal of trouble. Title 18, U.S.C., § 2520 provides for the recovery of civil damages for unauthorized disclosure or intentional use of wire, oral, or electronic communications.

Ultimately, the court must give prior approval to using the contents of or evidence derived from intercepted communications when it relates to offenses other than those specified in the interception order. Be very cautious on how agents handle or follow up on "other crimes" interceptions. Also, at least 10 days prior to a trial, hearing, or other proceeding in a Federal or state court, each party must be given a copy of the application and order for interception before the contents of the intercepted communications or evidence derived from the interception can be received in evidence or otherwise disclosed [§ 2518(9)]. This requirement can be waived if the judge finds this is not possible and the parties are not prejudiced by the delay. Therefore, the 10-day requirement may be waived at a detention hearing at which the Government wants to offer the contents of intercepted communications or evidence derived from them.

"Murphy's Law"

One of the laws that applies to virtually every interception case is "Murphy's Law." What can go wrong, does. Whether the target is literally throwing the

subject cellular telephones in the bayou every few days and getting new ones, or there is the probability of an attorney-client privileged interception, something **always** happens to challenge your patience and knowledge of Title III.

For example, have you ever had an electronic bug installed next to a dishwasher that is in use constantly? Or how about the AUSA who was returning a call from the agent conducting a wire interception and accidentally called the target telephone rather than the agent and was intercepted by the monitors? In that instance, you have to hope the target didn't have caller ID. You also need to ask yourself, do you have to give the AUSA an inventory? Have you ever had a pole camera that was incorrectly wired into the target's cable so every time he flipped through the television channels he saw the picture of his own front door? After several trips to view his front door and back to check out the television, the target figured out he had a problem. What about the minimization dilemma when the target falls asleep while dialing the subject telephone and all that is being recorded are snores? After all, the telephone **is** "off the hook or otherwise in use," but do zzzzzzz's really fall within the ambit of the order?

Multi-Jurisdiction Interceptions

In recent years, law enforcement has discovered the value of multi-jurisdictional electronic surveillance. Now, related and common interceptions are occurring simultaneously in districts across the United States. This trend has evolved to thwart the practices of large-scale drug trafficking organizations that operate in multiple cities throughout the United States and communicate primarily through the use of cellular telephones and pagers. As a trafficker moves from city to city using his cellular telephone's roam feature, AUSAs are able to intercept in any jurisdiction, and agents are able to identify individuals with whom the trafficker engages in a criminal conspiracy. As a result, "spin-off" Title IIIs are generated with the cooperation of AUSAs and agents in the visited districts.

This technique requires that United States Attorneys' offices and Federal agents across the country work in unison, sharing information and coordinating their efforts. It is extremely important that AUSAs not only coordinate wire intercepts and related seizures, but indictments and arrests as well. In multi-jurisdiction interceptions, agents and AUSAs are not free to make unilateral decisions impacting other jurisdictions. Court-ordered disclosure of one application and order for interception pursuant to the mandates of § 2518(8)(b) and (9), and Rule 16, Federal Rules of Criminal Procedure, in one district will risk disclosure of the wire and electronic surveillance in other districts because of the prior application section in the affidavit and the large amount of information shared with the judge in the affidavit in establishing probable cause.

Multi-jurisdiction wire and electronic surveillance is a powerful tool against the cartels and one that ought to be used where feasible. It is also a tool that cannot succeed without the coordination and cooperation of all AUSAs involved.

Litigation of Intercepted Communications

Grand Jury

Even at the grand jury stage, the prosecutor may receive challenges to the Title III interception. A grand jury witness can claim a violation of Title III as a defense to contempt charges brought as a result of the witness' refusal to answer questions. Once a preliminary showing has been made by the witness that the questions for the witness were based on information obtained through illegal intercepts, the Government must overcome the allegation. Depending on the circuit, you might have to turn over the application and order to the grand jury witness at a hearing on the legality of the Title III. Obviously, the Government should argue for an *in camera* review by the court because of the potential of prejudice in turning over to the witness the application, affidavit, and order.

Suppression

Suppression is a battle that should be fought from the inception of the interception authorization process, and can only be avoided by the preparation of and continuous attention to the logistical and technical operations of the wire.

The prosecutor can expect to fight both pretrial and at trial over the admissibility of intercepted communications and the evidence derived from the interception. Mistakes made regarding the interceptions will be pointed out and blown out of proportion, and mistakes will suddenly take on the mantle of a major constitutional violation as a result of bad faith.

Any "aggrieved person" can move to suppress illegally intercepted communications or evidence derived from it. The interception can be challenged on several grounds: (1) the communication was unlawfully intercepted, (2) the order of authorization or approval was insufficient on its face, or (3) the interception was not conducted in conformity with the order

[§ 2518(10)(a)]. Another basis for suppression is improper sealing [§ 2518(8)(a)]. As discussed in this article, popular suppression issues include minimization, necessity, and exculpatory or omitted material facts.

A growing suppression issue is the claim that the Government has failed to include exculpatory or omitted material evidence in the affidavit supporting the wiretap application. This issue has been used to challenge the necessity for interception when, according to the defense, the court has not been completely apprised of all the "normal investigative techniques" that have not been employed prior to applying for the authorization to intercept. This is often spun as a desire on the part of the Government to "recklessly mislead" the court, and then the defense requests *Franks v. Delaware* hearings. If counsel can twist or turn certain statements or even omissions in the affidavit into a *Franks v. Delaware* argument, they often will. An opportunity to get a case agent on the witness stand in any pretrial hearing is a golden one for the defense, and most will exploit it to the fullest, and beyond. Innocent statements in the affidavit and the mental workings of the agent suddenly become fair game and seemingly not so innocent any more. While the potential for *Franks* issues should be an encouragement to be extra careful and thorough in the affidavit analysis, the defense should be held to their burden of making a substantial preliminary showing that a false statement was knowingly and intentionally included in the affidavit, or was made with reckless disregard for the truth [*Franks v. Delaware*, 438 U.S. 154 (1978)]. Some circuits have expanded *Franks* to include reckless omissions.

Voice Identification

Voice identification can be the biggest challenge in laying the foundation or predicate for the admissibility of tapes and transcripts. Voice identification can be accomplished circumstantially through the tapes themselves, or through identification by a co-conspirator witness, the informant, undercover officer, or even the arresting officer or anyone else who has heard the person speak. Voice exemplars can also be used for comparison purposes. Occasionally, a defendant admits that the voice on the tape is his, but the normal reaction from a defendant confronted with one of his incriminating conversations is, in the immortal words of one such unlucky individual, "that myself is not me."

Remember to have the agents go back and relisten to all the tapes in an attempt to identify previously unknown speakers. As the wire progresses, this becomes easier. If earlier tapes are not re-examined, important evidence may be missed. If you provide the defense with a copy of the transcripts prior to re-examining the tapes, be sure to mark them "draft" so that necessary changes can be made later, with the least amount of controversy.

Evidence

The contents of the interceptions can be powerful evidence of guilt. The jury hears from the horse's mouth that the defendant participated in the criminal activity as charged. Interception evidence can be used very effectively at trial by weaving the interceptions together with other evidence such as co-conspirator testimony, physical surveillance, evidence from searches, financial evidence, business records, toll and pen register information, etc. Some jurors may perceive wiretapping as a heavy-handed measure, even though it is court authorized. Balancing or weaving this evidence with other, perhaps in some instances, more palatable evidence, makes for a more effective presentation of the contents of interceptions. This may also be important in cases where the defendants made extensive use of code words during the course of the taped conversations. The noninterception evidence can assist with corroborating your version of which words used by the defendants are code words and their true meaning. For sentencing purposes, the contents of the interceptions can influence the Probation Department and the court in making sentencing guidelines findings.

Conclusion

The application for and interception of wire, oral, and electronic communications is not meant to be simple. As one of the most intrusive searches the Government can conduct, there are numerous and complicated thresholds and requirements that must be met to succeed in each step of the process. Technology has literally exploded in the communications arena, and the law is struggling to keep up. Law enforcement

and the tools they have readily remain several steps behind potential defendants and their ability to violate the law with little or no detection or interruption from law enforcement. Nevertheless, with sufficient prudence and persistence coupled with an abundance of patience and pain-staking attention to detail, these tools remain arguably the most effective for dismantling criminal organizations and getting the biggest bang for the law enforcement effort and buck. Accordingly, they should be sought and used with great care—and for the greatest effect. ❖

So You've Always Wanted to do a Wiretap: Practical Tips If You Never Have

Assistant United States Attorney Monica Bachner
Central District of California

Preparing and supervising a Federal wiretap is a very time consuming process with a lot of pitfalls. This article highlights some practical tips to avoid common pitfalls[*] for those of you who have never worked on a wiretap.

Affidavit Preparation

The first major hurdle in supervising a wiretap[**] is obtaining a satisfactory affidavit from the law enforcement officer. Often, the affidavit proposed by the investigating agent sets forth probable cause for the crime but does not set forth sufficient probable cause that the facility—the subject of the wiretap application, whether it be a telephone, pager, or room—is being used to facilitate the crime, as is required by the statute. In addition, the affidavit is often too long and contains unnecessary historical information. The Assistant United States Attorney (AUSA) should explain to the agent that the affidavit should summarize background information and then cut to the chase. The affidavit needs to emphasize recent and current activity, focusing on the facility that is the target of the wiretap request.

Similarly, the proposed affidavit often includes boilerplate language concerning the necessity for the wire. This is a crucial portion of the wiretap application and, if found insufficient, will cause suppression. This section should document why particular investigative techniques were tried and failed, would be unlikely to succeed if tried, or are too dangerous. For example, with respect to surveillance, if the investigation is in an unpopulated wilderness or desert area, the affidavit should explain that it would be difficult to conduct vehicle surveillance without being detected because unfamiliar cars would be noticed immediately. Similarly, if the investigation is in a highly populated city gang area where outsiders are noticed, the affidavit should explain that surveillance would be difficult without detection.

In addition to preparing a substantive affidavit, the format is important to expedite the review. First, it is helpful to Department of Justice (DOJ) reviewers and the district court to include sections and headings in the probable cause section of the affidavit. At a minimum, a description of the background of the criminal organization or the history of the investigation and the recent activities of the facility should be included. Second, including an index of (1) the targets and subjects of the investigation and (2) the target telephones, pagers, or other facilities will assist the reviewers and the district court, and is useful for assuring that there is sufficient probable cause for each particular individual and target facility.

Review of the Proposed Wiretap

[*] The checklist that follows this article can be used by AUSAs who have never handled a wiretap to make sure all the steps in applying for or handling wiretaps are completed.

[**] Since the same statutory provisions generally apply to interception of wire communications, oral communications, and electronic communications (such as pagers), the generic term "wiretap" is used to refer to all such communications unless otherwise specified.

Both DOJ and the headquarters of the law enforcement agency requesting the wiretap must review and approve the wiretap application, affidavit, and proposed orders before they are filed with the district court. (An application to intercept a pager does not require DOJ review but must be reviewed by the agency.) This can take from a few days to a few weeks.

The Office of Enforcement Operations lawyer who is assigned to review the application painstakingly and thoroughly checks content and style. At the same time, that lawyer also is reviewing many other wiretaps, so, to obtain the most expeditious review, a final wiretap application should be submitted rather than a draft.

One of the main purposes the agency headquarters reviews the wiretap application is to provide a statement of all other applications for authorization to intercept the same persons, facilities, or places specified in the application. [See 18 U.S.C. § 2518(1)(e).] Since the agency applying for the wiretap must contact the other agencies that conduct wiretaps (FBI, DEA, and Customs) to perform this check, the review is not instantaneous.

Presentation to the District Court

When waiting for final written approval from DOJ, the review by the district court can be expedited after the AUSA is notified orally that the wiretap is approved. Before receiving the written approval (which must be attached to the application), the AUSA can send an advance copy to the judge to review prior to formal presentation. This can speed up the court's review process.

Finally, at the time the AUSA presents the affidavit and application to the district court, the agent should be sworn under oath. A court reporter should be present in case the judge asks the agent substantive questions, as the answers could be considered additional testimony used by the court in support of the authorization of the application. [See 18 U.S.C. § 2518(2).]

Agency Support

A problem often encountered by AUSAs supervising wiretaps is that the investigating agency does not provide sufficient personnel to support the wiretap—during the interception, prior to indictment, or during trial preparation. If this is the case, the following consequences might occur:

- If there are not enough agents or other personnel to monitor the wiretap, the interception may not be able to take place on a 24-hour basis;
- If there are not enough translators or surveillance personnel, the intercepted conversations may not be followed up in a timely manner;
- If there are insufficient personnel to prepare transcripts during the interception, the conversations may not be followed up in a timely manner for investigative purposes; and
- If transcripts have not been prepared pre-indictment, the AUSA may not be able to provide them in a timely manner pursuant to a post-indictment discovery order.

So before agreeing to a wiretap, it is important to obtain the agency's commitment to provide sufficient personnel in all stages, including trial.

Supervising the Wiretap During Interception

Once a wiretap is submitted and approved by the court, the AUSA's job just begins, with the responsibility of submitting additional filings with the court and being available to provide legal advice to the monitoring agents.

First, AUSAs are responsible for providing periodic progress reports to the court, usually every 10 days. These reports, referred to as "10-day reports," inform the court of the progress of the interception, the minimization undertaken, and the need for continued interception. It is useful to include in these reports a provision for written approval of the report by the district court, and continued authorization to intercept. This approval can be used subsequently to defend a claim that the interception was not properly minimized.

In addition to preparing the 10-day reports and if the wiretap needs to be extended, the AUSA should start the extension process almost immediately. To avoid a break in the interception, the application should be submitted to DOJ about one week prior to the end of the 30-day period.

Additionally, AUSAs should be available 24 hours a day by pager to provide advice regarding privileged conversations and on disclosure. The potential privileges most often encountered are attorney-client or spousal communications. Generally, the agent can disclose the contents of the interception to another law enforcement or investigative officer for use in their

duties; however, to provide the information to a foreign law enforcement officer or to civil AUSAs (for example, for use in asset forfeiture), a court order is necessary. [See 18 U.S.C. § 2517.] Finally, AUSAs need to be available to provide strategic and legal advice on possible seizures of contraband, or an unexpected interception of evidence of another crime, such as a proposed kidnapping or homicide.

A problem sometimes encountered during a wiretap is that the target telephone number is changed by the crooks. Terminating the interception can be avoided if the affidavit, application, and order document that the authorization applies not only to the target telephone number but also to any changed number subsequently listed to the same subscriber and assigned the same cable, pair, and binding post used by the target telephone (hard-line telephone), same electronic serial number assigned to the target telephone (cellular telephone), or any other telephone numbers bearing the same CAP code (pager).***

Post-interception Requirements

One area in which AUSAs inexperienced with the minutiae of wiretap procedures can be tripped up is in complying with post-interception requirements. The statute requires that interceptions be sealed **immediately** upon the expiration of the order, or of an extension of the wiretap. If not, the Government must give a "satisfactory explanation." [See 18 U.S.C. § 2518(8)(a); *United States v. Ojeda Rios*, 495 U.S. 257, 110 S.Ct. 1845 (1990).] And the explanation that an AUSA has a heavy workload is not satisfactory. [*United States v. Quintero*, 38 F.3d 1317 (3d Cir. 1994), cert. denied, 115 S.Ct. 1263 (1995).]

In addition, the statute requires that within 90 days after termination of the order or extensions, the AUSA must serve notice of the interception on named parties or other people that the court believes should receive notice (such as people who have been intercepted and located, and are not commercial entities). [See 18 U.S.C. § 2518(8)(d).] The service of an inventory can be postponed with an ex parte showing of "good cause"; the fact that the investigation is ongoing is sufficient cause.

Conclusion

The preparation and supervision of wiretap or other electronic surveillance is a painstaking, very time-consuming task. It is, however, worth all the time invested, as there is no evidence as strong for a jury as a defendant's own voice setting forth his involvement in criminal activity. ❖

_____

***This same documentation may be included in pen register or trap and trace orders.

Wiretap Checklist

I. Application

☐ Identity of applicant and his authority
☐ Type of communication to be intercepted:
  ☐ Wire
  ☐ Oral
  ☐ Electronic
☐ Probable cause that an enumerated offense is being committed (See 18 U.S.C. § 2516.)

- **Wire or Oral Communications**

☐ Narcotics
☐ Bribery
☐ Loan fraud
☐ RICO
☐ Money laundering
☐ Wire or bank fraud
☐ Counterfeiting
☐ Other enumerated offense [See 18 U.S.C. § 2516(1).]

- **Electronic Communications**

☐ Any Federal felony [See 18 U.S.C. § 2516(3).]
☐ Probable cause to believe that particular communications regarding the commission of the enumerated offense will be obtained at the facility (specific telephone or location)
☐ Description of persons expected to be intercepted
☐ Location of facility or place where interception is to occur, unless roving interception, in which case, see 18 U.S.C. § 2518(11)
☐ Statement of necessity:
  ☐ Informants
  ☐ Undercover
  ☐ Surveillance
  ☐ Pen register, trap and trace, toll analysis
  ☐ Search warrants
  ☐ Grand jury
  ☐ Interviews
  ☐ Trash searches
  ☐ Financial investigation
☐ Length of time of interception (30 days)
☐ Identification of all previous wiretap applications
☐ Results of original wiretap when application is for an extension
☐ Surreptitious entry to install, maintain, and remove (for oral and sometimes wire)
☐ Request for authorization to apply for any changed number assigned to target facility
  ☐ Hard line telephone: same cable, pair, and binding post
  ☐ Cellular telephone: same electronic serial number
  ☐ Pager: same CAP code

II. Affidavit as to probable cause

☐ Sworn and attested to by investigative or law enforcement office [18 U.S.C. § 2510(7)]. State or local officers must be deputized.
☐ Establishes probable cause that named interceptees are using targeted telephone or location to commit offenses.
  ☐ Summarizes background
  ☐ Focuses on use of facility
  ☐ Recent and current activity of facility
    ☐ Facility used within 21 days
    ☐ Informant information

- ☐ Undercover information
- ☐ Pen register, trap and trace, toll analysis
  – pen register is usually not enough
- ☐ Surveillance

☐ Statement of necessity
☐ Identification of all prior electronic surveillance
☐ Statement that agents will minimize
☐ If request is for cellular mobile telephone or bug in automobile, state that interceptions not only will be within the territorial jurisdiction of court but anywhere in United States [See 18 U.S.C. § 2518(3).]

III. Ex parte order [18 U.S.C. § 2518(3)]

☐ Probable cause to believe that someone is, has, or is about to commit enumerated offense
☐ Probable cause to believe that interception will reveal communications concerning the offense
☐ Statement of necessity
☐ Probable cause to believe that phone or place where interception is to take place is being used in commission of an offense or if roving interception, statement as to why specification of the place or facility is not practical

IV. Review of Application/Affidavit

- **Wire or Oral Interception**
  - ☐ In-house review
  - ☐ Department of Justice, Office of Enforcement Operations review
  - ☐ Assistant Attorney General review and approval
  - ☐ Agency review

- **Electronic Interception**
  - ☐ In-house review only

V. Procedure for Submission

☐ In camera and under seal
☐ One original for court plus minimal copies of the
- ☐ Application and affidavit
- ☐ Order
- ☐ Redacted order for telephone company

☐ Advance copy to judge while awaiting final authorization
☐ Agent sworn under oath, if Court requires additional sworn testimony [18 U.S.C. § 2518(2)]
☐ Court reporter present
☐ Clerk places order, minutes, and notes under seal
Evidence kept in separate vault in evidence room
Documents in a sealed envelope

VI. Conducting the Interception

☐ Review log forms and procedures with case agent
☐ Interception after order signed, within 10 days
☐ Minimization meeting
☐ 10-day reports to judge
☐ Transcripts
☐ Extension

VII. Post-interception

- **Sealing** [18 U.S.C. § 2518(8)(a)]
  ☐ Immediate: last day of interception or upon expiration of order
  ☐ Tapes presented to judge who initials seal as witnessed by agent
  ☐ Sealed tapes maintained at the agency for 10 years

- **Inventory** [18 U.S.C. § 2518(8)(d)]
  ☐ Within 90 days after termination of the order or extensions, the notice of interception must be served:
    ☐ Named parties
    ☐ Other people that court believes should receive notice (other people who have been intercepted and located but not commercial entities)
  ☐ Can postpone service of the inventory for "good cause" [18 U.S.C. § 2518(8)(d)]
  ☐ Application for Inventory, provides notice of:
    ☐ Entry of the order or the application
    ☐ Date of entry and period authorized, or denial of application
    ☐ Whether or not communications intercepted
- **Disclosure** [18 U.S.C. § 2517(1)-(5)]
  ☐ Other law enforcement or investigative officers for use in official duties
  ☐ Foreign officials (court order required)
  ☐ Civil forfeiture
    ☐ Assistant Attorney General approval
  ☐ Disclosure order

Common (and Uncommon) Problems Encountered During the Course of Title III Investigations

Assistant United States Attorney Patricia Diaz
Southern District of Florida

Introduction

When I first was assigned to the High-Intensity Drug Trafficking Area (HIDTA) division in the Southern District of Florida six short years ago, I had no wiretap experience. This was quite a scary situation because, at that time, it was believed that HIDTA would be doing the majority of the Title III investigations in the Southern District of Florida. That prediction, for at least the first few years, proved to be accurate. During my first year at HIDTA, under the direction of Deputy Chief Theresa Van Vliet, now Chief of the Narcotic and Dangerous Drug Section at the Department of Justice, HIDTA attorneys oversaw about 33 wiretaps, compared to less than five wiretaps the previous year for the entire district.

Now things are different; wiretap investigations are common throughout the district and the different divisions, and HIDTA attorneys no longer bear the brunt of these investigations. However, I still do my share of wiretaps, and continually learn more and more about them and the strange and wonderful things that can happen to an unsuspecting Assistant United States Attorney (AUSA) during these time-consuming and often confusing investigations.

First Rule—What Can Go Wrong, Usually Will

When I was assigned my first wiretap investigation, like most AUSAs I was overwhelmed and uncertain. The first rule I learned was that if something could go wrong, it probably would. What this means in real-life is that if you want any kind of life during the period of time you are working a wiretap investigation, PLAN AHEAD. If not, more than likely you will be spending more time putting out fires than planning your next investigative step. With that in mind, I will share with you three situations that caught me completely off guard. Although the situations are rare, they happened to me and can happen anywhere, especially if you don't expect them. Hopefully, the knowledge I share with you will be your shield against them.

Musical Cellular Telephones

One of the first problems I encountered during a wiretap was by far the most serious. We were tapping a cellular telephone and anticipated, quite correctly, that the targets might change either the telephone instrument itself or the telephone number of the instrument. Accordingly, we planned ahead and, as is common, the court's order permitted us to track the telephone instrument either by the telephone number or by the electronic serial number (ESN) used by the cellular instrument. That way, as long as one of the two stayed consistent—the targets used either the same telephone number or the same cellular instruments—we could continue the interception. We knew that if the target went to a completely different instrument with a completely different telephone number, we would have to reapply for authorization to intercept the communications. What actually happened was much more complicated and resulted in our inability to use the bulk of the intercepted communications.

On the first day of the interception, everything went fine. On the second day, the service provider informed us that the targets changed their telephone number although the ESN remained the same. The service provider gave us the new telephone number and we kept intercepting the communications because we still had the same ESN. Approximately a week or so later, the targets again changed their telephone number. When questioned, the service provider confirmed that when the new telephone number was initiated, the ESN did not change.

Unfortunately, the service provider failed to tell us that on the third day, the day after first changing their telephone number, the targets changed their ESN. When the targets changed their telephone number again, the ESN remained unchanged, but it was the second ESN that remained unchanged, not the original ESN in the court order. To further complicate the situation, after the second telephone number change, the targets **again** changed their ESN. At this point, we had two telephone number changes and two ESN changes, all occurring at different times. This was a rare occurrence and we never learned why the targets did this, although we do not believe it was done to evade law enforcement scrutiny. The bottom line is that from the point the ESN was changed on the third day, we began intercepting an instrument with a new telephone number and a new ESN, neither of which was authorized under the court order. We were then in violation of the law.

The service provider never told of us the subsequent ESN changes; we discovered these facts accidentally during the sealing of the tapes. Although the investigating agency and the USAO both acted in good faith, there was no way to save the wiretap. The statutory exclusionary rule (at 18 U.S.C. 2515) contains no explicit, good-faith exception. Fortunately, the investigation continued without reliance on the wiretap or any tainted information, and the targets were successfully prosecuted and convicted.

The motto of this difficult lesson is to always double-check the information received from your service provider. Make sure they know to call you immediately if **either** the telephone number **or** ESN changes at **any** time. Also, remember that cellular telephones break, and it is not unusual for cell phone companies to give out "loaners" that do not have the same ESN. If your target has already changed his/her telephone number during the course of the interception, stay alert to this possibility. Even your service provider might be unaware of a switch to a "loaner" by a service department.

Cloned Cellular Telephones

A problem reaching epidemic proportions in South Florida, as well as in many other areas, is that of individuals cloning cellular telephones. Many times those individuals are involved in other illegal activities and the "cloned" phone might be the one you want to intercept. The problem arises where you are intercepting calls over a cellular telephone and, after your interception has begun, the phone usage changes and you believe the target telephone has been cloned. All of a sudden, you are intercepting persons who are not your targets. This may be heralded by a dramatically increased volume of calls. If your targets themselves generate a large volume of calls, or if several targets use the same telephone, the situation can become confusing.

This situation is not nearly as serious as my first example. Inadvertently intercepting this independent group of persons not authorized in your court order will not result in the suppression of your wiretap. Additionally, the solution to the problem is fairly simple: inform the court of the situation and minimize those calls that are outside the scope of the original court order. Determining that your target telephone has been cloned can take awhile, especially if it is the first time it happens.

You can't completely avoid this problem but you can anticipate it. Stay in touch with the flow of your intercepted communications. Read your line sheets and try to identify your major targets as soon as possible. Watch for dramatic changes in volume or in conversational context, and if the situation arises, call the service provider and ask them to provide the subscriber with a personal identification number (PIN) and allow them clone free phone-usage. This will permit you to continue your interception uninterrupted by irrelevant calls

Computer Linkages

The final situation arose just last year. We were intercepting a hard-line phone, not a cellular telephone as is now more common. We obtained our court order authorizing the interception of the wire communications, and were proceeding quite nicely. DEA had installed a new state-of-the-art CD-ROM system to replace our cumbersome "three tapes in the machine" system. That CD-ROM system simplified our reporting and tracking of significant conversations—in short, it simplified our lives.

During the interception, one of the calls yielded not voices, but facsimile machine noises (you know the ones). We later learned that the target had a computer with facsimile capabilities hooked up to her telephone line. That situation is common; targets sometimes use their telephones for both verbal conversations and faxes. It usually doesn't matter because you are authorized to intercept either the faxes (electronic communications) and the voices (wire communications) or only one of the two and, thus, don't have the technical set up to intercept the other type.

What we didn't realize at the time was that once those "fax" noises were captured on CD-ROM, they were 'intercepted" in the legal sense of the word. The noises captured by the CD-ROM could be interpreted by that CD-ROM and a print out of the fax generated. In other words, the CD-Rom system is different. It has the built-in capacity to intercept both "wire" and "electronic" communications, and we were not in a position to "disconnect" one or the other.

In this case, although we did not generate the fax print out, there was no doubt that we had, in fact, intercepted "electronic" communications along with the court-authorized interception of wire communications. Needless to say, "electronic" communications were not authorized under our court order. Luckily, the court, whom we informed immediately, found the situation humorous. Subsequently, we were able to establish sufficient probable cause—independent of the improperly intercepted fax transmissions—to obtain an amended order granting the authorization to intercept both wire and electronic communications, and we were able to intercept both the verbal communications and the faxes on that telephone. The solution to the problem in the meantime was simple but cumbersome— we shut off the system whenever the fax noises began—and we

walled off those portions of the CD-Rom that contained the errant fax transmissions that we had inadvertently intercepted.

Check with your investigating agency and see what kind of system they are using. For agencies now using the CD-ROM system, alert them to the potential of this problem, and discuss how to handle it. Do you have enough probable cause to get authorization to intercept faxes as well as voices? If not, get a commitment that those noises will not be intercepted, and include this information in your minimization instructions to your monitoring agents. Failure to do this may not result in the suppression of your wire, but you will have to explain the situation to the court and you will be in violation of the law.

Conclusion

Plan for the unexpected with wiretaps. Just because the above situations were new to this AUSA, doesn't mean that they won't happen to you. The best advice I can give you is to stay alert to any apparent changes in your subjects' use of the targeted facilities, or other variations from the "norm," and keep the lines of communication open among everyone involved in the investigation. Do your best and when in doubt, scream for help. ❖

Attorney General Highlights

Appointments

Deputy Attorney General

On July 18, 1997, United States Attorney Eric Holder, District of Columbia, was sworn in as the Deputy Attorney General. His installation ceremony took place on September 5, 1997, at the Department's Great Hall in Washington, D.C.

Deputy Chief of Staff

On July 16, 1997, Attorney General Janet Reno announced that Kent Markus is her new Deputy Chief of Staff.

Associate Attorney General

On July 21, 1997, Raymond C. Fisher was nominated by President Clinton for the position of Associate Attorney General.

Acting Solicitor General

On September 1, 1997, Seth P. Waxman became Acting Solicitor General.

Assistant Attorney General of Antitrust

On July 17, 1997, Joel I. Klein was confirmed as Assistant Attorney General of the Antitrust Division.

Assistant Attorney General of Civil Rights

On June 12, 1997, William Lann Lee was nominated by President Clinton for the position of Assistant Attorney General of the Civil Rights Division.

Powell Nominated Commissioner of FCC

On August 6, 1997, President Clinton nominated former Chief of Staff Michael K. Powell, Antitrust Division, as Commissioner of the Federal Communications Commission. ❖

New Guidance on

Parallel Proceedings

On July 28, 1997, Attorney General Janet Reno sent a memo to United States Attorneys, Assistant United States Attorneys, Assistant Attorneys General of the Litigating Divisions, and DOJ Trial Attorneys, concerning the coordination of parallel criminal, civil, and administrative proceedings to combat white-collar crime. She discussed the need for attorneys to consider whether there are investigative steps common to civil and criminal prosecutions, and to agency administrative actions, and for them to discuss with colleagues the significant issues that might have a bearing on the matter as a whole. When appropriate, criminal, civil, and administrative attorneys should coordinate an investigative strategy that includes prompt decisions on the merits of criminal and civil matters; sensitivity to grand jury secrecy, tax disclosure limitations, and civil statutes of limitation; early computation and recovery of the full measure of the Government's losses; prevention of the dissipation of assets; global settlements; proper use of discovery; and compliance with the Double Jeopardy Clause.

Additionally, the Attorney General stated that every United States Attorney's office and each Department Litigating Division should have a system for coordinating the criminal, civil, and administrative aspects of all white-collar crime matters within the office. The system should contain management procedures to address parallel proceedings issues including:

1. Timely assessment of the civil and administrative potential in all criminal case referrals, indictments, and declinations;
2. Timely assessment of the criminal potential in all civil case referrals and complaints;
3. Effective and timely communication with cognizant agency officials, including suspension and debarment authorities, to enable agencies to pursue available remedies;
4. Early and regular communication between civil and criminal attorneys regarding Qui Tam and other civil referrals, especially when the civil case is developing ahead of the criminal prosecution; and
5. Coordination with state and local authorities, when appropriate.

The Attorney General directed that appropriate staff in each office receive comprehensive training on parallel proceedings through a course of instruction and training materials to be developed by the Council on White-Collar Crime and the Office of Legal Education. ❖

National Church Arson Task Force Releases Report

On June 8, 1997, the National Church Arson Task Force released a one-year report to the President detailing the results of the Administration's three-pronged response to the nation's church arson crisis, including:

- launching 429 investigations into arsons, bombings, or attempted bombings at houses of worship since January 1, 1995, resulting in the arrest of 199 suspects in connection with 150 of these investigations;

- a 35 percent arrest rate in Task Force arson cases—more than double the 16 percent arrest rate for arsons in general;

- the conviction by Federal, state, and local prosecutors of 110 defendants in connection with fires at 77 houses of worship since January 1995.

For a copy of the report, contact the Department's Office of Public Affairs, (202) 616-2777. ❖

National Methamphetamine Strategy Update

In May 1997, Attorney General Janet Reno and Office of National Drug Control Policy Director Barry McCaffrey released the National Methamphetamine Strategy Update. The report summarizes the methamphetamine problem, the Administration's response, and the progress made during the last year. For personnel in USAOs, your office should have a copy of this report. If not, you may call (202) 616-1681. ❖

President Supports Change in Cocaine Penalties

On July 22, 1997, President Clinton embraced a recommendation from Attorney General Janet Reno to narrow the 100-fold disparity between crack and powder cocaine sentences and urged Congress to reach "an acceptable resolution." Attorney General Janet Reno and Drug Control Policy Advisor Barry McCaffrey proposed that those selling 25 grams of crack and 250 grams of powdered cocaine receive the same mandatory five-year prison sentence. Under current law, selling five grams of crack draws a five-year sentence. A dealer of powdered cocaine would have to sell 500 grams to receive the same amount of prison time. ❖

Immigration and Reform Transition Act of 1997

On July 24, 1997, President Clinton sent to Congress the proposed Immigration Reform Transition Act of 1997. This proposal reflects his commitment to balance firm controls against illegal immigration with common sense and compassion. It would provide a needed transition for individuals who apply for a form of immigration relief called "suspension of deportation" and who had immigration cases pending before the 1996 immigration law took effect.❖

Release of FY 95-96 Health Care Fraud Report

On August 13, 1997, the Department released a report highlighting significant enforcement accomplishments in civil and criminal investigations, prosecutions, convictions, and monetary recoveries during Fiscal Years 1995 and 1996. Increased resources, focussed investigative strategies, and better coordination among law enforcement are ways in which the Department is working to fulfill Attorney General Janet Reno's commitment to make health care fraud one of the Department's top priorities. The Attorney General said recently that, "For the last four years the Department has made significant progress against unscrupulous health care providers," and " . . . our efforts are sending a message to those who would rip-off our health care system that we have the know-how, we have the resources, and we have the will to come after you." According to the report, health care fraud investigations by the FBI more than tripled, from 657 in FY 1992 to 2,200 in FY 1996; criminal prosecutions increased from 83 cases and 116 defendants in FY 1992 to 246 cases and 450 defendants in FY 1996; and convictions—guilty pleas and verdicts—rose from 90 defendants in FY 1992 to 307 in FY 1996. The number of civil health care fraud investigations handled by the Department increased from 270 in FY 1992 to 2,488 in FY 1996. Copies of the report are available at the Department's Office of Public Affairs or by calling (202) 514-2008. ❖

Seventh Anniversary of ADA

On July 24, 1997, Attorney General Janet Reno released a public service announcement in which President Clinton stressed the importance of the Americans with Disabilities Act (ADA). During the one-minute radio spot entitled, "America the Beautiful: Bringing Down Barriers," President Clinton emphasized that access benefits everyone, and urged communities, schools, and businesses to do more to make ADA work. Since the law was signed on July 26, 1990, the Department has investigated hundreds of complaints and reached more than 600 settlements leading to greater access for the disabled. It also has filed nearly 50 lawsuits. The radio announcement urged listeners to learn more by calling the toll-free ADA information line that receives more than 75,000 calls per year. The number is (800) 514-0301
or (800) 514-0383 (TDD). The ADA Home Page on the World Wide Web is http://www.usdoj.gov/crt/ada/adahom1.htm. ❖

Additional Cops to Fight Crime

On July 16, 1997, President Clinton announced nearly $50 million in grants for cities and towns across the nation to hire more than 600 new officers and deputies. The grants are part of the Administration's effort to add 100,000 community policing officers to America's streets. In less than three years of the six-year program, more than 62,000 officers have already been funded. The grants are being awarded under the COPS Universal Hiring Program which funds 75 percent of the total salary and benefits of each officer hired for three years, up to a maximum of $75,000 per officer, and the remainder is paid by state or local funds. More than 9,000 agencies in all 50 states and U.S. territories have received grants for additional community policing officers. ❖

Child Safety Locks

On July 9, 1997, Attorney General Janet Reno called on the Senate Judiciary Committee to support an amendment requiring licensed firearm dealers to include a child safety lock with every handgun sale. The amendment is expected to be introduced this fall. Attorney General Reno's call came at a joint bill signing ceremony in Upper Marlboro, Maryland. Prince George's County Executive Wayne K. Curry and Montgomery County Executive Douglas M. Duncan signed legislation enacted by their county councils to require the sale of child safety locks with every handgun sold in their jurisdictions. The

county legislation, proposed by Duncan and Curry in February, is designed to help prevent the unintentional discharge and unauthorized use of handguns by children. The two bills, which differ slightly, were passed by the Montgomery and Prince George's County Councils on July 1, 1997. ❖

United States Attorneys' Offices/ Executive Office for United States Attorneys

Appointments

Droney Confirmed as District Court Judge

On September 11, 1997, United States Attorney Chris Droney, District of Connecticut, was confirmed by the Senate as United States District Court Judge. ❖

New United States Attorneys

Southern District of Florida

On August 29, 1997, Tom Scott, was sworn in as United States Attorney for the Southern District of Florida. Bill Keefer was the interim United States Attorney for the Southern District of Florida since 1996.

Northern District of Mississippi

On July 31, 1997, the United States Senate confirmed Calvin Buck Buchanan as the United States Attorney for the Northern District of Mississippi. Assistant United States Attorney Al Moreton served as interim United States Attorney since 1993.

Southern District of Ohio

On September 12, 1997, Sharon Zealey was confirmed by the Senate as United States Attorney for the Southern District of Ohio. She takes over for Dale Goldberg who served as interim United States Attorney since August 1996.

District of the Virgin Islands

On September 11, 1997, James A. Hurd, Jr., was confirmed by the Senate as United States Attorney for the District of the Virgin Islands. He served as interim United States since August 6, 1995. ❖

Interim United States Attorneys

Northern District of Alabama

On September 2, 1997, the President nominated Doug Jones to be the United States Attorney for the Northern District of Alabama. The Attorney General appointed Mr. Jones interim United States Attorney on September 8, 1997. Mr. Jones takes over for Caryl Privett who served as interim United States Attorney since February 1995.

District of Columbia

On July 18, 1997, Assistant United States Attorney Mary Lou Leary was sworn in as interim United States Attorney for the District of Columbia. She served as Chief of the Superior Court Division in the district for the past two years.

Northern District of Georgia

On August 15, 1997, Assistant United States Attorney Janet King was sworn in as the interim United States Attorney for the Northern District of Georgia. Janet joined the office in 1980 as an Assistant United States Attorney and most recently served as First Assistant United States Attorney.

Northern District of Illinois

On August 20, 1997, the Attorney General appointed Scott Lassar as the interim United States Attorney for the Northern District of Illinois. Lassar, a former Assistant United States Attorney, rejoined the office in 1993 and, since then, has served as First Assistant United States Attorney.

Eastern District of Oklahoma

On August 15, 1997, the Attorney General appointed Civil Chief Bruce Green, Eastern District of Oklahoma, as interim United States Attorney. From 1961 to 1965, he served as an Assistant United States Attorney. He was appointed United States Attorney by President Johnson in 1965 and served until 1969. He returned to the United States Attorney's office in 1991 and has served there since that time.

Western District of Pennsylvania

On August 1, 1997, Attorney General Reno appointed Assistant United States Attorney Linda Kelly as interim United States Attorney for the Western District of Pennsylvania. Linda has been with the office for four years, serving most recently as First Assistant United States Attorney. ❖

Resignations/Retirement

Northern District of Georgia

On August 15, 1997, United States Attorney Kent Alexander, Northern District of Georgia, resigned after serving as United States Attorney since January 1994.

Northern District of Illinois

On August 20, 1997, United States Attorney Jim Burns, Northern District of Illinois, resigned after serving as United States Attorney since November 1993.

Eastern District of Oklahoma

On August 15, 1997, United States Attorney John Raley, Eastern District of Oklahoma, retired after serving as United States Attorney since April 1990.

Western District of Pennsylvania

On August 1, 1997, United States Attorney Fred Thieman, Western District of Pennsylvania, resigned after serving as United States Attorney since 1993. ❖

Significant Issues/Events

New Bluesheet on Prisoner Confinement

On July 16, 1997, Attorney General Janet Reno sent to United States Attorneys a new bluesheet which establishes procedures for requesting special confinement conditions for Bureau of Prisons (BOP) inmates whose communications pose a substantial risk of death or serious bodily injury to persons. The bluesheet creates a new chapter in Title 9 of the *United States Attorneys' Manual*—9-24.000, Prisoner Confinement. All *Manual* holders should incorporate this bluesheet into Title 9. For personnel in USAOs, your office should have this bluesheet. If not, you may call (202) 616-1681. ❖

Attorney General's Advisory Committee Meetings

The Attorney General's Advisory Committee (AGAC) met at the United States Attorneys' Conference in Santa Fe, May 28-30, 1997. Items discussed were performance appraisals, professional responsibility issues, the Youth Handgun Act, Civil Rights resources, health care fraud, legislation, BOP taping of prisoner conversations, outside activities, environmental issues, and emergency representation of Assistant United States Attorneys.

At another AGAC meeting on June 25-26, 1997, in Washington, D.C., items discussed included the FBI Working Group, health care fraud, reduction in IRS's Criminal Investigative Division resources, death penalty cases, revocation of naturalization proceedings, expanded outreach and recruitment of attorneys, and legislative proposals and updates.

The AGAC met for the final summer session on July 30, 1997, in Washington, D.C. Items discussed included child support cases, the Emergency Witness Assistance Plan, the budget update, the Government Performance Results Act, FBI-DEA Joint Operational Strategy to target major Mexican and Colombian drug trafficking organizations operating in the United States, the functional review of litigating components, sentencing departures based on stipulated deportation, the *Bailey* fix, and requests from the National Association of Former United States Attorneys.

A meeting was held on September 16-17, 1997, and another will be held on October 15-16, 1997, in Washington, D.C. ❖

New Members for LECC/Victim-Witness Subcommittee's Coordinators Advisory Committee

On August 2, 1997, EOUSA Director Carol DiBattiste; United States Attorney Thomas P. Schneider, Eastern District of Wisconsin; and United States Attorney Joseph L. Famularo, Eastern District of Kentucky, sent a memo to United States Attorneys and LECC/Victim-Witness Coordinators announcing the new members of the Coordinators Advisory Committee of the LECC/Victim-Witness Subcommittee. The members will serve a two-year term and will be engaged in policy and programmatic issues surrounding LECC and Victim-Witness priorities. The new members are Fred Alverson, LECC Coordinator, Southern District of Ohio; Eric Day, LECC Coordinator, Southern District of Alabama; Kathleen Griffin, LECC Coordinator, District of Massachusetts; Mary Jane Lattie, LECC/Victim-Witness Coordinator, Eastern District of Louisiana; Mary Jo Speaker, Victim-Witness Coordinator, Eastern District of Oklahoma; and Kathy West, Victim-Witness Coordinator, Western District of Texas. The memo provided background information on all members. The Committee's first meeting took place at the LECC Conference in Miami, September 11-13, 1997. ❖

Criminal and Civil Issues

Federal Witness Security Program

On May 9, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys, First Assistant United States Attorneys, and Criminal Chiefs a memo from Acting Assistant Attorney General John C. Keeney, Criminal Division, requesting the assistance of United States Attorneys' offices (USAOs) in compiling information to substantiate the effectiveness of the Federal Witness Security Program ("Program"). The Criminal Division's Office of Enforcement Operations (OEO), which oversees the Program, needs indictment, conviction, and sentencing data involving defendants for whom witnesses were authorized into the Program, including related information concerning forfeitures, fines, seizures, and restitution. OEO has created a new unit specifically to work with USAOs to analyze Program data, and forms are being sent to the appropriate USAOs. ❖

Fraud Involving Rule 35(b)

On August 14, 1997, EOUSA Director Carol DiBattiste forwarded a memo to United States Attorneys and First Assistant United States Attorneys from Inspector General Michael Bromwich, discussing serious fraudulent schemes involving the use of Federal Rule of Criminal Procedure 35(b) by defense attorneys, informants, inmates, and former officers and agents. The schemes involve defense attorneys who approach inmates and sell them information and cooperation from informants and former officers to use to obtain Rule 35 reductions in their sentences. The inmates then approach Government attorneys with the cooperation, claiming a prior relationship with the informants and seeking sentence reductions based on the work of the informants.

Evidence obtained in the cases indicates that these schemes may be widespread. Inspector General Bromwich advised Assistant United States Attorneys to use extreme caution when considering whether to pursue Rule 35 relief for an inmate based on cooperation or information provided by a third party. Questions should be directed to Assistant United States Attorney Joseph E. Koehler, EOUSA's Counsel to the Director staff, (202) 616-0188. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Ochran v. United States

On August 19, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys, First Assistant United States Attorneys, and Victim-Witness Coordinators informing them that on July 21, 1997, the Court of Appeals for the Eleventh Circuit held that in *Ochran v. United States*, the discretionary function exception to the waiver of sovereign immunity in the Federal Tort Claims Act does not apply to an Assistant United States Attorney's failure to provide information to victims and witnesses about available remedies against intimidation and harassment. Although the court did not reach the issue of whether the failure to provide information gives rise to a cause of action, the decision creates exposure to potential liability in all types of cases involving victims and non-law enforcement witnesses. On September 2, 1997, Acting Solicitor General Seth Waxman authorized the Government's request for rehearing *en banc*. Attached to Ms. DiBattiste's memo is a summary of the decision. Questions should be directed to Assistant United States Attorney Joseph E. Koehler, EOUSA's Counsel to the Director staff, (202) 616-0188. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Illegal Immigrant Reform and Immigrant Responsibility Act

On August 21, 1997, EOUSA Director Carol DiBattiste forwarded a memo to United States Attorneys from Acting Executive Associate Commissioner for Programs Paul Virtue, Immigration and Naturalization Service (INS), regarding the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1997. The memo discusses substantial changes in immigration law as a result of IIRIRA's enhanced criminal penalties to Assistant United States Attorneys who handle immigration matters. Questions should be directed to Assistant United States Attorney Judy Feigin, Counsel to the Director staff, (202) 514-1023, or Senior Special Agent Dave Yost, Office of Investigations, INS, (202) 842-9244. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Economic Espionage Act of 1996

On June 18, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys, First Assistant United States Attorneys, and Criminal Chiefs, a January 10, 1997, memo from Acting Assistant Attorney General John C. Keeney, Criminal Division, concerning the Economic Espionage Act of 1996; a description of the provisions of that Act; and an October 1, 1996, letter from Attorney General Janet Reno to Senator Orrin G. Hatch discussing prior approval of charges under the Act. These documents were forwarded to United States Attorneys' offices again to ensure that there is compliance with the Act. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Hatch Act Amendments

On June 5, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys, First Assistant United States Attorneys, Administrative Officers, and EOUSA Senior Staff, a memo from Assistant Attorney General Stephen Colgate, Justice Management Division, concerning personnel recommendations from members of Congress. Mr. Colgate's memo provides information concerning recent changes to the political recommendation provision of the Hatch Act. Also attached to the memo is a draft letter to be used as guidance when responding to recommendations from Congress. In addition to forwarding Mr. Colgate's memo and accompanying information, EOUSA Director Carol DiBattiste also attached previous memoranda on this subject. Questions should be directed to Legal Counsel Marcia W. Johnson or Senior Attorney Advisor Page Newton, EOUSA's Legal Counsel's office, (202) 514-4024. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Defining a Scheme to Defraud in Mail and Wire Fraud Cases

On May 8, 1997, Acting Assistant Attorney General John C. Keeney, Criminal Division, sent a memo to United States Attorneys, Criminal Division Section Chiefs, and Fraud Prosecutors regarding instructions that define a scheme to defraud in mail and wire fraud cases. In *United States v. Brown*, 79 F.3d 1550 (11th Cir. 1996), the Eleventh Circuit took a restrictive view of the mail fraud statute, 18 U.S.C. 1341, and held that, in order for a mail fraud prosecution to be successful, the Government had to prove that a scheme was capable of deceiving a reasonable person. The court relied on language often used in instructions defining a scheme to defraud and said, "Several courts have said that, because the definition of a 'scheme to defraud' does not have to conform to any technical standards, the scheme need not be fraudulent on its face but must involve some sort of fraudulent misrepresentations or omissions 'reasonably calculated to deceive persons of ordinary prudence and comprehension.'" The memo cites numerous cases and their outcomes. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Repeal of Section 6103(h)(5), Internal Revenue Code

On August 20, 1997, Assistant Attorney General Loretta C. Argrett, Tax Division, sent a memo to United States Attorneys announcing that on August 5, 1997, the Taxpayer Relief Act of 1997 was signed into law as Pub. L. No. 105-34. The Act repeals 26 U.S.C. §6103(h)(5), the provision requiring the IRS to disclose, upon written inquiry by a party, whether prospective jurors in a tax case have been audited or are subject to an investigation by the IRS. Questions should be directed to Chief Robert E. Lindsay, Criminal Appeals and Tax Enforcement Policy Section, Tax Division, (202) 514-3011. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Prosecutions Under Section 7206 of the Internal Revenue Code

On September 9, 1997, Assistant Attorney General Loretta C. Argrett, Tax Division, sent a memo to United States Attorneys, Criminal Chiefs, and Appellate Chiefs concerning pending appellate cases involving the question of materiality under the Supreme Court decision in *United States v. Gaudin*, in prosecutions under section 7206 of the Internal Revenue Code. In *Gaudin*, 115 S.Ct. 2310 (1995), a prosecution for making materially false statements in a matter within the jurisdiction of a Federal agency, the Supreme Court held that the issue of materiality could not be decided by the court as a matter of law but, rather, had to be submitted to the jury for determination. Following the decision in *Gaudin*, courts have considered the applicability of its holding in prosecutions involving other statutes where materiality is an element of the offense.

In tax cases, the issue has arisen in prosecutions under section 7206(1) of the Internal Revenue Code, which makes it a crime to make and subscribe any return or other document that contains or is verified by a written declaration that it is made under the penalties of perjury which the defendant does not believe to be true and correct as to every material matter, and section 7206(2), which makes it a crime to aid and assist in the preparation or presentation of a return or other document which is false or fraudulent as to a material matter. The majority of courts that have considered the question have concluded that the issue of materiality in a prosecution under section 7206 must be submitted to the jury.

The Tax Division requests notification of any cases still pending in the court of appeals or on their way to any courts of appeals that raise the question whether the issue of materiality in a section 7206 prosecution can be taken from the jury and decided by the court. If your office has any such cases, contact Chief Robert E. Lindsay, Criminal Appeals & Tax Enforcement Policy Section, Tax Division, (202) 514-3011. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Alien Terrorist Removal Court

One of the important features of the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) was the creation of the Alien Terrorist Removal Court (ATRC). ATRC is designed to allow the United States to deport alien terrorists on the basis of classified information without having to disclose that information to the alien or the public. An "alien terrorist" is defined as an alien who has engaged, is engaged, or at any time after admission "engages in any terrorist activity." See U.S.C. § 1531(1) and 8 U.S.C. § 1227(a)(4)(B). The phrase "engage in terrorist activity" is a term of art defined in 8 U.S.C. § 1182(a)(3)(B)(iii); see also 8 U.S.C. §1182(a)(3)(B)(ii).

The statute creating ATRC (Title V of the Immigration and Nationality Act, 8 U.S.C. §§1531-1537, as added by the AEDPA and amended by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996) provides for the ex parte filing of a removal application, under seal, by the Government. ATRC approves the application if the Government demonstrates probable cause that (1) the subject of the application is an alien terrorist present in the United States and (2) removal of the alien pursuant to conventional immigration procedures would pose a risk to national security. See 8 U.S.C. §1533.

If ATRC approves the removal application, then a removal hearing is held at which the Government must demonstrate by a preponderance of the evidence that the alien is an "alien terrorist." Although the hearing is public, the Government can introduce classified evidence ex parte and in camera. The alien will not be able to review the classified evidence, although he may receive an unclassified summary of it. See 8 U.S.C. § 1534.

Five ATRC judges were appointed last year by Chief Justice Rehnquist, and the Chief Judge of ATRC, the Honorable Earl H. Carroll, recently issued a set of Court Rules. Although ATRC has nationwide jurisdiction, all of its public hearings are held in the United States Courthouse in Washington, D.C.

The Department's efforts with regard to the ATRC are coordinated by a Task Force chaired by the Terrorism and Violent Crime Section (TVCS) of the Criminal Division. It includes representatives from the Office of Immigration Litigation in the Civil Division, the Immigration and Naturalization Service, the FBI, and the Office of Intelligence Policy and Review.

If you are aware of alien terrorists, call the Chief of TVCS, James S. Reynolds, or TVCS attorneys Jeffrey Breinholt and Yoel Tobin at (202) 514-0849. ❖

Perjured Testimony by Witnesses and Relationships with Witnesses, Subjects, and Targets

On July 30, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys and Professional Responsibility Officers concerning the correction of known instances of perjured testimony by witnesses, and the notification of supervisors of personal relationships with witnesses, subjects, and targets. This memo provides detailed guidance concerning both issues. In summary, it is imperative that AUSAs discuss specific

issues and courses of action with their supervisors when there is doubt about a witness's testimony. Prosecutors should generally err on the side of disclosure to the court if testimony has already been given, and should refrain from putting on a witness if perjury or misleading testimony is anticipated. Additionally, if an AUSA has a personal or business relationship with a witness, subject, or target in a case, that information should be disclosed to a supervisor whether or not the AUSA is involved with the case. Questions should be directed to Senior Attorney-Advisor Robert Marcovici, Legal Counsel's office, (202) 514-4024; AEX13.PO. RMARCOVI (Phoenix); AEX13(RMARCOVI) (Eagle); or fax (202) 514-1104. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681.❖

Federal Money Laundering Cases

On April 23, 1997, Gerald E. McDowell, Chief, Asset Forfeiture and Money Laundering Section (AFMLS), Criminal Division, forwarded to United States Attorneys, a compilation of cases interpreting the Federal money laundering statutes and related forfeiture provisions. To obtain additional copies, contact AFMLS, (202) 514-1263. This publication is also available on the Asset Forfeiture Bulletin Board. ❖

Schedule for Restitution Payments

On May 2, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys and Criminal Chiefs, a memo from Acting Assistant Attorney General John C. Keeney, Criminal Division, notifying United States Attorneys of the Department's position in a United States Supreme Court case regarding statutory changes to the Victim and Witness Protection Act. Prior to the enactment of the Mandatory Victims Restitution Act of 1996 (MVRA) (Pub. L. 104-132), some courts delegated to probation officers the responsibility of establishing restitution payment schedules. The MVRA applies to restitution orders imposed for convictions that occurred on or after April 24, 1996 (the effective date of the MVRA). As the memorandum states, the Department's position on this issue is that a district court may not delegate its responsibility to set restitution payment schedules if the MVRA applies. Please ensure that the memorandum is provided to and reviewed by all prosecutors. Questions regarding this memo should be directed to Associate Director Lynne Solien, Financial Litigation Staff, (202) 616-6444. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Crisis Victim-Witness Response Protocol

On May 9, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys, First Assistant United States Attorneys, LECC Coordinators, Victim-Witness Coordinators, and LECC/Victim-Witness Coordinators, the Department's Crisis Victim-Witness Response Protocol, signed by the Federal Bureau of Investigation (FBI), the Office for Victims of Crime (OVC), and EOUSA. This interagency agreement sets forth the terms of a Department protocol for responding to victims of catastrophic events which result from violations of Federal law. This document was prepared jointly by the FBI, OVC, and EOUSA to identify the responsibilities of personnel called upon to respond to crisis.

The document includes Letters of Intent developed with the Red Cross and the Federal Emergency Management Agency, and a Memorandum of Understanding entered between the Department and the National Transportation Safety Board which addresses families of victims of domestic aviation disasters. For further information, contact Assistant Director Kim Lesnak, LECC/Victim-Witness Staff, (202) 616-6792. Preliminary information concerning the Department's protocol appeared on page 49 of the June 1997 issue of the *United States Attorneys' Bulletin*. ❖

New Equitable Sharing Procedures for Judicial Forfeitures

On April 29, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys, Criminal Chiefs, Civil Chiefs, and Asset Forfeiture Assistant United States Attorney Contacts, a memo from Gerald E. McDowell, Chief, Asset Forfeiture and Money Laundering Section, Criminal Division, concerning the new equitable sharing procedures for judicial forfeitures that have been developed to speed up the process by reducing the equitable sharing paper flow in judicial forfeitures and using the Consolidated Asset Tracking System (CATS). When CATS is fully implemented, sharing information will be posted for all agencies in that system. If you have any questions, contact Suzanne M. Warner, Assistant Director, Legal Programs staff, Executive Office for United States Attorneys, 600 E Street, NW, Room 8500, Washington, D.C. 20530, or call (202) 616-6444. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Follow-up on 911 Compliance Review

On June 6, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys, First Assistant United States Attorneys, Criminal Chiefs, and Civil Chiefs providing follow-up information and guidance on their participation in the Attorney General's initiative to institute an Americans with Disabilities Act (ADA) compliance review of 911 facilities within their communities. This is an effort to initiate the process of compliance review of 911 facilities with the long-term goal of increasing awareness of the need for 911 centers to comply with ADA.

Each United States Attorney's office (USAO) will be required to undertake compliance reviews of five to ten 911 centers within the community. A compliance review involves an on-site review of a 911 center with follow-up for the purpose of assuring that the center has met ADA requirements. The Attorney General has asked larger districts to strive to complete at least ten compliance reviews and smaller districts to strive to complete five reviews by the end of calendar year 1997. Any USAO staff member may conduct a compliance review as long as that staff member has been provided appropriate training and is supervised by an attorney.

The Department's Civil Rights Division is in the process of providing training to staff selected by USAOs to participate in these reviews. The training will be provided by video conference and lasts approximately two hours.

Enclosed with Ms. DiBattiste's memo is a list of the most frequently asked questions about issues relating to this review process, with brief answers to these questions and the name, telephone number, and Email address of the person(s) who can furnish more detailed information; a *9-1-1 ADA Compliance Reviews: A How-To Guide*, which provides answers to many questions about the process and follow-up for compliance review of these centers; and a packet of the training materials used during training sessions including sample letters, settlement agreements, press releases, and other technical assistance materials. Questions should be directed to Jeanette Plante, EOUSA Legal Programs staff, (202) 616-6459. ❖

Reporting Requirement of Systemic Weaknesses Identified in Health Care Benefit Programs

On June 5, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys a June 2, 1997, memo from the Attorney General to Heads of Department components regarding the need to report any systemic weakness identified in a Health Care Benefit Program during the course of a health care fraud investigation. The purpose of the reporting system is to identify and resolve systemic vulnerabilities in Health Care Benefit Programs, thus reducing the probability of future health care fraud in those programs. Assistant United States Attorneys should forward all Systemic Weakness Reports through their Health Care Fraud (HCF) Coordinators to HCF Coordinator Robert W. Liles, EOUSA Legal Programs staff. EOUSA is working with the Executive Level Health Care Fraud Working Group to coordinate the Department's efforts to address systemic problems. Questions concerning the Attorney General's memo should be directed to Robert W. Liles, (202) 616-6444. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Western District of Michigan Publishes Victim-Witness Manual

On May 29, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys and Victim-Witness Coordinators announcing that the United States Attorney's office (USAO) for the Western District of Michigan produced a Victim-Witness Training manual that they would like to share with other USAOs entitled, *Victims' Rights, Witnesses' Rights and Federal Responsibilities: A Guide to the Law*. The manual provides guidance to attorneys and support staff regarding their legal responsibilities to victims and witnesses. It also includes information on victims' rights/Federal responsibilities, restitution in Federal criminal cases, children as victims and witnesses, witness protection, and the responsibilities of the USAOs. For more information or to order a copy of the manual, contact Victim-Witness Coordinator Helen Haring at (616) 456-2404 or AMIW01(HHARING). ❖

Personnel and Administration

Recent Decision Involving Special AUSAs

On May 13, 1997, EOUSA sent a memo to United States Attorneys regarding the decision in *United States v. Navarro*, an Eastern District of California case prosecuted by a cross-designated Special Assistant United States Attorney (SAUSA). The judge dismissed the case, concluding that the cross-designated SAUSA could only serve as a SAUSA for a maximum of four years, the time limitation found in the Intergovernmental Personnel Act, 5 U.S.C. § 3371 et seq. The Department believes the decision is incorrect and is deciding if it will appeal the decision. For more information, contact Senior Attorney-Advisor Robert Marcovici, EOUSA's Legal

Counsel staff, (202) 514-4024. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Special AUSA Program

On August 18, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys, First Assistant United States Attorneys, and Administrative Officers regarding the authority of Special Assistant United States Attorneys (SAUSAs) and the appointment process and delegation of authority under the SAUSA program. Questions should be directed to Personnel Assistant Dorothy Croom, EOUSA Attorney Hiring Staff, (202) 616-6800, or Senior Attorney-Advisor Robert Marcovici, EOUSA Legal Counsel staff, (202) 514-4024. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Intermittent Details

On August 28, 1997, EOUSA Director Carol DiBattiste sent a memo via Email to United States Attorneys, First Assistant United States Attorneys, and Administrative Officers informing them that Attorney General Janet Reno issued a policy that "intermittent" or part-time details outside the Department will be granted only in special or extraordinary circumstances. Ms. DiBattiste's memo included a reminder that all details must be coordinated with EOUSA and details outside the Department must be approved by the Deputy Attorney General. She asked for cooperation in ensuring that no one agree to "intermittent" or part-time details. Questions should be directed to EOUSA's Principal Associate Director Theresa Bertucci, (202) 514-4506. ❖

Timely Reporting of Disposed Criminal Defendants

On July 9, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys, First Assistant United States Attorneys, Criminal Chiefs, Administrative Officers, and System Managers, reminding them that district court records for defendants must be closed at the time of sentencing. Attached to the memo is a report indicating that disposition information for many defendants is being reported in local case management systems long after dismissal or sentencing from district court, which makes it difficult to reconcile district court defendant disposition information with that of the Administrative Office for the United States Courts, or to respond to questions concerning trial trends, since trial information is reported as part of the disposition information. The United States Attorneys' Central System counts defendants and cases disposed of after trial rather than trials. Ms. DiBattiste stated that when a Judgment and Commitment order is issued, the defendant's disposition should be reported, even if an appeal is still ongoing, or if there are other pending defendants. United States Attorneys' offices (USAOs) receive

credit for a "closed defendant" in district court at that time. When the last defendant in a case is closed, USAOs receive credit for a case disposed of after trial. Questions should be directed to Assistant Director Eileen Menton, Case Management Staff, (202) 616-6918. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

More Questions and Answers Regarding the Administratively Determined Pay Plan Revisions

On June 4, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys, First Assistant United States Attorneys, and Administrative Officers, for distribution to all Assistant United States Attorneys, containing answers to more AD Pay Plan questions received since April 28, 1997, when the revisions were announced. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Performance Rating Grievances

On May 21, 1997, EOUSA Director Carol DiBattiste sent a memo to United States Attorneys and First Assistant United States Attorneys concerning the deciding official on performance appraisal grievances. Under current procedures, the EOUSA Director can make the final decision or can delegate the authority. To date, no formal delegation of general applicability has been made, but there have been several ad hoc delegations. The issue of general delegation will continue to be reviewed but, meanwhile, performance appraisal grievances should be submitted to EOUSA's Legal Counsel staff for determination as to the appropriate deciding official. Questions regarding performance appraisal grievances should be directed to Senior Attorney-Advisor Page Newton, EOUSA Legal Counsel staff, (202) 514-4024. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

CTAP Changes

The Office of Personnel Management's (OPMs) changes to CTAP (the DOJ Career Transition Plan) were effective in June 1997. OPM published final regulations on CTAP in the Federal Register (FR), volume 62, number 110, on June 9, 1997. The International CTAP portion of the final regulations were effective 30 days from the publication date of the FR.

Districts may now make internal assignments without regard to CTAP unless there are surplus or displaced employees in any USAO or EOUSA (which there are none). This means that districts may effect internal actions, such as reassignments or changes to lower grade with no further promotion potential, without having to issue a vacancy announcement. Districts may also advertise for internal promotions without having to consider surplus and displaced employees. (These notices of vacancy no longer need to be posted on the DOJ Career Opportunities listing.) Vacancy announcements for internal actions may be prepared in the old format.

If one of the districts or EOUSA has a displaced or surplus employee, EOUSA will notify all districts that CTAP must be cleared before filling internal positions. A one-page summary fact sheet highlighting the major changes contained in the final regulations was distributed at the June 19, 1997, Bureau Personnel Officers' meeting. ❖

Expanded Family and Medical Leave Policies

On May 22, 1997, EOUSA Director Carol DiBattiste forwarded to United States Attorneys and Administrative Officers an April 14, 1997, memo from Director James B. King, Office of Personnel Management (OPM), concerning the President's action to permit employees an additional 24 hours of unpaid leave per year for participation in school activities, routine family medical appointments, and elderly relatives' health needs. Also forwarded were the President's memorandum and questions and answers concerning the expanded Family and Medical Leave Polices. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

American Express Charge Cards for EWAP Expenses

On May 23, 1997, Resource Management and Planning Deputy Director Frank Kalder sent a memo to United States Attorneys and Administrative Officers concerning guidance, use, and implementation of Government centrally billed American Express (AMEX) charge cards for the Emergency Witness Assistance Program (EWAP). Under this program, each United States Attorney may designate one person in their office under whose name the

EWAP/AMEX charge card will be issued. That person may use the card to pay for EWAP expenses **only**. The card may not be used for any other purpose, including personal use. Unauthorized use by the named account holder or others will result in appropriate disciplinary action. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Government Travel Charge Card Program

On June 25, 1997, EOUSA sent a memo to First Assistant United States Attorneys, Budget Officers, and Administrative Officers for distribution to all employees, clarifying the policy and procedures for the Government Travel Charge Card Program. This program was created by the General Services Administration (GSA) as a travel and transportation payment and expense control system and includes employee travel charge cards, automated teller machine services, Government Transportation Accounts, and Travelers Cheques for use by Government employees traveling on official business. Travel Cards are issued to employees who expect to travel two or more times per year. American Express is the company currently under contract to GSA to provide these services to the Government. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

New Limit on Actual Subsistence

On June 27, 1997, EOUSA sent a memo to United States Attorneys, First Assistant United States Attorneys, and Administrative Officers announcing that travel regulations have been amended to permit agencies to authorize actual subsistence reimbursement of up to 300 percent of per diem for travel within or outside the continental United States and in foreign countries. This authority may be exercised for travel circumstances in which actual subsistence up to 150 percent of per diem was formerly authorized. The new limit is effective for travel performed on or after May 1, 1997. Questions regarding this matter should be directed to Michelle Whitted, Travel Cost Coordinator, EOUSA Resource Management and Planning, (202) 616-6886. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Delegation of Authority to Obtain GSA-Leased Vehicles

On August 13, 1997, David W. Downs, EOUSA Deputy Director of Operations, sent a memo to United States Attorneys, First Assistant United States Attorneys, and Administrative Officers, delegating districts the authority to acquire leased motor vehicles from local GSA Fleet Management Offices. Code of Federal Regulations 101-38.103 authorizes use of only Class II compact sedans. Mini vans and 4x4 sport utility vehicles may only be acquired if special needs exist; e.g., weather or transportation of large parcels that will not fit in a compact sedan. Because of the expense, special needs must be documented. If a vehicle is not available from your local GSA Fleet Management Office, one may be available through the Department's Commercial Lease Program. Mr. Downs's memo includes information on funding, billing, reporting mileage, and internal control procedures. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

New FOIA Pamphlet

The Justice Management Division published, "Responding to Requests Under the Freedom of Information Act or The Privacy Act." The pamphlet defines the Freedom of Information Act and the Privacy Act of 1974; answers the questions, "How does the Department respond to requests for access to records?" and What is your role in the Department's response?"; and lists the DOJ Components' FOIA contacts. For a copy of the pamphlet, contact Acting Assistant Director Bonnie Gay, EOUSA FOIA Staff, (202) 616-6757. ❖

EOUSA Telephone Directory

On August 9, 1997, EOUSA Principal Associate Director Theresa Bertucci forwarded to United States Attorneys, First Assistant United States Attorneys, Administrative Officers, and United States Attorneys' Secretaries, the new EOUSA telephone directory and revised organizational listing. The telephone directory is an alphabetical list of EOUSA employees containing telephone and fax numbers, Email addresses, and a backup person for each staff member. The organizational listing is in alphabetical order by staff. By October 1, 1997, the telephone directory will be available on USANet and updated biweekly. Questions or suggestions should be directed to EOUSA Principal Associate Director Theresa Bertucci, (202) 514-4506. For personnel in USAOs, your office should have a copy of these lists. If not, you may call (202) 616-1681. ❖

District of Minnesota Relocates

The District of Minnesota moved to a new location. Their address is 600 United States Courthouse, 300 South 4th Street, Minneapolis, Minnesota 55415. The telephone number is (612) 664-5600, and the fax number is (612) 664-5787. ❖

New Numbers for District of Maryland

Effective August 25, 1997, the main number for the District of Maryland is (410) 209-4800. ❖

New Area Code for Southern District of Texas

The new area code for the Brownsville, Laredo, and McAllen branch offices is 956. The area code for the Corpus Christi branch office, 512, remains the same. ❖

EOUSA Staff Update

Personnel Staff Restructuring

On August 21, 1997, EOUSA Director Carol DiBattiste sent a memo via Email to United States Attorneys, Administrative Officers, Personnel Officers, and EOUSA Staff, announcing the streamlining and restructuring of EOUSA's Personnel Staff to provide better service and guidance to the United States Attorneys' offices, the Community Relations Service, and EOUSA. An organizational chart of the revised structure and a mission and function statement detailing the new structure are attached to the memo. For personnel in USAOs, your office should have a copy of this memo. If not, you may call (202) 616-1681. ❖

Personnel Changes

Security Programs Staff

On June 7, 1997, EOUSA Director Carol DiBattiste announced that Tommie Barnes, who has been serving as Acting Assistant Director of Security Programs during the past year, was selected as the Assistant Director.

Counsel to the Director Staff

AUSA Joseph Koehler, District of Arizona, began a detail with the Counsel to the Director Staff on June 23, 1997. He will serve as liaison with the following AGAC Subcommittees: Controlled Substances/Drug Abuse Prevention and Education, Domestic Safety, Executive Review Board (OCDETF), Investigative Agency, Organized Crime/Violent Crime, and Public Corruption. AUSA Koehler replaced Lee Stapleton who transferred to the Criminal Division as Director of OCDETF.

Claudia Flynn, formerly from DOJ's Criminal Division, joined the Counsel to the Director Staff on September 2, 1997. She will be involved in issues concerning detention, death penalty, investigative agency policy, white collar crime, economic espionage, cyber-bank fraud, criminal results procedures, media relations, special cities, Giglio policy, Government Performance and Results Act, Sentencing Guidelines/BOP, public corruption, and Telemarketing Working Group.

Legal Counsel Staff

On August 4, 1997, Marcia W. Johnson, former Civil Chief for the Northern District of Ohio, became EOUSA's new Legal Counsel. She replaced Juliet Eurich, District of Maryland, who returned to her district at the conclusion of her detail in August. In 1980, Ms. Johnson joined the Northern District of Ohio's Civil Division where she served as Deputy Chief from 1984 to 1988, and as the Chief since 1988. She managed a staff of 34 AUSAs and support staff.

AUSA Phyllis Dow, District of New Mexico, joined the Legal Counsel staff as an attorney-advisor on July 1, 1997. During her detail, she will handle ethics, standards of conduct, adverse actions, and other general legal issues.

AUSA Matthew Orwig, Northern District of Texas, began a detail with the Legal Counsel staff on May 1, 1997. He handles contacts with represented parties issues, immunity issues, ethics matters, and other general legal issues. AUSA Orwig replaced AUSA Sandra Bower from the Middle District of Florida, who transferred to the District of Massachusetts upon completion of her detail.

Office of Legal Education

AUSA Carolyn Adams, Northern District of Georgia, began a detail with OLE as an Assistant Director for LEI Programs on July 7, 1997. She replaced AUSA Eileen Gleason, Eastern District of Louisiana, who returned to her district at the conclusion of her detail on June 9, 1997.

AUSA Johnny Griffin, Eastern District of California, began a detail with OLE as an Assistant Director for Asset Forfeiture Programs on June 16, 1997. He replaced AUSA Tony Hall, District of Idaho, who returned to his district at the conclusion of his detail on June 30, 1997.

AUSA Patricia Kerwin, Middle District of Florida, began a detail with OLE as the Assistant Director for Civil Programs on April 1, 1997. She replaced Jeffrey Senger, an attorney from the Civil Rights Division.

AUSA Stewart Robinson, Northern District of Texas, began a detail with OLE as an Assistant Director for Criminal Programs on February 28, 1997. He replaced AUSA Mary Jude Darrow, Eastern District of Louisiana, who returned to her district in January 1997.

AUSA Elizabeth Woodcock, District of Maine, began a detail with OLE as an Assistant Director on September 2, 1997.

Legal Programs Staff

AUSA Robert Liles, Southern District of Texas, joined the Legal Programs staff on April 1, 1997. Mr. Liles serves as the Health Care Fraud Coordinator and is responsible for implementing program guidelines established pursuant to the passage of the Health Insurance Portability and Accountability Act. He also is the liaison to the Health Care Fraud Subcommittee of the AGAC.

On August 31, 1997, AUSA Leslie Herje returned to the Western District of Wisconsin after a one-year detail with EOUSA Legal Programs staff. ❖

Office of Legal Education

USABook Corner

This month's featured USABook publication is the February 1997 edition of *Guideline Sentencing, An Outline of Appellate Cases on Selected Issues*, by Jefri Wood and Diane Sheehey of the Federal Judicial Center. As with all USABook publications, this work can be downloaded by your systems manager from the EOUSA Bulletin Board, or from USANet.

To make this work more useful, we have attached the complete text of the *United States Sentencing Commission Guidelines Manual* and selected statutes, all of which can be accessed through the table of contents or through hypertext jump links in the text of *Guideline Sentencing*. The result is an extremely comprehensive research manual on sentencing guideline issues.

This is a replacement of the 1995 edition of *Guideline Sentencing*, previously published as a USABook file. If your installation of USABook still features the 1995 edition, ask your systems manager to update your USABook installation. ❖

National Advocacy Center Update

Metric Constructors, Inc., continues to project that the National Advocacy Center building will be substantially completed by January 1998, at which time furnishings and technical systems will be installed during a 90-day period.

The Center's 262,300 square feet of space will accommodate 2,000 people. Office space and parking will be available for a staff of up to 60 people, including 15 who will be affiliated with the National District Attorneys Association, the National College of District Attorneys, and/or the American Prosecutors Research Institute. The rest of the staff will be employees of the Executive Office for United States Attorneys. Each of the 264 single occupancy guest rooms will be equipped with a desk, telephone with a "data jack," queen size bed, private bath, television, and refrigerator. ❖

OLE Projected Courses

OLE Director Michael W. Bailie is pleased to announce projected course offerings for October 1997 through March 1998 for the Attorney General's Advocacy Institute (AGAI) and the Legal Education Institute (LEI).

AGAI

AGAI provides legal education programs to Assistant United States Attorneys (AUSAs) and attorneys assigned to Department of Justice (DOJ) Divisions. The courses listed are tentative; however, OLE sends Email course announcements to all United States Attorneys' offices (USAOs) and DOJ Divisions approximately eight weeks prior to the courses.

LEI

LEI provides legal education programs to Executive Branch attorneys (except AUSAs), paralegals, and support personnel. LEI also offers courses designed specifically for paralegal and support personnel from

USAOs. OLE funds all costs for paralegals and support staff personnel from USAOs who attend LEI courses. Please note that OLE does not fund travel or per diem costs for students who attend LEI courses. Approximately eight weeks prior to each course, OLE sends Email course announcements to all USAOs and DOJ Divisions requesting nominations. Nominations are to be returned to OLE via Fax, and then student selections are made.

Other LEI courses offered for Executive Branch attorneys (except AUSAs), paralegals, and support personnel are officially announced via quarterly mailings to Federal departments, agencies, and USAOs. Nomination forms are available in your Administrative Office or attached as **Appendix A**. They must be received by OLE at least 30 days prior to the commencement of each course. Notice of acceptance or non-selection will be mailed to the address typed in the address box on the nomination form approximately three weeks prior to the course.

Videotape Lending Library

A list of videotapes offered through OLE and instructions for obtaining them are attached as **Appendix B**.

Office of Legal Education Contact Information

Address:	Bicentennial Building, Room 7600 600 E Street, NW Washington, DC 20530-0001	Telephone: FAX:	(202) 616-6700 (202) 616-6476

Director . . . . . Michael W. Bailie
Deputy Director . . . . . Kent Cassibry, FAUSA, SDTX
Assistant Director (AGAI-Criminal) . . . . . Jackie Chooljian, AUSA, CDCA
Assistant Director (AGAI-Criminal) . . . . . Stewart Robinson, AUSA, NDTX
Assistant Director (AGAI-Civil and Appellate) . . . . . Patricia Kerwin, AUSA, MDFL
Assistant Director (AGAI-Asset Forfeiture and
Financial Litigation) . . . . . Johnny Griffin, AUSA, EDCA
Assistant Director (LEI) . . . . . Donna Preston
Assistant Director (LEI) . . . . . Carolyn Adams, AUSA, NDGA
Assistant Director . . . . . Elizabeth Woodcock, AUSA, Maine
Assistant Director (LEI-Paralegal and Support) . . . . . Donna Kennedy
Assistant Director (Victim-Witness) . . . . . Michelle Tapken, AUSA, South Dakota

AGAI Courses

Date	Course	Participants
	October	
7-9	Federal Tort Claims Act	AUSAs, DOJ Attorneys
7-10	Grand Jury	AUSAs, DOJ Attorneys
15-17	Introduction to Financial Litigation	AUSAs, DOJ Attorneys
20-31	Civil Trial Advocacy	AUSAs, DOJ Attorneys
21-23	Basic Money Laundering/Asset Forfeiture	AUSAs, DOJ Attorneys
21-24	Narcotics/Electronic Surveillance	AUSAs, DOJ Attorneys
21-24	United States Attorneys' Office Management	USAO Management Teams
	November	
4-6	Bankruptcy Fraud	AUSAs, DOJ Attorneys
12-14	Asset Forfeiture for Criminal Prosecutors	AUSAs, DOJ Attorneys
12-14	Enhanced Negotiation/Mediation	AUSAs
17-20	Criminal Chiefs Conference	USAO Criminal Chiefs
17-21	Advanced Civil Trial	AUSAs, DOJ Attorneys
18-21	Computer Crimes	AUSAs, DOJ Attorneys
	December	
1-4	United States Attorneys' Office Management	USAO Management Teams
8-11	Advanced Civil Practice	AUSAs, DOJ Attorneys
2-4	Financial Investigations for AUSA/Agents	AUSAs, DOJ Attorneys, Agents
2-12	Criminal Trial Advocacy	AUSAs, DOJ Attorneys
8-11	Information Technology in Litigation and Investigation	AUSAs, DOJ Attorneys
9-11	Affirmative Civil Enforcement/Health Care Fraud Investigators	ACE/HCF Investigators
16-18	Enhanced Negotiation/Mediation	AUSAs, DOJ Attorneys
	January 1998	
5-9	Advanced Criminal Trial	AUSAs, DOJ Attorneys
6-8	Selected Topics-FLU Agents	Financial Litigation Staff
12-15	Narcotics/Electronic Surveillance	AUSAs, DOJ Attorneys
12-15	Economic Crimes	AUSAs, DOJ Attorneys
13-15	Basic Bankruptcy	AUSAs, DOJ Attorneys
13-16	International/National Security Coordinators	Inter./Nat. Security Coordinators
20-22	Asset Forfeiture for Support Staff	USAO, DOJ Support Staff
22-23	Enhanced Negotiation/Mediation	AUSAs
26-29	Native American Issues	AUSAs, DOJ Attorneys
26-30	Appellate Advocacy	AUSAs, DOJ Attorneys
27-30	USAO Management	USAO Management Teams
	February	
2-4	Health Care Fraud	AUSAs, DOJ Attorneys
2-11	Criminal Trial Advocacy	AUSAs, DOJ Attorneys
3-5	Financial Litigation Team Training	USAO Fin.Lit. Personnel
10-13	Employment Discrimination	AUSAs, DOJ Attorneys
17-19	Asset Forfeiture/Advanced Money Laundering	AUSAs, DOJ Attorneys
17-20	Computer Crimes	AUSAs, DOJ Attorneys
18-19	Enhanced Negotiations/Mediation	AUSAs, DOJ Attorneys
23-27	Criminal FPS	AUSAs, DOJ Attorneys
23-3/6	Civil Trial Advocacy	AUSAs, DOJ Attorneys
	March	
2-6	Professional Responsibility Officers Conference	Professional Responsibility Officers
10-12	Asset Forfeiture for Criminal Prosecutors	AUSAs, DOJ Attorneys
10-13	Advanced Criminal Practice	AUSAs, DOJ Attorneys
16-18	Advanced Bankruptcy	AUSAs, DOJ Attorneys
16-20	Appellate Advocacy	AUSAs, DOJ Attorneys
17-20	USAO Management	USAO Management Teams
24-25	Enhanced Negotiations/Mediation	AUSAs
24-26	Financial Litigation Team Training	USAO Fin.Lit. Personnel

LEI Courses

Date	Course	Participants
	October	
1-3	Discovery	Agency Attorneys
6-10	Legal Research and Writing Refresher (Agency)	Agency Support Staff
14-15	Freedom of Information Act for Attorneys and Access Professionals	Agency Attorneys
16	Privacy Act	Agency Attorneys
22	Ethics for Litigators	Agency Attorneys
24	Legal Writing	Agency Attorneys
27-31	Basic Paralegal (Agency)	Agency Paralegals
	November	
4-5	Freedom of Information Act for Attorneys and Access Professionals	Agency Attorneys
6	Privacy Act	Agency Attorneys
12	Ethics and Professional Conduct	Agency Attorneys
13	Introduction to Freedom of Information Act	Agency Attorneys
17-21	Legal Support - DOJ	USAO, DOJ Support Staff
24-26	Contracts/Federal Acquisition Regulations	Agency Attorneys
24-26	Debt Collection for Agency Counsel	Agency Attorneys
	December	
3	Advanced Freedom of Information Act	Agency Attorneys
4	Administrative Forum	Agency Attorneys
8-12	Experienced Legal Secretary	USAO, DOJ Secretaries
9-11	Public Lands and Natural Resources	Agency Attorneys
17-18	Agency Civil Practice	Agency Attorneys
	January 1998	
5-9	Support Staff Supervisors	USAO Support Staff Management
6-9	Examination Techniques	Agency Attorneys
16	Legal Writing	Agency Attorneys, Paralegals
21-22	FOIA for Attorneys and Access Professionals	Agency Attorneys and Support Staff
26-30	Basic Paralegal-DOJ	USAO and DOJ Paralegals
	February	
3-5	Federal Tort Claims Act for Agency Counsel	Agency Attorneys
9-13	Civil Paralegal	USAO and DOJ Paralegals
10-12	Attorney Supervisors	Agency Supervisors
18	Introduction to FOIA	Agency Attorneys and Support Staff
19	Ethics for Litigators	Agency Attorneys
23-27	Legal Support Staff-DOJ	USAO and DOJ Support Staff
	March	
10-11	Evidence	Agency Attorneys
16-20	Legal Research and Writing-DOJ	USAO and DOJ Support Staff
24-25	FOIA for Attorneys and Access Professionals	Agency Attorneys and Support Staff
26	Privacy Act	Agency Attorneys and Support Staff
27	Legal Writing	Agency Attorneys, Paralegals
30-4/3	Support Staff Supervisors	USAO Support Staff Management
31-4/2	National Environmental Policy Act	Agency Attorneys

Computer Tips

With the move to Phoenix and WordPerfect 6.1, our Computer Tips column will now focus on WP 6.1 tips. If you have tips to share with the AUSA community, please send them to Barbara Jackson, AEX12(BJACKSON), or write: Executive Office for United States Attorneys, 600 E Street, N.W., Washington, D.C. 20530-0001.

WordPerfect 6.1 Tips and Techniques I

Judy Johnson
EOUSA's Financial Litigation Staff

Legal Programs' Judy Johnson submitted the following two articles to share with *FYI* readers. They previously appeared in the newsletter, *DebtBeat*.

You've got a new computer program to learn, and it's called WordPerfect 6.1 for Windows. Those of you who are continuing to desperately cling to the antiquated program, WordPerfect 5.1, take note: the Windows version is faster, easier to use, and a hundred times more versatile.

I must admit that my first few times using the program were frustrating, but I bought a book (*Using WordPerfect 6.1 for Windows*, by Que, copyright 1994) and just kept at it. There are several good books out there, and some are very basic. The *Dummies* (no insult intended) series of books is a good place to begin. I also did something else: I had my office subscribe to WordPerfect's magazine. For only about $30 per year, you can get helpful articles on WordPerfect for Windows. For an additional charge, you can also get a diskette containing the macros and programs from each issue.

Here are some of the reasons why I think this program is so great:

UNDO At the top of your menu, you should see an arrow curving to the left. This is your Undo button (it's also accessible from the Edit menu (**Edit, Undo**). Clicking on the button will undo the last action. Accessing the same feature through your Edit menu does the same thing but with one exception. You have the option of choosing **Undo/Redo History**, and you could literally undo every action you've taken.

UNDELETE Hitting the delete key doesn't totally get rid of your deletion; it is possible to undelete deleted text. You can undelete text either through the **Edit** menu (**Edit, Undelete**) or by the following key combinations: **Ctrl+Shift+Z**.

MARGINS Setting margins is a snap. WordPerfect's default is one inch on each of the four sides of the document (top, bottom, left, and right). Margins are easily changed through the **Format** menu (**Format, Margins**, or **Ctrl-F8**). The values can be entered in decimals (.5) OR, here's a special feature, you can add them in fractions (½).

The ***REALLY*** special feature, however, is to call up the Ruler Bar (**View, Ruler Bar** or **Alt+Shift+F3**). With the Ruler Bar on the screen, you can move the left and right margins wherever you want them.

TABS Setting tabs is also snap. WordPerfect's default is a tab every half inch, but you can easily change them to suit your needs. When I want to set individual tabs for a document, I start by clearing all tabs (**Format, Line, Tab Set, Clear All**). Then I call up the ruler bar (**View, Ruler Bar** or **Alt+Shift+F3**) and click wherever I want to place a tab. Double clicking brings up the tab set menu and you can change the justification (or change them from relative to absolute, or pick an exact spot for a tab). You can remove unwanted tabs by dragging them off the ruler bar. Setting tabs used to be SOP before WordPerfect decided to set them for us, but they've simplified personalizing tab sets to prevent having to do five or six tabs just to get to a spot in a document where you want to type something.

SELECTING TEXT

To select text, hold down the **Shift** key and use the arrow keys to highlight what you want to select. **Shift+Ctrl+An arrow key** selects a whole word. **Shift+End** selects to the end of the line. **Shift+Ctrl+Down arrow** selects a whole paragraph. **Shift+Ctrl+End** selects to the end of the document. **Ctrl+C** copies the selected text to the clipboard, **Ctrl+X** deletes the selected text to the clipboard, and **Ctrl+V** moves the text to your selected location.

QUICK CORRECT

WordPerfect's QuickCorrect feature is a Godsend. Type "teh," and the program automatically changes it to "the." "Adn" becomes "and," "april" becomes "April," and on and on and on. What's ***REALLY*** nice is that you can add your own. If you always misspell a word, add it to your Quick Correct menu and you'll never have to worry about misspelling it again. ***AND***, if you type "TWo"(mistakenly capitalize the first two letters of a word which I do ALL THE TIME), Quick Correct changes it automatically to "Two." Quick Correct is accessed through the **Tools** menu (**Tools, Quick Correct**).

I put acronyms here so that when I type, "flpm" it automatically expands it to "Financial Litigation Program Manager." If I type it in all caps "FLPM," the words come out in all caps. There's no end to the uses for Quick Correct. ***BUT***, there's also "***ABBREVIATIONS***!"

ABBREVIATIONS

Here's where I store all of my acronyms. Once stored, a simple command (**Ctrl+A**) expands them for you. Never again type out "United States District Court" (just type USDC and then **Ctrl+A**) or United States Attorney's Office (USAO and then **Ctrl+A**), or any other acronyms. Abbreviations are accessed through the **Insert** menu (**Insert, Abbreviations**). You type the full name of the acronym, go into the Abbreviations menu, and then create the acronym. The acronyms you create are case sensitive, by the way, so if you type "USDC" it will expand as "United States District Court." But you could also create "usdc" to expand as "District Court." ***NOTE: I just read in the May 1997 issue of WordPerfect for Windows magazine that you can use Abbreviations to expand whole paragraphs or PAGES of text. Really helpful when you're doing boilerplate work. I LOVE WordPerfect for Windows magazine!!!***

WordPerfect 6.1 Tips and Techniques II

Judy Johnson
EOUSA's Financial Litigation Staff

Opening Multiple Documents to Work on Them. WordPerfect 6.1 for Windows allows you to work on multiple documents during a session, a great help when you are involved in cutting and pasting. I don't think there's a limit to the number of documents you can have open, but I personally have had at least four open at once. You can also easily choose how you want to display the multiple documents. You can cascade them (fan them like you would paper), tile them horizontally (one on top of the other) or tile them vertically (beside each other). I usually just work on one and switch to the other when I need to, giving me a whole screen for each of the documents I'm working on.

To open multiple documents just do **Ctrl-O** or click on the open file folder on your tool bar OR open your documents using the file menu (**File, Open**). Do this for as many documents as you wish. To cascade or tile them click on **Window** and then choose the one you want (**Cascade, Tile Horizontal, Tile Vertical)**. If you would rather have only one document in a window at a time, select **Window** and then select the number of the document you want to switch to.

Keeping Text Together 1. A personal favorite of mine. I wish I had a dollar for every time someone entered extra hard returns to break a page exactly where they want it (or entered a hard page break). This is fine if you only work on a document once (NOT!). There are three different things you can do to keep text together:

1. You can turn on Widows and Orphans which will prevent one line in a paragraph from remaining on a page.

2. You can block and protect text to ensure it always stays together (block protect).

3. You can enter a Conditional End of Page code to keep text together.

To do any of the above, you go into the **Format** menu. Select **Format, Page, Keep Text Together** and choose the one you want. I have modified my Initial Style (at the top of every single document you open) to have Widows and Orphans turned on for every document I work on. (More on modifying the Initial Style in a later article.)

Before you use Block Protect, you must block the text you want to protect. As I said in the last article, simply hold down the shift key and move the arrow through however much text you want to protect. Then select **Format, Page, Keep Text Together** and click the box that says **Block Protect**.

Before you use Conditional End of Page, you must count the number of lines you want to stay together beginning with the first line of the text (**NOTE: This is a change from WP5.1 which required that you begin counting with the line above the text you wanted to keep together.)** Then select **Format, Page, Keep Text Together** and click the box that says **Conditional End of Page**.

Keeping Text Together 2: Sometimes you must keep text together (e.g., not have the month on one line and the day and year on the next). Instead of using hard returns (which throw off the spacing, you can use a **HARD SPACE** by holding down the **CTRL** key as you hit the space bar. This works for any text you always want together on the same line. The **CTRL** key also works with the "dash" or "hyphen." Cites (USAM 3-11.500) and dates (1-3-97) are an excellent example of wanting to keep them on the same line. **CTRL+-** changes the symbol in reveal codes from **-Hyphen** to a dash.

Helping WP Know When to Split Text. If you have ever used the slash to keep two similar words together ("and/or" or "full-service/full-function"), WP treats it as one word and will keep it together (if you're using the hyphen instead of the dash, discussed above, it will break the text after a hyphen). To tell WP it's okay to split up text containing a slash, use a **Hyphenation Soft Return** code, which is in the **Format, Line** menu.

Inserting Characters in Your Text. Under the **Insert** menu you'll find the selection "**Character**." There's lots of goodies here. Check it out. For example, this is where you get your "**§**" symbol. You change to **Typographic Symbols** and you'll see it. Check out all of the different character sets you can use.

Fonts. Under the **Format** menu you'll find **Font** (the easier way: **F9**). But an even easier way to keep from having those pesky font codes in the document you're working on is to change the font through the format menu's **Document** screen. Select **Format, Document, Initial Font.** Another way to keep from having unnecessary font codes in your document is to use the font menu's **Relative Size** option. If you want the heading of a document to be larger than the text, do **F9** (or **Format**, **Font**) and then choose **Relative Size**. The selections here are **Fine, Small, Normal, Large, Very Large, and Extra Large**. Block the text first before entering the Font menu or you'll change the size of the entire document. I use Large for headings, and small for footnotes.

Italics. The easiest way to italicize text is to use the tool bar at the top of the screen. When you look up there you'll see an italicized ***"I"*** which you click on when you want to start italicizing text (you can also do **CTRL+I**). If you have already typed the text, simply block the text and then select **CTRL+I** or click on the italicized ***"I."***

DOJ Highlights

Appointments

Civil Rights Division

Acting Deputy Chief and Coordinator for Involuntary Servitude and Slavery Matters

On May 8, 1997, EOUSA Director Carol DiBattiste forwarded a memo to United States Attorneys, First Assistant United States Attorneys, Criminal Chiefs, and Civil Chiefs from Richard Roberts, Chief, Criminal Section, Civil Rights Division, announcing that Peggy Kuo will serve as Acting Deputy Chief of the Criminal Section, Civil Rights Division, for matters in the 4th, 6th, 7th, and 8th Circuits. She can be reached on (202) 616-3948. Additionally, Lou de Baca will serve as the section's Coordinator for Involuntary Servitude and Slavery matters. He can be reached on (202) 514-2734.

Criminal Division

New OCDETF Director

On June 2, 1997, AUSA Lee Stapleton Milford, Southern District of Florida, was selected as the Director for the Executive Office of Organized Crime Drug Enforcement Task Force program.

Environment and Natural Resources Division

New Chief of Environmental Crimes Section

On July 21, 1997, the Department's Environment and Natural Resources Division named Steven P. Solow Chief of the Environmental Crimes Section. Solow was Acting Chief of the Section since May 1997, and served as an Assistant Chief in the Section since 1994.

Solow is responsible for environmental criminal investigations and prosecutions, as well as coordination with and support for United States Attorneys throughout the country handling environmental crimes. He succeeds Ronald Sarachan who left the Section to return to the United States Attorney's office in Philadelphia.

Solow named Deborah Smith Deputy Chief of the Section, which is a new position. Smith served as an Assistant Chief in the Section since 1995. ❖

Office of the Solicitor General

United States v. Brockamp, No. 95-1225. Argued December 3, 1996, by Deputy Solicitor General Lawrence G. Wallace. (Decided February 18, 1997.)

In a unanimous decision, the Court ruled that the Ninth Circuit erred when it read into Section 6511 of the Internal Revenue Code a nonstatutory "equitable tolling" exception to that Section's time (and related amount) limitations for filing tax refund claims. ❖

Robinson v. Shell Oil Co., No. 95-1376. Argued November 6, 1996, by Assistant to the Solicitor General Paul R. Q. Wolfson. (Decided February 18, 1997.)

The Court unanimously held that the term "employees" under Section 704(a) of Title VII of the Civil Rights Act of 1964 includes former employees, thus allowing petitioner to sue respondent for its alleged retaliatory post-employment actions. ❖

Maryland v. Wilson, No. 95-1268. Argued December 11, 1996, by Attorney General Janet Reno. (Decided February 19, 1997.)

In a 7-2 decision, the Court extended to passengers of lawfully stopped cars the rule of *Pennsylvania v. Mimms*, 434 U.S. 106 (1977), which permits police officers as a matter of course to order drivers of lawfully stopped cars to exit their vehicles. ❖

Schenck v. Pro-Choice Network of Western New York, No. 95-1065. Argued October 16, 1996, by Acting Solicitor General Walter Dellinger. (Decided February 19, 1997.)

This case involved the constitutionality of an injunction entered against petitioners after a number of blockades and other illegal conduct at reproductive health care clinics. The injunction provided, *inter alia*, that petitioners were prohibited from demonstrating "within fifteen feet * * * of * * * doorways or doorway entrances, parking lot entrances, driveways or driveway entrances" of the clinics (fixed buffer zones), and from demonstrating "within fifteen feet of any person or vehicle seeking access to or leaving such facilities" (floating buffer zones). An additional provision of the injunction allowed two "sidewalk counselors" inside the buffer zones, but required them to cease and desist from their activities within the zone if the woman so requested. Petitioners contended that the injunction violated their right to free speech under the First Amendment. We argued as *amicus curiae* in support of respondents. In an opinion by Chief Justice Rehnquist, the Court applied the test from *Madsen v. Women's Health Center, Inc.*, 512 U.S. 753 (1994), and upheld the injunction with regard to the fixed buffer zone and the cease and desist provision as it applied to that zone. The Court struck down the floating buffer zones, because they burdened more speech than necessary to serve the relevant governmental interests. The Court emphasized the lack of certainty as to how a protester would remain in compliance with such a zone around people on sidewalks and the fact that such a zone around vehicles would restrict peaceful speech at the curb—even where there is no blocking of entrances or the street. ❖

United States v. Wells, No. 95-1228. Argued November 4, 1996, by Deputy Solicitor General Michael R. Dreeben. (Decided February 26, 1997.)

The Supreme Court held that 18 U.S.C. 1014, which prohibits making false statements for the purpose of influencing the actions of a federally insured financial institution, does not require proof of materiality. ❖

Bennett v. Spear, No. 95-813. Argued November 13, 1996, by Deputy Solicitor General Edwin S. Kneedler. (Decided March 19, 1997.)

This case held that a biological opinion issued by the Fish and Wildlife Service is final agency action and, therefore, subject to review under the Administrative Procedure Act. ❖

Turner Broadcasting System, Inc. v. FCC, No. 95-992. Argued October 7, 1996, by Acting Solicitor General Walter Dellinger. (Decided March 31, 1997.)

After 18 months of additional fact finding following the Supreme Court's remand in *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622 (1994), in a 5-4 decision the Court affirmed on direct appeal the district court's conclusion that the expanded record contained substantial evidence supporting Congress's predictive judgment that the "must-carry" provisions of the Cable Television Consumer Protection and Competition Act of 1992, which require cable television systems to dedicate some of their channels to local broadcast television stations, further important governmental interests in preserving the benefits of free, over-the-air broadcast television and that the provisions are narrowly tailored to promote those interests. ❖

United States v. Lanier, No. 95-1717. Argued January 7, 1997, by Deputy Solicitor General Seth Waxman. (Decided March 31, 1997.)

Respondent, a Tennessee state judge, was convicted under 18 U.S.C. 242 for violating the constitutional rights of five women by sexually assaulting them while serving as a judge, thereby depriving them of their Fourteenth Amendment due process right to liberty. The Sixth Circuit set aside the convictions based on its interpretation of the "fair warning" requirement of *Screws v. United States*, 325 U.S. 91 (1945). Justice Souter, writing for a unanimous Court, reversed. The Court held that the Sixth Circuit had employed a more rigid standard than was required under *Screws* for determining whether the particular conduct is proscribed under Section 242. Reasoning that the "touchstone" is whether the statute, either alone or as interpreted, made it reasonably clear that the conduct was criminal, the Court held that "fair warning" did not require a Supreme Court decision based on very similar facts. ❖

***Chandler v. Miller*, No. 96-126. Argued January 14, 1997. (Decided April 15, 1997.)**

This case held that requiring candidates for state office to pass a drug test is not a constitutionally permissible suspicionless search. Writing for a majority of eight Justices, Justice Ginsburg stated that without evidence of a drug problem among Georgia's elected officials there is no special "need" to perform such tests. The Court distinguished its prior cases involving Customs Agents, transportation employees, and high school athletes, noting that the hazards in those cases are real and not simply hypothetical. The Court also took care to distinguish a singular drug examination from a comprehensive medical examination designed to provide certification of a candidate's health, and expressed no opinion on the latter situation. ❖

***Richards v. Wisconsin*, No. 96-5955. Argued March 24, 1997, by Assistant to the Solicitor General Miguel A. Estrada. (Decided April 28, 1997.)**

The Court held that the Fourth Amendment does not permit a blanket exception to the knock-and-announce requirement for felony drug investigations. In order to justify a "no-knock" entry, the police must have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or lead to the destruction of evidence. However, the Court upheld the conviction, reasoning that the police had a reasonable suspicion to proceed with a "no-knock" entry based on petitioner's strange behavior. The United States argued as *amicus curiae* in support of the State. ❖

***Strate v. A-1 Contractors*, No. 95-1872. Argued January 7, 1997, by Assistant to the Solicitor General Jonathan E. Nuechterlein. (Decided April 28, 1997.)**

In a unanimous decision rejecting our position as *amicus curiae*, the Court held that tribal courts may not entertain claims against nonmembers arising out of accidents on state highways, absent a statute or treaty authorizing the tribe to govern the conduct of nonmembers on the highway in question. In an opinion by Justice Ginsburg, the Court observed that "[t]he right-of-way North Dakota acquired for the State's highway renders the [strip running through the reservation] equivalent, for nonmember governance purposes, to alienated, non-Indian land." ❖

***Johnson v. United States*, No. 96-203. Argued February 25, 1997, by Deputy Solicitor General Michael R. Dreeben. (Decided May 12, 1997.)**

The Court held that a trial court's failure to allow a jury to decide the issue of materiality in a perjury case, although in direct conflict with the Court's holding in *United States v. Gaudin* that the materiality of a false statement is to be decided by a jury, does not require reversal under Fed. R. Crim. P. 52(b)'s "plain error" rule. ❖

***Clinton v. Jones*, No. 95-1853. Argued January 13, 1997, by Acting Solicitor General Walter Dellinger. (Decided May 27, 1997.)**

The Court ruled that the President does not have temporary immunity from civil damages litigation arising out of events that occurred before he took office. ❖

***United States v. LaBonte*, No. 95-1726. Argued January 7, 1997, by Deputy Solicitor General Michael R. Dreeben. (Decided May 27, 1997.)**

The Court upheld our position that the phrase "at or near the maximum term authorized" in 28 U.S.C. 994(h), which addresses sentencing guidelines for adult repeat offenders, includes all applicable statutory sentencing enhancements and accordingly invalidated as inconsistent with Section 994(h)'s plain language the Sentencing Commission's contrary interpretation, embodied in Amendment 506 of the Sentencing Guidelines, which precluded consideration of statutory enhancements. ❖

***United States v. Hyde*, No. 96-667. Argued April 15, 1997, by Assistant to the Solicitor General James A. Feldman. (Decided May 27, 1997.)**

The Court upheld our position that, even though a district court has deferred decision on whether to accept or reject a plea agreement, Federal Rule of Criminal Procedure 32(e) requires a defendant seeking to withdraw his guilty plea to offer a "fair and just reason" for doing so. ❖

***Gilbert v. Homar*, No. 96-651. Argued March 24, 1997, by Assistant to the Solicitor General Ann Hubbard. (Decided June 9, 1997.)**

Adhering to its view that the Due Process Clause of the Fourteenth Amendment calls for a "flexible" approach, the Court agreed with our position as *amicus curiae* and rejected as "indefensible" the Third Circuit's absolute rule that public employees suspended without pay are in all cases entitled to notice and a hearing prior to such suspension. ❖

***Hughes Aircraft Co. v. United States ex rel. Schumer*, No. 95-1340. Argued February 25, 1997, by Deputy Solicitor General Seth Waxman. (Decided June 16, 1997.)**

In 1986, Congress amended the *qui tam* provision of the False Claims Act, 31 U.S.C. 3730(b), to partially remove a bar to suits if the information on which the suits were based was already in the Government's possession. In 1989, respondent filed a *qui tam* action involving false claims submitted between 1982 and 1984 and based on information already in the Government's possession. In this case, a unanimous Court held, contrary to our position as *amicus curiae*, that the 1986 amendment does not apply retroactively, and it accordingly determined that the underlying action must be dismissed. ❖

***Idaho v. Coeur d'Alene Tribe of Idaho*, No. 94-1474. Argued October 16, 1996. (Decided June 23, 1997.)**

Respondent sought declaratory and injunctive relief precluding Idaho officials from regulating or interfering with its possession of submerged lands beneath Lake Coeur d'Alene. In a 5 to 4 decision, the Court held, contrary to our position as *amicus curiae*, that the Eleventh Amendment bars a Federal court from hearing the Tribe's claims. In his opinion for the Court, Justice Kennedy reaffirmed the principle that sovereign immunity restricts not only suits by individuals against sovereigns but also suits by sovereigns against sovereigns. Accordingly, the Court reasoned, the Tribe's suit was barred unless it fell within the exception under *Ex parte Young*, 209 U.S. 123 (1908), for certain suits seeking declaratory and injunctive relief against state officers in their individual capacities. ❖

***Richardson v. McKnight*, No. 96-318. Argued March 19, 1997, by Deputy Solicitor General Edwin S. Kneedler. (Decided June 23, 1997.)**

In agreement with our position as *amicus curiae*, the Court held that individuals employed as prison guards by "a private firm, systematically organized to assume a major lengthy administrative task (managing an institution) with limited direct supervision by the Government, [and which] undertakes that task for profit and potentially in competition with other firms," are not entitled to a qualified immunity from suit by prisoners charging a violation of 42 U.S.C. 1983. ❖

***Glickman v. Wileman Bros. & Elliott, Inc.*, No. 95-1184. Argued December 2, 1996, by Assistant to the Solicitor General Alan Jenkins. (Decided June 25, 1997.)**

In agreement with our position, the Court held in a 5 to 4 decision that a marketing program— administered under marketing orders issued by the Secretary of Agriculture pursuant to the Agricultural Marketing Agreement Act of 1937, requiring handlers of California peaches, plums, and nectarines to fund a generic advertising program for those commodities— does not violate the First Amendment. ❖

***City of Boerne v. Flores*, No. 95-2074. Argued February 19, 1997, by Acting Solicitor General Walter Dellinger. (Decided June 25, 1997.)**

The Court considered the constitutionality of the Religious Freedom Restoration Act of 1993 (RFRA), which was designed to nullify the effect of *Employment Division, Department of Human Resources v. Smith*, 494 U.S. 872 (1990), by providing that facially neutral laws of general applicability may not burden a person's exercise of religion unless justified by a compelling interest and narrowly tailored. In a 6 to 3 decision, the Court held, contrary to our position, that RFRA is not a proper exercise of Congress's power under Section 5 of the Fourteenth Amendment and "contradicts vital principles necessary to maintain separation of powers and the Federal balance." ❖

***United States v. O'Hagan*, No. 96-842. Argued April 16, 1997, by Deputy Solicitor General Michael R. Dreeben. (Decided June 25, 1997.)**

The Court upheld our position in all respects. It first held in a 6 to 3 decision that a person who trades in securities for personal profit, using confidential information misappropriated in breach of a fiduciary duty to the source of the information, may be held liable under Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. 78j(b), and Rule 10b-5 of the Securities and Exchange Commission (SEC), 17 C.F.R. 240.10b-5. The Court also held in a 7 to 2 decision that the SEC did not exceed its rulemaking authority under Section 14(e) of the Act, 15 U.S.C. 78n(e), when it adopted SEC Rule 14e-3(a), 17 C.F.R. 240.14e-3(a), which prohibits certain persons from trading while in possession of material, non-public information relating to a tender offer obtained from the bidder or the target, without requiring a showing that the trading at issue entailed a breach of fiduciary duty. ❖

Reno v. ACLU, No. 96-511. Argued March 19, 1997, by Deputy Solicitor General Seth Waxman. (Decided June 26, 1997.)

Contrary to our position, the Court invalidated as contrary to the First Amendment two provisions of the Communications Decency Act of 1996 (CDA): 47 U.S.C. 223(a), which prohibited the knowing transmission of "obscene or indecent" messages to any recipient under 18 years of age; and 47 U.S.C. 223(d), which prohibited the knowing sending or displaying of "patently offensive" messages in a manner that is available to a person under 18 years of age. Although the Fifth Circuit held that those provisions violated both the First Amendment and the Fifth Amendment, the Court, in an opinion by Justice Stevens, concluded that, because it discussed "the vagueness of the CDA" in relation to its "First Amendment overbreadth inquiry," it would affirm the judgment of the Fifth Amendment "without reaching the Fifth Amendment issue." The Court surveyed its precedents and concluded that the provisions imposed "a content-based blanket restriction on speech," that there were "significant differences" between the CDA and other "narrower" statutes it had upheld, that the Internet "has no comparable history" to that of other media, and that the "special justifications for regulation of the broadcast media"—the history of extensive Government regulation, the scarcity of available frequencies at its inception, and its "invasive" nature— "are not present in cyberspace." ❖

Raines v. Byrd, No. 96-1671. Argued May 27, 1997, by Acting Solicitor General Walter Dellinger. (Decided June 26, 1997.)

In agreement with our position, the Court held in a 7 to 2 decision that Members of Congress lack standing to bring a suit challenging the constitutionality of the Line Item Veto Act. ❖

Printz v. United States, No. 95-1478, *Mack v. United States*, No. 95-1503. Argued December 3, 1996, by Acting Solicitor General Walter Dellinger. (Decided June 27, 1997.)

In a 5 to 4 decision rejecting our position, the Court "adhered" to the principle announced in *New York v. United States*, 505 U.S. 144 (1992), that "the Federal Government may not compel the States to enact or administer a Federal regulatory program" and held that certain interim provisions of the Brady Handgun Violence Prevention Act "commanding state and local chief law enforcement officers to conduct background checks on prospective handgun purchasers" were "fundamentally incompatible with our constitutional system of dual sovereignty." ❖

Office of Justice Programs

Breaking the Cycle of Drug Abuse and Crime

Assistant Attorney General Laurie Robinson

Studies and statistics indicate that the fastest and most cost-effective way to reduce the demand for illicit drugs is to treat chronic, hardcore drug users. They consume the most drugs, commit the most crimes, and burden the health care system to the greatest extent. Without treatment, chronic hardcore users continue to use drugs and engage in criminal activity and, when arrested, they too frequently continue their addiction upon release. The cycle of dependency must be broken and the revolving door of criminal justice brought to a halt. ❖

National Drug Control Strategy Office of National Drug Control Policy February 1995

Since its beginning, our criminal justice system has looked for effective ways to change criminal behavior. Research has shown a strong link between the use of illegal drugs and involvement in other crimes. The Office of Justice Programs (OJP) is attacking this twin problem by

encouraging expansion of drug testing, treatment, and sanctions at all levels of the criminal justice system.

The statistics linking drug abuse and crime are striking. The most recent data from the National Institute of Justice's (NIJ) Drug Use Forecasting program shows that an average of 63 percent of adult male arrestees test positive for drugs. Extensive research into the relationship between drug abuse and crime provides evidence that drug-addicted persons commit as many as three to five times more crimes than non-addicts. Yet, only about 11 percent of prison inmates participate in drug treatment programs. And those not treated all too often return to drug use and criminal activity when they are released back into the community. Moreover, drug users who are involved in criminal activity tend to consume an enormous amount of illegal substances. Earlier this year, the Office of National Drug Control Policy (ONDCP) estimated that about 60 percent of the cocaine and heroin consumed by the entire nation over a year is consumed by individuals arrested in that year.

These compelling findings have brought treatment of drug-abusing criminal offenders to the forefront of the Administration's drug control strategy. Last year, for example, the President charged the Attorney General with implementing a comprehensive system of drug testing, sanctions, and treatment in the Federal court system. Modeled on a demonstration program conducted by the Administrative Office of the United States Courts, DOJ is working with the Administrative Office to implement Operation Drug TEST (Testing, Effective Sanctions, and Treatment) in 25 of the 93 Federal districts. The program calls for testing of all Federal defendants prior to their first appearance before the court. The results of their drug tests will be submitted to the judicial officer to use in determining if release is appropriate and, if so, under what conditions. Treatment will be provided to drug-addicted offenders.

OJP is implementing a wide range of programs that support the Administration's drug control strategy. While OJP's programs focus on state and local efforts, many of the issues are mirrored in the Federal system. United States Attorneys are a key component of bringing knowledge of what works and what's needed in the field to the table. I hope that OJP's programs at the state and local level can provide guidance for expanding drug testing and treatment efforts in the Federal system.

OJP Initiatives

The drug court experience has been a great example, both for demonstrating the ability to translate grass-roots successes into nationwide programs and for illustrating the coercive power of the court in intervening with drug-abusing offenders. With over 150 drug courts now operating around the country, we're seeing real success in reducing addiction and recidivism among drug court graduates. Starting at the local level, the drug court movement has received significant Federal support—$30 million in FY 1997 alone under our Drug Courts Grant Program, as well as allocations from local jurisdictions through the Local Law Enforcement Block Grant Program.

OJP is encouraging the spirit of collaboration that makes drug courts successful in other programs that comprehensively address drug addiction, crime, and corrections. Last year, with funding from the Office of National Drug Control Policy, NIJ provided funding to a research demonstration project in Birmingham, Alabama, called Breaking the Cycle. Under this project, which began operations in June 1997, everyone arrested in Birmingham will be tested for drug use, and every component of the criminal justice system—including prisons and jails, the pretrial and probation departments, judges, prosecutors, and defense counsel—will work together with the goal of reducing the level of drug use from the time of arrest to final disposition. The project will help us assess over several years the effectiveness of such system-wide intervention, and will look at the interrelationships of sanctions and treatment and their effect on changing criminal behavior.

OJP research has found that drug treatment is particularly effective in prison-based programs. To reach incarcerated drug-addicted offenders, OJP's Corrections Program Office (CPO) administers the Residential Substance Abuse Treatment (RSAT) Program, which provides formula grant funding—$30 million this year—to states to implement residential drug treatment programs in state and local prisons and jails.

RSAT programs provide comprehensive treatment services to offenders nearing the end of their term of confinement so they can be released from prison after completing the treatment program, rather than being returned to the general prison population. In addition to addressing the substance abuse problems of participants, RSAT treatment programs seek to address underlying problems that accompany drug abuse by developing the inmate's cognitive, behavioral, social, vocational, and other skills, including aftercare—a very key component—to make the transition to post-prison life successful.

A provision of the FY 1997 Appropriations Act requires states to implement a program of drug testing, sanctions, and intervention for offenders under corrections as a condition for continuation funding in FY 1999 under the Violent Offender Incarceration and Truth-in-Sentencing (VOI/TIS) Incentive Grant Program, another program administered by OJP. In accordance with these guidelines, before March 1, 1998, each state must submit to OJP a copy of its drug testing policies and procedures and a description of how the policies are being implemented. The treatment and testing provisions must be implemented by September 1, 1998. This additional provision is yet another indication

of the support at the Federal level for prison-based drug testing at the state and local levels.

Expanding Research and Evaluating Results

The programs and demonstration projects that have been developed to address the needs of drug-addicted offenders grew out of a combination of grass-roots experimentation and extensive scientific research into the linkage between drug abuse and crime. Through its grant programs, OJP will continue to encourage expansion and innovation on both fronts.

At the heart of much of OJP's work in this area is the Arrestee Drug Abuse Monitoring (ADAM, formerly Drug Use Forecasting, or DUF) program. ADAM is NIJ's national and local information system on drug abuse, crime, and social issues. In the next several years, ADAM will expand from its current network of 23 sites to 75 large United States city research sites. ADAM provides drug use data through interviews and testing of adult and juvenile arrestees and detainees, and will help us learn more about important issues like the relationship between drugs and violent crime, the occurrence of drug overdoses and drug-related medical emergencies, gun use and attitudes about guns among arrestees, and the need for drug treatment in the arrestee population. In addition to informing the national-level drug strategy, local law enforcement and policy makers can look to data generated from individual ADAM sites to make more informed policy decisions.

And to ensure our programs are having an impact, OJP incorporates evaluation requirements into most of its grant programs. Under the Residential Substance Abuse Treatment program, for example, each participating state is required to submit a detailed annual evaluation report. NIJ is conducting a national evaluation of the RSAT program, with technical assistance provided to the grantees from CPO and NIJ. CPO and NIJ also provide technical assistance to states conducting independent evaluations sponsored under the RSAT program. And CPO conducts national and regional workshops, as well as on-site technical assistance for RSAT grantees. Information about all these programs is available through our toll-free Corrections Technical Assistance Line, (800) 848-6325.

In addition, NIJ is supporting an evaluation of the Federal Operation Drug TEST, Breaking the Cycle, and the drug court program. Through such evaluations of existing programs, investments in promising initiatives in the field, and research based on information collected through ADAM, we will continue to expand efforts to break the cycle of addiction and crime. ❖

Bureau of Justice Assistance

Fact Sheet

The Bureau of Justice Assistance (BJA) fact sheet: "FY 1997 Local Law Enforcement Block Grants Program," is available. For a copy, contact the BJA Clearinghouse, (800) 688-4252, or write, P.O. Box 6000, Rockville, MD 20849-6000. ❖

Bureau of Justice Statistics

New Crime Data on Internet

The Bureau of Justice Statistics has revised its Internet Web Page, adding new graphs and data tables that show long-term and short-term crime trends and other criminal justice statistics. The revamped and expanded site can be found at: http://www.ojp.usdoj.gov/ bjs/.

Publications

The following Bureau of Justice Statistics (BJS) publications are available: "National Conference on Juvenile Justice Records: Appropriate Criminal and Non-criminal Justice Uses—Proceedings of a BJS/SEARCH Conference"; "Privacy and Juvenile Justice Records: A mid-decade status report"; "Criminal Victimization, 1973-1995," and a supporting technical document, "The Effects of Redesign on Victimization Estimates"; and "Prisoners in 1996." For copies, contact the BJS Clearinghouse, (800) 732-3277, or write, P.O. Box 6000, Rockville, MD 20849-6000. ❖

National Institute of Justice

Publications

The following National Institute of Justice (NIJ) publications are available: "Intermediate Sanctions in Sentencing Guidelines"; "Lethal Violence—Proceedings of the 1995 Meeting of the Homicide Research Working Group"; "National Institute of Justice Journal, Spring 1997"; "Guns in America: National Survey on Private Ownership and Use of Firearms"; and "Crack's Decline: Some Surprises Across U.S. Cities." For copies, contact the National Criminal Justice Reference Service (NCJRS), (800) 851-3420, or write, Box 6000, Rockville, MD 20849-6000. ❖

Office of Juvenile Justice and Delinquency Prevention

Juvenile Justice Bulletins

The following Office of Juvenile Justice and Delinquency Prevention (OJJDP) Bulletins are available: "Portable Guides to Investigating Child Abuse: An Overview"; and "Allegheny County, PA: Mobilizing To Reduce Juvenile Crime."

Program Report

The Office of Juvenile Justice and Delinquency Prevention (OJJDP) Program Report: "Sharing Information: A Guide to the Family Educational Rights and Privacy Act and Participation in Juvenile Justice Programs," is available.

Reference Guides

The Office of Juvenile Justice and Delinquency Prevention (OJJDP) published the 8th, 9th, and 10th reference guides in the Portable Guides to Investigating Child Abuse series. The new titles are, "Burn Injuries in Child Abuse," "Law Enforcement Response to Child Abuse," and "Criminal Investigation of Child Abuse."

Statistics Summary

The Office of Juvenile Justice and Delinquency Prevention (OJJDP) Statistics Summary: "Juvenile Offenders and Victims: 1997 Update on Violence," is available.

For copies of these OJJDP Publications, contact the Juvenile Justice Clearinghouse, (800) 638-8736, or write, Box 6000, Rockville, MD 20849-6000. ❖

Immigration and Naturalization Service

New Locations

On June 9, 1997, the Immigration and Naturalization Service (INS) announced the opening and expansion of a dozen INS offices in nine states—Arkansas, Delaware, Iowa, Mississippi, New Hampshire, South Dakota, West Virginia, and Wyoming. Existing INS offices will be expanded in South Carolina and Wyoming. The move will strengthen enforcement of the nation's immigration laws and extend the agency's presence to all 50 states. INS plans to have the new offices operational by September 30, 1997. ❖

Career Opportunities

The U.S. Department of Justice is an Equal Opportunity/Reasonable Accommodation Employer. It is the policy of the Department of Justice to achieve a drug-free workplace and persons selected for the following positions will be required to pass a drug test to screen for illegal drug use prior to final appointment. Employment is also contingent upon the satisfactory completion of a background investigation adjudicated by the Department of Justice.

The following announcements can be found on the Internet at http://www.usdoj.gov/careers/oapm/jobs.

GS-12 to GS-15 Trial Attorneys Civil Rights Division Educational Opportunities Section

DOJ's Office of Attorney Personnel Management is seeking two experienced attorneys for the Civil Rights Division, Educational Opportunities Section, Washington, D.C. (One of these positions is a term appointment NTE two years but maybe renewed for an additional two-year term.) Occasional travel may be required. As a trial attorney, the incumbent is responsible for analyzing and responding to allegations of violations; conducting field investigations; locating documentary evidence; preparing requests to the FBI for field investigations; performing legal research and making recommendations; preparing motions, pleadings, and briefs; conducting pre-trial discovery; and reviewing Federal court decisions. The Educational Opportunities Section is responsible for enforcing Federal statutes which prohibit public school officials from engaging in discriminatory practices under Title IV of the Civil Rights Act of 1964 and the Equal Educational Opportunities Act of 1974. The Section also enforces Section 504 of the Rehabilitation Act of 1973 and Title II of the Americans with Disabilities Act with respect to students enrolled in public educational institutions. The Section may intervene in private suits which allege violations of education-related anti-discrimination statutes and the Fourteenth Amendment of the Constitution. In addition, the Section represents the Department of Education (DOE) in certain types of suits filed against the Secretary of Education, as well as for filing suits on behalf of the Secretary when school districts and colleges fail to comply with DOE regulations.

Applicants must possess a J.D. degree, be duly licensed and authorized to practice as an attorney under the laws of a State, territory, or the District of Columbia, and have at least one year of post-JD litigation experience. **No telephone calls please**. Applicants must submit a current OF-612 (Optional Application for Federal Employment), SF-171 (Application for Federal Employment) or a resume, along with a writing sample to:

US Department of Justice
Civil Rights Division
PO Box 65958
Washington DC 20035-5958

Current salary and years of experience will determine the appropriate salary level. The possible range is GS-12 ($45,939-$59,725) to GS-15 ($75,935-$98,714). This position is open until filled but applications postmarked after October 10, 1997, will not be considered.

GS-12 to GS-14 Experienced Attorneys Environment and Natural Resources Division Environmental Defense Section

DOJ's Office of Attorney Personnel Management is seeking experienced attorneys to handle complex civil cases in Federal courts under all Federal environmental statutes for the Environment and Natural Resources Division's Environmental Defense Section in Washington, D.C.

Applicants must possess a J.D. degree, be duly licensed and authorized to practice as an attorney under the laws of a state, territory, or the District of Columbia, and have at least two years of post-J.D. experience. Applicants must submit a resume to:

US Department of Justice
Environment and Natural Resources Division
Attn Executive Officer
Post Office Box 7754
Washington DC 20044-7754

No telephone calls please. These positions are open until filled, but no later than October 3, 1997. Current salary and years of experience will determine the appropriate salary levels. Possible salary range is GS-12 ($45,939-$59,725) to GS-14 ($64,555-$83,922).

GS-13 to GS-15 Experienced Attorney Environment and Natural Resources Division

General Litigation Section

DOJ's Office of Attorney Personnel Management is seeking an experienced attorney for the General Litigation Section of the Environment and Natural Resources Division (ENRD), in its Washington, D.C., headquarters office. The section is primarily responsible for litigation of numerous environment and natural resources cases on behalf of the United States in the United States district courts and in the claims court. A moderate amount of travel is involved.

Applicants should have an excellent academic record; possess a J.D. degree; be duly licensed and authorized to practice as an attorney under the laws of a state, territory, or the District of Columbia; and have at least three or more years of post-J.D. civil litigation experience. Experience in environmental and natural resources litigation is highly desirable.

To apply, please submit a cover letter and resume to:

US Department of Justice
Environment and Natural Resources Division
Attn Executive Officer
Post Office Box 7754
Washington DC 20044-7754

No telephone calls please. The position is open until filled, but no later than October 3, 1997. Current salary and years of experience will determine the appropriate salary levels. Possible salary range is GS-13 ($54,629-$71,017) to GS-15 ($75,935-$98,714).

Detail—Immigration and Naturalization Service
Office of Naturalization Operations

DOJ's Office of Attorney Personnel Management is seeking an attorney for a six-month reimbursable detail for the Office of Naturalization Operations of the Immigration and Naturalization Service (INS) in Washington, D.C. Because of the nature of the detail, this position is open only to current DOJ attorneys.

The detailee will be responsible for the overall design and development of an assessment process for the English language and civics requirements related to naturalization, as defined by statute. INS is seeking an individual who: (1) has a background in working with designs and strategies for test development and implementation, including significant experience working with independent consultants in the areas of statistics, industrial/organizational psychology, and educational testing; (2) has a proven record of successful team-building and oversight for a project that involved design and development of an assessment technique; and (3) is familiar with legal principles affecting assessment validation and the legal defense of assessment systems. Extensive knowledge of testing case law and practical experience litigating in Federal courts on testing issues is highly desirable. INS prefers a detailee on a full-time basis, but may consider other arrangements.

Because assignment of the detail is subject to approval, all applications must be submitted through both the applicant's supervisor and the administrative office to evidence the consent of the employing organization. Applicants must submit a resume and most recent performance appraisal, if applicable, to:

US Immigration and Naturalization Service
Attn Shirley Lloyd
801 Eye Street NW
Suite 900
Washington DC 20536-0001

Applications must be submitted by October 3, 1997. No telephone calls please.

Immigration Judges
Executive Office for Immigration Review

DOJ's Executive Office for Immigration Review is seeking applicants for Immigration Judge positions which may become available in the future. The base pay for these positions is currently set at the Immigration Judge 1 level ($80,990) with promotion potential to the Immigration Judge 4 level ($106,444). Salaries may vary depending on geographic location. All applicants must be available for frequent travel, have a valid driver's license, and be willing to travel by air. Relocation expenses are not authorized.

Applications are being sought for locations throughout the country with current specific interest in Buffalo, New York; Bloomington, Minnesota; Chicago, Illinois; Dallas, Texas; Denver, Colorado; Eloy, Arizona; Houston, Texas; Lancaster, California; Las Vegas, Nevada; Los Angeles, California; Miami/Krome, Florida; Newark, New Jersey; New York City, New York; Oklahoma City, Oklahoma; Phoenix, Arizona; and Reno, Nevada.

The Immigration Judge presides in formal, quasi-judicial hearings. Proceedings before Immigration Judges include but are not limited to deportation, exclusion, removal, rescission, and bond. The Immigration Judge makes decisions, which are final unless formally appealed, in connection with these proceedings, exercises certain discretionary powers as provided by law, and is required to exercise independent judgment in reaching final decisions.

Applicants must have an LL.B. or a J.D. degree and must be duly licensed and authorized to practice law as an attorney under the laws of a state, territory, or the District of

Columbia. Applicants must also have a minimum of 7 years of relevant post bar admission legal experience at the time the application is submitted, with one year of experience equivalent to the GS-15 level in the Federal service.
Selective Placement Factors:

- Substantial knowledge of Immigration and Nationality Act and procedure.

- Substantial litigation experience, preferably in a high volume context.

- Experience handling complex legal issues.

- Ability to conduct administrative hearings.

- Knowledge of judicial practices and procedures.

All applicants are required to submit either a current OF-612, "Optional Application for Federal Employment," or SF-171, "Application for Federal Employment," and a resume that specifies the location(s) for which you are applying. **In addition, applicants must submit a supplementary narrative statement specifically addressing each of the Selective Placement Factors listed above.** Applicants who previously applied for this position and still wish to be considered must submit a new application. All applications must be submitted to:

US Department of Justice
Executive Office for Immigration Review
Office of the Chief Immigration Judge
Attn Assistant Chief Immigration Judge Jill H. Dufresne
5107 Leesburg Pike Suite 2545
Falls Church VA 22041

Applications must be received no later than September 30, 1997. Interviews will not be conducted until the latter part of 1997. Applicants are not limited to Federal Government employees. Telephone inquiries will not be accepted.

GS-13 to GS-14 Experienced Attorney Justice Management Division Personnel Staff

DOJ's Office of Attorney Personnel Management is seeking an experienced attorney for the Justice Management Division, Personnel Staff, Workforce Relations Group. Incumbent is primarily responsible for providing advice and or representation in matters regarding adverse actions and disciplinary actions and must be knowledgeable about Merit Systems Protection Board policies and practices (MSPB). Incumbent may also be called upon to draft exceptions to arbitration awards and unfair labor practice decisions by Administrative Law Judges, to draft appeals in response to Union negotiability appeals, and to support the Department in actions before the Courts of Appeals.

Applicants must possess a J.D. degree; be duly licensed and authorized to practice as an attorney under the laws of a state, territory, or the District of Columbia; have at least 3½ years post J.D. experience; and have MSPB experience. Applicants should submit a detailed resume and/or OF-612 (Optional Application for Federal Employment) and, if applicable, a copy of the latest SF-50 (Notification of Personnel Action) and a supervisory performance appraisal issued within the last 12 months to:

US Department of Justice
JMD Personnel Staff
Attn Vivian B. Jarcho
1331 Pennsylvania Avenue NW
Room 1150
Washington DC 20530

A current SF-171 (Application for Federal Employment) will still be accepted as well. No telephone calls please. Applications must be postmarked by October 17, 1997. Current salary and years of experience will determine the appropriate salary level from the GS-13 ($54,629-$71,017) to the GS-14 ($64,555-$83,922) range.

GS-11 to GS-14 Experienced Attorney United States Trustee's Office San Antonio, Texas

DOJ's Office of Attorney Personnel Management is seeking an experienced attorney for the United States Trustee's office in San Antonio, Texas. Responsibilities include assisting with the administration of cases filed under Chapters 7, 11, 12, or 13 of the Bankruptcy Code; drafting motions, pleadings, and briefs; and litigating cases in the Bankruptcy Court and the United States District Court.

Applicants must possess a J.D. degree, be duly licensed and authorized to practice as an attorney under the laws of a state, territory, or the District of Columbia, and have at least one year of post J.D. experience. Outstanding academic credentials are essential and familiarity with bankruptcy law and the principles of accounting is preferred. Applicants must submit an OF-612 (Optional Application for Federal Employment) or resume, and law school transcript to:

US Department of Justice
Office of the United States Trustee
Attn Peggy C. Taylor
515 Rusk Suite 3516
Houston TX 77002

A current SF-171 (Application for Federal Employment) will still be accepted as well. No telephone calls please. Current salary and years of experience will determine the appropriate salary level. The possible range is GS-11 ($37,507-$48,761) to GS-15 ($74,304-$96,594). This position is open until filled, but no later than October 10, 1997. ❖

The USABulletin Wants You

Below is our **revised** schedule for the next three issues. In order for us to continue to bring you the latest, most interesting, and useful information, please contact us with your ideas or suggestions for future issues. If there is specific information you would like us to include in the *USABs* below, please contact David Nissman at AVISC01(DNISSMAN) or (809) 773-3920. Articles, stories, or other significant issues and events should be Emailed to Wanda Morat at AEX12(BULLETIN).

November 1997	Electronic Investigative Techniques
January 1998	Special Commendations Issue
February 1998	Tax Prosecutions
April 1998	Trial Techniques