U.S. LAW ENFORCEMENT TECHNIQUES AGAINST ORGANIZED CRIME GROUPS

*Joseph K. Wheatley**

I. INTRODUCTION

Over decades of experience, the United States and other countries have acquired and developed techniques to disrupt and dismantle domestic and transnational organized crime groups. U.S. efforts against organized crime groups rely on the investigative and prosecutorial tools that were first developed in the long struggles against the Italian-American Mafia, and augmented and adapted for use against various kinds of organized crime groups. In surveying the most important law enforcement tools available to U.S. law enforcement authorities, this article will begin with three tools used by investigative agencies with the assistance and under the oversight of prosecutors: electronic surveillance, undercover operations and the use of confidential informants. Following that, this article will discuss certain tools used by U.S. federal prosecutors against organized crime groups: the Racketeer Influenced and Corrupt Organizations statute, compelled and voluntary testimony, witness protection, and financial tools such as forfeiture.

The United States Department of Justice coordinates its prosecution efforts against organized crime and gangs through the Criminal Division's Organized Crime and Gang Section ("OCGS"). OCGS is a specialized group of prosecutors charged with developing and implementing strategies to disrupt and dismantle the most significant regional, national and international gangs and organized crime groups. OCGS prosecutors work with other federal prosecutors, who are known as Assistant United States Attorneys and are located in U.S. Attorney's Offices around the country. In these cases, the investigators working with the prosecutors are drawn from local, state, and federal agencies, including the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and Homeland Security Investigations.

Federal prosecutors and agents also cooperate with their foreign counterparts to disrupt and dismantle organized crime groups. Cooperation with foreign law enforcement authorities continues to be essential to U.S. efforts against organized crime groups. This cooperation comes in various forms, such as information sharing, extraditions/expulsions, and stationing U.S. law enforcement officials in other countries. Information sharing depends on the type of information and the technique through which it was obtained. Information may be shared informally in ways that are fully consistent with the laws of the countries involved or through formal channels, such as multilateral conventions and Mutual Legal Assistance Treaty requests. U.S. law enforcement officials stationed abroad work side-by-side with their foreign counterparts to investigate crimes against United States nationals committed overseas. Where offenders are identified, these officials also work to locate, apprehend, and return the perpetrators of such crimes through extradition, expulsion or other lawful means. They also facilitate the arrest and extradition of international fugitives located in the United States and wanted abroad.

II. ELECTRONIC SURVEILLANCE

Electronic surveillance is a highly effective law enforcement tool against organized crime groups. Such surveillance may occur live and real-time or occur after-the-fact. In proving a crime, nothing is more effective than the use of the defendant's own words, as those words generally provide reliable, objective evidence of crime. Electronic surveillance also enables law enforcement agencies to learn about crimes before they occur by surveilling criminal activities, such as conspirators making plans to meet or deliver contraband, or disrupting activities, where appropriate. Such surveillance is also helpful against transnational groups

* Trial Attorney, Organized Crime and Gang Section, Criminal Division, United States Department of Justice, United States of America. The author gratefully acknowledges the extensive contributions to this paper provided by Bruce H. Ohr, Frank J. Marine, and Amy Chang Lee.

because it enables law enforcement agencies to intercept conspirators in the United States discussing future crimes with associates outside the country, which is evidence that would otherwise be difficult to obtain.

Electronic surveillance has moved beyond the more traditional telephone surveillance, oral eavesdropping devices, and video surveillance. Now, electronic surveillance also includes a variety of content and other data, including live and stored electronic communications, social media activity, computer keystrokes, and cell-site locations.

A. Stored Electronic Communications and Records

Stored electronic communications, retained by a service provider, such as e-mail or social media messages, may be obtained pursuant to search warrants under a probable cause standard, but more general information, such as subscriber records and billing records, may be obtained with only a subpoena. While not as helpful as live, real-time electronic surveillance, stored electronic communications nonetheless show the inside of organized crime groups, including their membership and leadership, structure, common purpose, continuity, and the offences that the groups commit. For instance, gangs in the United States have used social media sites, such as Facebook and Twitter, to arrange meetings, threaten rivals, issue orders to members, and plan attacks against rivals.

B. Live, Real-time Electronic Surveillance

The remainder of this section discusses live, real-time electronic surveillance. While very helpful, electronic surveillance is a sensitive tool due to privacy interests, and there are burdens of proof that the government has to satisfy to obtain permission to use the technique. The standard applied by the judge varies depending on the type of electronic surveillance sought. For pen registers, and trap and trace devices, which identify outgoing telephone calls and incoming telephone calls, respectively, the surveillance must merely be relevant and material to the investigation. However, intercepting live communications requires an even higher showing than the normal probable cause standard: there must be very little doubt in the judge's mind that the device is being used for criminal activities.

For live electronic surveillance, there are substantial restrictions on its use that are designed to protect an individual's privacy interests. For example, electronic surveillance can only be used to obtain evidence of specific serious offences that are listed in the governing statute.[1] The government must first request and receive the permission of a neutral, independent judge for the surveillance. To request and receive the authorization, a law enforcement agent must submit an affidavit to a U.S. district judge that contains specific facts establishing probable cause to believe: 1) that the subject of the surveillance is committing certain specified offences, and 2) that it is likely that evidence of such crimes will be obtained through the electronic surveillance.[2] In a requirement known as "necessity", the government must also establish that other investigative methods have been attempted and failed to obtain the desired evidence, or establish why other techniques would be unlikely to succeed or are too dangerous to attempt. U.S. Department of Justice policy also requires that the suspect has recently used the method of communication, such as the telephone or text messages that will be intercepted.

1. Wiretaps

While conducting a wiretap of a telephone, emails, text messaging or other real-time communication, the government must attempt to minimize the interception of innocent conversations by taking reasonable steps to assure that only conversations relevant to a crime are captured.[3] Thus, monitors must turn off the interception equipment when conversations stray from matters relevant to the crimes under investigation. The U.S. Department of Justice also has policies for situations when the surveillance records privileged or confidential information, such as attorney-client communications. In the event that such communications are intercepted, the recordings are immediately sealed, the judge and supervising attorney are informed and no other investigative officers may learn the content of the conversations.

Electronic surveillance also has statutory time limits. Court-authorized electronic surveillance orders are limited to thirty days, but may be extended for additional thirty-day periods as long as the requirements are

[1] *See* 18 U.S.C.A. § 2516 (West).
[2] *See* 18 U.S.C.A. § 2518 (West).
[3] *See* 18 U.S.C.A. § § 2511, 2518 (West).

met every thirty days and approved by the judge.[4] Courts have ruled that, if the surveillance is being used to aid in a good faith prosecutorial effort, the surveillance may be extended indefinitely. At the end of the electronic surveillance, the intercepted individuals must be informed of the surveillance within ninety days, unless the court authorizes delayed notification due to the government's showing that it would impair an ongoing investigation. Immediately at the end of the surveillance, the recordings must be sealed in order to preserve the integrity of the evidence.

In recent years, criminals have grown more aware of the likelihood that law enforcement is surveilling their communications, and have begun to take proactive steps to elude surveillance. This includes frequently changing telephones or using encrypted communication. In response, law enforcement officials may obtain authorization to "spin-off", which adds more telephones to the court authorizations as they become necessary to monitor the subjects. A "roving" interception is also allowed in cases where individuals frequently change their methods of communication in order to avoid detection by authorities.

One of the greatest challenges in using electronic surveillance to investigate transnational organized crime is the variety of languages that are intercepted. Real-time minimization of personal conversations is not always possible, especially when the monitoring agents are unfamiliar with the language being spoken or the participants are speaking in code. When that occurs, "after the fact" minimization is permitted by the law. In such situations, an interpreter or expert listens to the conversation as soon as is reasonably possible after the recording is made, and turns over only the relevant portions of the recording to the investigators. Privacy concerns under the U.S. Constitution are also not invoked when the parties are not American citizens and have no attachment to the United States, although interceptions may be excluded if they were not reasonable under the laws of the country in which they occurred.[5]

2. Consensual Recording

Judicial authorization is required only when neither party to the conversation has consented to make a recording. If one party makes his or her own recording, or agrees to be recorded by the government, which is known as a "consensual recording", privacy concerns are no longer implicated. Also, because prison inmates are aware that they have a diminished expectation of privacy in custody, their conversations may be recorded without obtaining an electronic surveillance order.

III. UNDERCOVER OPERATIONS

An undercover operation is another significant technique against organized crime groups, and often complements electronic surveillance efforts. Undercover operations allow law enforcement agents to infiltrate the highest levels of organized crime groups by posing as criminals while real criminals meet to discuss their plans and seek assistance in committing crimes. The scope of undercover operations varies greatly. Such operations can be short, lasting only a few hours, or quite lengthy, lasting years. They may investigate a single criminal incident, or a complex criminal enterprise that commits various crimes. The types of crimes investigated by undercover operations also vary. For instance, undercover operations may involve the purchase of contraband such as drugs, stolen property or illegal firearms, or they may involve the operation of an undercover business where criminals meet and discuss their activities with undercover officers or informers.

In such operations, agents often succeed in gaining the confidence of suspects and induce them to reveal past criminal activities or to unwittingly plot with the agents in ongoing criminal endeavours. Especially when done in conjunction with electronic surveillance, undercover operations provide comprehensive coverage of suspects' daily activities. Inherently, going undercover is a dangerous and sensitive process. It also poses the risk of luring otherwise innocent individuals into criminal activity. Accordingly, such operations require exceptional preparation and oversight.

Crucially, law enforcement officials must always protect the physical safety of the undercover agent. To prevent a premature disclosure of his or her identity, the agent is given a substantiated past history (referred

[4] *See* 18 U.S.C.A. § § 2518, 2519 (West).
[5] *See* U.S. v. Verdugo-Urquidez, 494 U.S. 259 (1990); U.S. v. Barona, 56 F.3d 1087 (9th Cir. 1995).

to as "backstopping"). Also critical are careful briefings of the target's patterns, habits and modes of operation. Before a lengthy or particularly dangerous undercover investigation may occur, the Special Agent in Charge ("SAC"), as well as the prosecutors involved, must consent. As sensitive circumstances develop in the investigation, the level of review escalates. The general concerns of approving any investigation look to: 1) the risk of injury to individuals or property, both civilian and governmental; 2) privacy concerns, particularly where an undercover operation might intrude upon privileged or confidential discussions; 3) and the risk that the undercover operative may have to participate in illegal activities. An undercover operation may not last longer than is necessary to achieve the objective nor last longer than six months, unless there is renewed authorization to proceed.

If the duration of the undercover operation is relatively brief, such as the single purchase of narcotics, a first line investigative agency supervisor and first line prosecutor must approve the activity after having been informed of all the facts of the investigation. An operation of longer duration, with an undercover agent and informant engaging in what would otherwise be ongoing violations of law, requires the approval of a higher level supervisor, such as a local lead investigative agent, and a supervisory prosecutor must be informed of all the facts before giving approval. Long-term operations are crucial to infiltrating entrenched organized crime groups that commit their illegal activity over an extended period of time.

If the situation is one of extreme sensitivity, such as a risk to innocent third parties, or if there is extensive criminal activity of a serious nature, then investigative headquarters and Justice Department prosecutors must review and approve the undercover investigation. To balance prosecutorial concerns with the safety of the undercover operative and the public, the Department of Justice created the Undercover Review Committee, composed of senior prosecutors and investigators. The Committee is responsible for reviewing, approving and controlling all sensitive undercover operations. The request for approval must be in writing, contain a full factual description of the suspected criminal activity and the participants, and adequately detail the undercover scenario, the expertise of the undercover team, the duration of the project, the foreseeable legal issues, and risks to the agents and public.

Finally, law enforcement officials must avoid, at all costs, entrapment. Entrapment is inducing a person to commit an offence that he or she otherwise would not commit. Accordingly, there are restrictions to limit undercover operations and avoid this potential entrapment mishap. Law enforcement personnel are also required to take steps to prevent violence from occurring if they learn of potential violent crimes. This may include warning a potential victim, arresting suspects who pose a threat, or ceasing an undercover investigation altogether.

IV. INFORMANTS

Another critical law enforcement technique is the use of confidential informants. In the U. S. law enforcement community, a confidential informant is someone who provides information or assistance to the authorities in return for a promise that the authorities will try to keep his or her identity confidential. Some confidential informants are willing to testify, while others are not. In the event that a confidential informant is not willing to testify, law enforcement authorities cannot absolutely guarantee the informant's confidentiality, because in relatively rare circumstances courts may decide that due process, or concerns of fundamental fairness, require that a confidential informant's identity be disclosed to a defendant charged with a crime where the informant can provide evidence that could exculpate the defendant. However, those situations are rare. In most cases, law enforcement authorities are able to keep an informant's identity confidential.

Confidential informants are typically motivated to provide information to the authorities in exchange for money or lenient treatment regarding charges pending against them or likely to be brought against them. In many cases, confidential informants are themselves engaged in criminal activities, which enables them to provide valuable direct evidence of criminal activities by their criminal associates. Confidential informants frequently provide the information that enables law enforcement officials to obtain judicial warrants authorizing electronic surveillance. Many successful prosecutions of the leadership of organized crime groups, including the Italian-American Mafia, have involved information supplied by confidential informants who provided information for many years about the leadership of the organized crime groups; indeed some of the informants have been "made members" of the Italian-American Mafia. Incriminating evidence by informants who deal directly with the leadership of organized crime groups is simply invaluable to break

through the layers of insulation that the leadership uses to conceal their activities.

However, there are significant risks associated with the use of informants. Sometimes, informants do not fully disclose their own criminal activities, or they falsely implicate their enemies in crimes, or they engage in unauthorized criminal activities. In that latter respect, under U.S. law, law enforcement authorities may authorize informants to participate in some forms of non-violent criminal behavior that would otherwise be illegal if they were not acting as informants with authority to engage in the activities. For example, depending on the circumstances, in order to protect an informant's cover and to enable him to be in a position to obtain incriminating evidence against others, informants may be authorized to participate in illegal gambling, trafficking in stolen property, and other non-violent crimes. Therefore, it is important for law enforcement authorities to closely monitor the activities of informants to minimize the danger that the informant would use his association with law enforcement to shield his own unauthorized criminal activities.

These three techniques, electronic surveillance, undercover operations, and use of informants are the most important tools that have assisted investigative agencies against domestic and transnational organized crime groups. Next, this article will discuss the tools used by U.S. federal prosecutors against organized crime groups.

V. RACKETEER INFLUENCED AND CORRUPT ORGANIZATION STATUTE

In every organized crime case, the objective is always to find and convict the highest levels of a criminal organization, in an effort to disrupt and dismantle the group. Accomplishing this goal requires special prosecutorial tools, including a statute that explicitly prohibits participation in a crime group through specified unlawful activity. The most common antiracketeering law is the Racketeer Influenced and Corrupt Organizations Statute ("RICO"), passed in 1970. RICO provides heavy penalties when a defendant conducts, or conspires to conduct, the affairs of an enterprise through a pattern of specified acts, also known as "predicate crimes." An enterprise can be anything from an ostensibly legitimate entity, such as a corporation or labour union, to a group of individuals working together to commit a crime, such as the MS-13 gang or the Italian-American Mafia.

Despite RICO's broad power, there were only a handful prosecutions against organized crime in the statute's first 15 years. The shortage of prosecutions was mainly because it took time for federal prosecutors to feel comfortable with such a complex statute to make it the focus of organized crime prosecutions. Additionally, the investigative techniques, such as electronic surveillance and undercover operations, necessary to build a convincing RICO cases, were not routinely used against organized crime bosses in the 1970's.

RICO has proven to be an effective tool in helping to prosecute organized crime in the United States. RICO's power, however, also means that there is oversight and approval for its use. To protect against potential misuse, the U.S. Department of Justice's Organized Crime and Gang Section ("OCGS") has a specialized unit of attorneys who carefully review all proposed RICO indictments for legal and factual sufficiency, which ensures that RICO is only used when necessary. Further, OCGS staffs its own prosecutors on RICO cases around the country and provides advice to other prosecutors on their RICO cases after indictment.

Disrupting and dismantling organized crime groups without RICO would be inconceivable. RICO is not used solely for organized crime cases; it has been used in official misconduct cases, against hundreds of police officers, judges, and public officials, as well as against terrorist groups, hate groups, stock manipulators, and drug cartels.

A. Basic RICO Features

It is important to note that all of RICO's original 46 predicate offences, such as murder, arson, and extortion, were criminalized well before 1970. RICO represented a significant legislative initiative because it permitted many different crimes to be charged within a single indictment. Under RICO, these different crimes could be charged in a single count against a defendant, provided that the crimes were part of the defendant's pattern of acts that related to the enterprise. Essentially, RICO criminalized participating in or conducting a business of crime.

RICO is particularly useful for organized crime cases because it allows prosecutors to detail the complete criminal activity of one person or a group of criminals. Significantly, RICO contains a reach-back provision, which allows prosecutors to demonstrate a pattern of racketeering activity. Since indictments cannot usually allege crimes that occurred more than five years prior to the date of the indictment, evidence of past criminal activity is often outside the period for which a person could be prosecuted. However, under RICO, as long as one of the predicate crimes alleged occurred within five years of when the indictment was first brought, the next previous crime in the pattern of racketeering is only required to be within ten years of the most recent crime. Similarly, the third most recent crime must have only occurred within ten years of the second act. In this fashion, the reach-back feature allows this process to extend back as long as twenty years in the past, in some cases, making RICO particularly useful in organized crime cases involving systematic criminal activity stretching across decades. RICO also allows prosecutors to present evidence of criminal activity from earlier prosecutions, which would ordinarily be prohibited due to constitutional rules against successive prosecution of the same conduct.

The reach of RICO is quite broad, as its predicate crimes cover various forms of criminal activities. Most judges would ordinarily prohibit the prosecution of such diverse crimes in a single case and seek to break it up into a series of smaller trials, especially if it involves many defendants. Splintered adjudication in this fashion, where no single jury can see the entire picture of criminal activities, generally benefits organized crime groups, as their crimes are often composed of many crimes linked by a single chain of command. Thus, effective prosecution of crime groups requires proof of many crimes in a single trial. RICO permits this, allowing the jury to see an entire pattern of crimes.

B. Extraterritorial Application of RICO

RICO is useful against transnational organized crime groups because it can reach some extraterritorial activity. Generally, statutes have been found applicable to conduct outside of the United States where inherent powers of the United States as a sovereign are threatened, or where its impact is on a substantial number of U.S. citizens. It is settled U.S. law that Congress has the authority to enforce its laws beyond the territorial boundaries of the United States when Congress expresses its intent that a particular statute has such extraterritorial application.[6]

RICO's legislative history reflects Congressional intent that the RICO statute be liberally construed to effectuate its remedial purpose. Its broad goals of eliminating organized crime and effects of organized crime warrant extraterritorial application. The language of the statute itself addresses racketeering enterprises "engaged in or the activities of which affect interstate or foreign commerce."[7] Moreover, Congress has added new offences to the list of crimes which can be predicates for RICO that clearly apply to conduct outside of the United States. These include alien smuggling violations which were added in 1994, and terrorism offences which were added in 2001. The extraterritorial application of RICO in a given case must satisfy the Principles of International Law as set for the in the Restatement of Foreign Relations, Section 402. These include the objective territorial principle, nationality of the defendant, the passive personality principle, the protective principle, and the universality principle.

VI. COMPELLED AND VOLUNTARY TESTIMONY

A. Immunity System

The ability to grant immunity to an individual allows the U.S. government to compel testimony from a reluctant witness who would otherwise invoke the Fifth Amendment privilege against compulsory self-incrimination.[8] This authority is derived from the principle that compelling its citizens to testify is one of the government's most important powers to assure effective functioning.[9] Because a witness may not refuse to comply with such a court order, the testimony, and any other information compelled by the order, cannot be used against the witness in any subsequent criminal case.

Until 1970, there were many federal immunity statutes which provided transactional immunity, which is

[6] *See* Equal Employment Opportunity Comm'n v. Arabian Am. Oil Co., 499 US, 244, 248 (1991).
[7] 18 U.S.C.A. § 1962(c) (West).
[8] *See* 18 U.S.C.A. § 6002 (West); Kastigar v. United States, 406 U.S. 441 (1972).
[9] *See* Murphy v. Waterfront Comm'n378 U.S. 52, 93 (1964) (White, J., concurring).

providing immunity to witnesses from future prosecutions as to any transactions or matters about which he or she testified. Currently, however, the federal system has replaced transactional immunity with use immunity. In 1970, Congress enacted use immunity statutes which proscribed the use in any criminal case of testimony compelled under court-ordered immunity grants. Thus, use immunity only provides protection for the witness from his or her own testimony. It does not immunize a witness from matters about which he or she testified before a grand jury. While not providing as broad coverage as transactional immunity, use immunity is nevertheless consistent with Fifth Amendment principles because it "prohibits the prosecutorial authorities from using the compelled testimony in any respect, and it therefore insures that the testimony cannot lead to the infliction of criminal penalties on the witness."[10]

Federal prosecutors, with the approval of the Attorney General, the Deputy Attorney General, or a designated Assistant Attorney General, may seek a court order granting immunity when, in the government's judgment, the testimony or other information is necessary in the public interest and the individual has asserted, or is likely to assert, his or her privilege against self-incrimination. Non-exhaustive factors in invoking the public interest include 1) the importance of the prosecution to effective enforcement of the law, 2) the value of the person's testimony, and 3) the person's relative culpability in relation to the offence being prosecuted. Finally, there is a "close family exception," in which the Department refrains from compelling the testimony of a close family relative of the defendant on trial.

B. Non-Prosecution Agreements and Cooperation Agreements

In addition to the immunity system, there is also an "agreement" system which, while not contained in the U.S. Code, is a widespread, valid practice in obtaining witnesses. There are two kinds of agreements that the government can enter into with witnesses: non-prosecution agreements and cooperation agreements.

Non-prosecution agreements are generally used when the witness plays a minor role in a crime.[11] Essentially, non-prosecution agreements grant immunity from prosecution from the case at bar in return for full, truthful cooperation. However, in practice, they are rarely used.

Cooperation agreements, meanwhile, are the most commonly-used tool to gain truthful testimony from a culpable witness. These agreements require some liability for the witness's criminal conduct; the defendant agrees to fully and truthfully cooperate, testify in any court proceeding concerning matters asked of him or her, and enter a guilty plea on other charges. In exchange for this cooperation, the government files a motion giving the judge special discretion in determining the defendant's sentence.[12] Often the sentencing judge will reduce an otherwise fixed sentence. This creates an incentive to cooperate, and often assists in prosecuting organized crime groups.

During a trial which includes a witness testifying under immunity or under a non-prosecution or cooperation agreement, the prosecutor anticipates that the lawyer who represents the accused may attack the witness's credibility. The defence attorney may try to convince the jury that the witness will say whatever the government wants him or her to say in order to receive the benefit of the deal negotiated in the cooperation agreement. To ensure credibility of these witnesses, prosecutors usually present additional evidence which corroborates the testimony of the cooperators. Documentary evidence, forensic evidence, surveillance, and the testimony of other witnesses are all used to bolster the jury's confidence in the truth of cooperator testimony.

VII. WITNESS PROTECTION

Another valuable tool that assists the government in prosecuting organized crime groups is witness protection. Because organized crime groups can often be violent, witness intimidation can pose a substantial obstacle to successful prosecution. While the Witness Security Program, discussed below, is the most famous witness protection system, police departments and federal agents also provide protection to witnesses as needed. These ad hoc witness protection services remove obstacles to testimony by witnesses that may otherwise be harmed before testifying or refuse to testify out of fear.

---

[10] *See* Kastigar, 406 U.S. at 453.
[11] U.S. Department of Justice, United States Attorney's Manual, ch. 9, § 27.600 (B)(1)(c).
[12] U.S. Sentencing Guidelines Manual, § 5K1.1 (2005).

Separately, there are other witness programs that, while not providing protection, nonetheless remove obstacles to witnesses testifying. The Emergency Witness Assistance Program ("EWAP"), for instance, provides temporary funding for threatened witnesses, including transportation, housing and moving expenses, subsistence, telephones, and child or elder care.

A. Witness Security Program

The Department of Justice created the Federal Witness Security Program in 1970. Subsequently, the Witness Security Reform Act, passed in 1984, expanded the authority of the Attorney General to provide security through relocation for witnesses in cases involving organized crime or other serious offences where a violent crime against the witness is likely to occur.

Requests for witness protection are made when it is clear that a candidate will be an essential witness, and will require relocation from the danger area. Due to the safety concerns of a witness and his or her family, a witness's participation in the Program is not disclosed unless the Department of Justice's Office of Enforcement Operations authorizes it. For a witness to be admitted into the Program, he or she must supply significant evidence in important cases, and must show that there is a perceived threat to his or her security.

Before approval for entry, the United States Marshals Service ("USMS") must conduct procedures to minimize disruption to both government agencies and witnesses. First, the USMS will interview the applicant so as to determine that the witness is essential to the prosecution, is endangered, and requires entry into the Program. The witness is also provided with an overview of the Program and what he or she can, and cannot, expect to receive through it. Next, the USMS will arrange for psychological testing and evaluation for each prospective witness and adult member of the witness's household who are also to be protected. This test will attempt to determine if the individuals will pose a safety risk to their relocation communities. Potential participants who are incarcerated are required to undergo a polygraph examination to ensure that they do not intend to harm or disclose other protected witnesses.

In order to ensure that the witness's testimony will be available at trial, it is recommended that the witness either testify before a grand jury or otherwise commit to providing the requested testimony at trial. Once in the Program, the witness and his or her family are relocated to a less dangerous area, and are given new identities and financial assistance until the witness can obtain secure employment.

Transnational organized crime groups presents a new challenge since the Witness Security Program operates only in the United States. However, aliens can be eligible for the Program following appropriate immigration authorization allowing the witness and family members to remain in the United States. Despite its costs, the Witness Security Program has proven to be effective in the prosecution of organized crime groups.

VIII. FINANCIAL TOOLS, INCLUDING FORFEITURE

A. Financial Tools

There are two primary reasons why a government may choose to follow the money and assets of organized crime groups using financial tools. First, many people commit crime for the money and assets it gives them. Accordingly, the government can catch criminals through their money and assets, by following the paper trails and digital trails left by the criminal networks. Once the government has found the money and assets, it can forfeit the money and the assets, and provide restitution to any victims. Second, money also helps pay for more crimes. By cutting off the flow of money and forfeiting it, the government can help prevent future crimes from being committed.

Financial tools can help many different kinds of investigations. Financial tools are not only used for investigations of financial crimes, such as money laundering and fraud. For instance, financial tools can also be used to investigate organized crime groups, violent crimes, human trafficking/smuggling, narcotics, child exploitation, terrorism, cybercrime, and public corruption.

There are different kinds of kinds of financial information that government investigators can obtain, including:

1) Ordinary records from financial institutions, such as records about checks, credit cards, savings, loans, investments, and safe deposit boxes.

2) Due diligence records, also known as "Know Your Customer" records. These are account opening records and account monitoring records that financial institutions maintain about their customers, such as corporate history, signature cards, references, and taxes.

3) Records that financial institutions are required by law to create and maintain, such as Currency Transaction Reports ("CTRs") and Suspicious Activity Reports ("SARs").

4) Electronic fund transfers, including international wire transfers through SWIFT.

5) Nonbank financial records, such as hawala and hundi.

In most countries, including the United States, domestic financial information is available through legal process, such as subpoenas or court orders. In some countries, domestic financial records are available to government investigators automatically, without the need for legal process. There are different ways to obtain foreign financial information, including:

1) Treaty requests, which are official requests for information through bilateral Mutual Legal Assistance Treaties or international legal conventions.

2) Law enforcement agency contacts, in which a government's law enforcement agency requests and obtains information from a law enforcement agency in another country.

3) Requests through the Egmont Group.

The Egmont Group is composed of government Financial Intelligence Units ("FIUs") from more than 150 countries. The Egmont Group focuses on fighting money laundering, terrorist financing, and other financial crimes. It is open to new member countries, at www.egmontgroup.org/membership. The Egmont Group helps member states share financial information with each other.

B. Forfeiture

With the exception of organized crime groups that commit violence for the sake of power and dominance, such as certain gangs, organized crime groups are primarily motivated by material gain. Therefore, it is essential to take the profit out of crime. Strong forfeiture laws aid in that mission. Forfeiture is a criminal penalty for many offences in the United States.

Generally speaking, upon conviction for an offence that carries forfeiture as a penalty, a defendant may be ordered to forfeit all profits or proceeds derived from the criminal activity, any property, real or personnel, involved in the offence, or property traceable to the offence such as property acquired with proceeds of criminal activity. For example, if a defendant uses a residence or car to distribute drugs, that property is subject to forfeiture. Thus, a convicted defendant may be ordered to forfeit all proceeds of his or her criminal activity including money and other forms of property.

In addition to criminal forfeiture, civil forfeiture laws also allow the government to obtain property used in criminal activities. The principal difference between criminal and civil forfeiture is that criminal forfeiture is limited to a convicted defendant's personal interest in property subject to forfeiture, whereas civil forfeiture focuses on the property itself.

For example, suppose a defendant repeatedly used a house to sell drugs, but he did not have an ownership interest in the house. If he is convicted of drug dealing, that house is not subject to criminal forfeiture because the defendant did not own the house. However, a civil forfeiture law suit could be brought against the house itself as a defendant, even if the owner of the house was not engaged in criminal activity. The house, nonetheless, is subject to civil forfeiture because it was repeatedly used to facilitate criminal activities, and the owner did not take adequate steps to prevent his house from being used for criminal activities. There are various defenses to such civil forfeiture, such as the "innocent owner defense", but those are beyond the scope

of this article.

Criminal and civil forfeiture laws are powerful weapons in the prosecutor's arsenal to take the profit out of crime.

IX. CONCLUSION

Organized crime groups operate all over the world, whether they take the shape of the Mafia, gangs, cybercrime groups, or a variety of other forms. Likewise, they pose a variety of dangers, including murders, child exploitation, human trafficking, robbery, frauds, narcotics, identity theft, and extortion. In recent years, these dangers have been amplified by advances in technology and globalization. Capitalizing on these advances, organized crime groups communicate faster, hide their money in more locations, travel more cheaply, and may conceal their activities through encryption. The tools discussed in this article are essential to the U.S. government's efforts against such organized crime groups. Electronic surveillance, undercover operations, informants, RICO, compelled and cooperating witness testimony, witness protection, and financial tools such as forfeiture all help the U.S. government pierce the secretive and violent world of organized crime groups and bring those groups to justice.