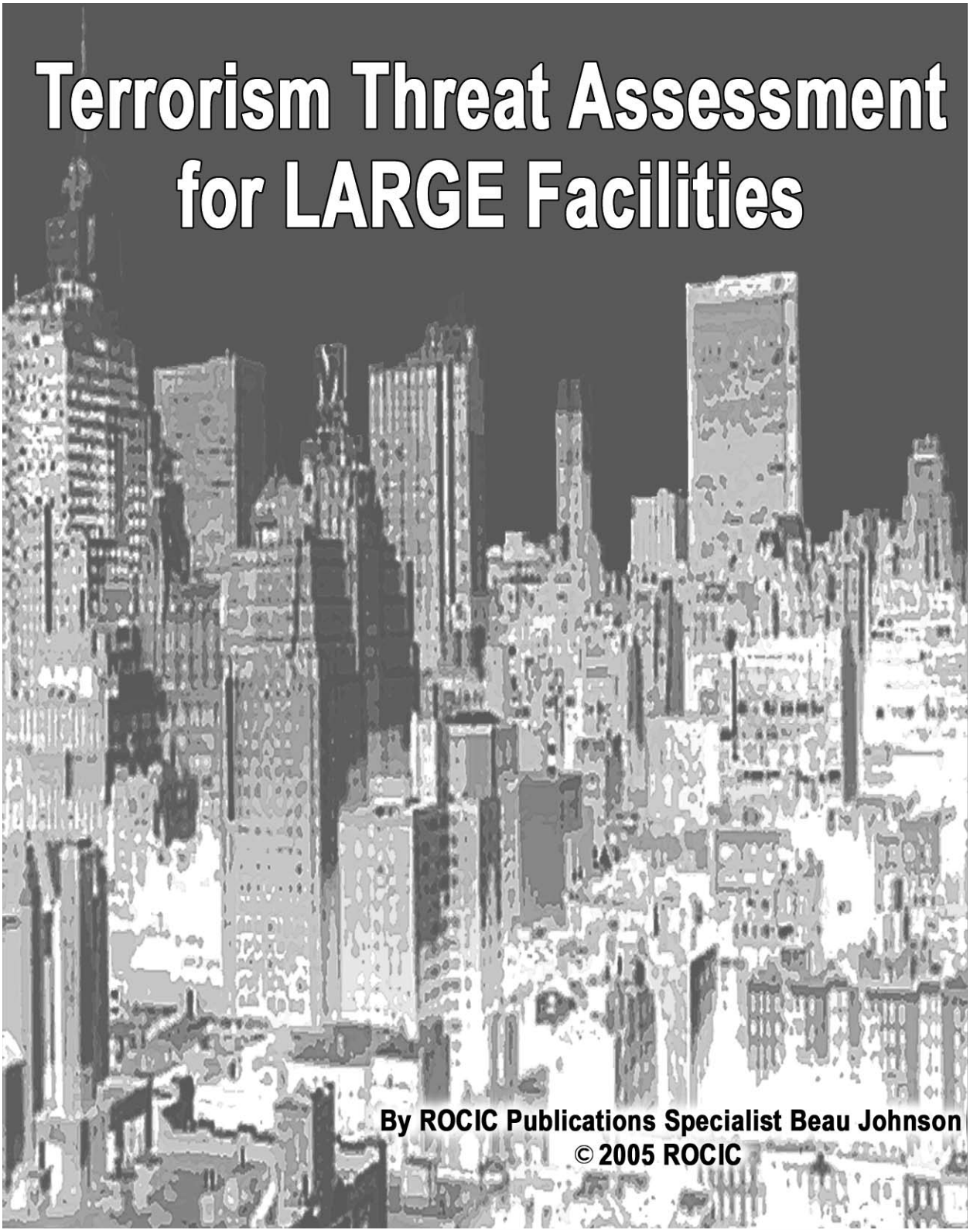
Regional Organized Crime Information Center

SPECIAL RESEARCH REPORT

Terrorism Threat Assessment for LARGE Facilities



By ROCIC Publications Specialist Beau Johnson

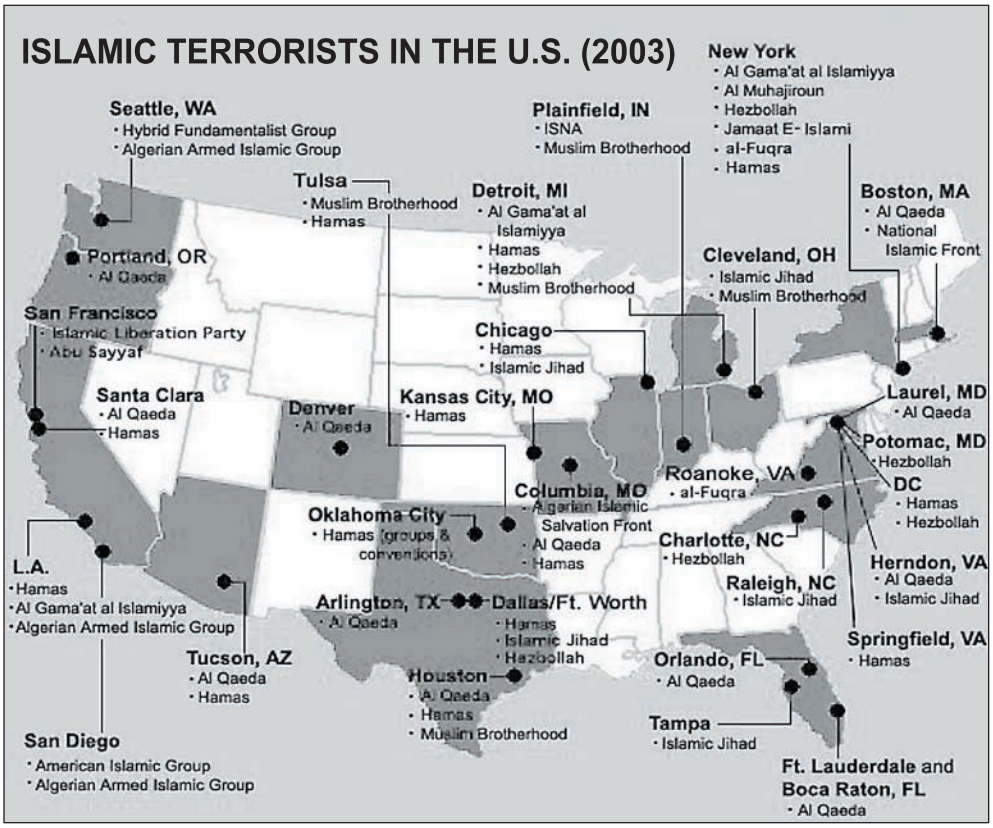
BJA Bureau of Justice Assistance
Office of Justice Programs - U.S. Dept. of Justice

The war on terror is an upward spiral of offense versus defense, with new threats continually under analysis and defensive weaknesses evaluated and reinforced. This process of strengthening vulnerabilities is a burden that falls largely on the shoulders of the law enforcement community. Police and security officers are charged with the tasks of exposing/prosecuting enemies, protecting structural targets, protecting the population, and enhancing security, as well as helping the population to protect themselves and their assets.

In other parts of the world, the terror threat may be more ominous and more easily defined. Palestinian radicals attempting to infiltrate Israel in the hopes of suicide bombing a bus or cafe is disconcerting, but largely different than current domestic concerns in the United States.

Perhaps the primary difference between foreign lands and the United States is that the U.S. is largely an open society, free of restrictions on speech, religion, and way of life, and those freedoms are largely reflected in our structural designs. There are very few visible barriers, i.e., walls, bars, barricades, separating citizens from a destination (or terrorist from a target) because to a U.S. citizen, such barriers would give the impression of a police state. So, it is up to law enforcement, the military, and security forces to compensate for those physical separations with greater alertness and enhanced technology to perceive, prevent, and prosecute terrorists.

Terrorism exists in a variety of forms and with many different goals. Additionally, a terrorist is difficult to profile and may come from a variety of backgrounds. There is no one type of terrorism method and no one type of terrorist. The U.S. faces threats from both domestic and international terrorists, with political, religious, and/or economic motivations. Many international groups are currently operating on U.S. soil. Law enforcement officers must try to understand terrorist goals and recognize security vulnerabilities before they become an avenue to a terror attack.



Map of known Islamic terrorist sleeper cells in the United States as of 2003.

From American Jihad by Steven Emerson

HIGH-LIKELIHOOD TARGETS

Government and military buildings are a prime target of terrorists because they are a direct extension of the United States' infrastructure that they hope to topple. The most noted attacks in U.S. history are the 1995 bombing of the Murrah Federal Building in Oklahoma City, OK and the 2001 attack on the Pentagon.

As a result of the Oklahoma City bombing and the Sept. 11, 2001 attacks, security was greatly enhanced around federal buildings and airports. The result is that terrorists are tending to attack softer targets, such as businesses, with greater frequency. According to the U.S. Department of State, attacks on business buildings accounted for 61 of 208 worldwide attacks in 2003, more than three times the number of attacks on government and military structures combined. Also, this trend rings overwhelmingly true in attacks on the U.S. In 2000, 86.4 percent of U.S. targets were businesses.

Hotels are at particular risk simply because their function is to house people (potential casualties). Hotels also are not difficult for terrorists to gain access to, as regulating patrons' entry would harm their business. The recent coordinated suicide bombings of three hotels in Amman, Jordan on Nov. 9, 2005 (written in the Arab world as 9/11), which killed 67 people and wounded more than 150, are indicative of hotel vulnerabilities.

The aftermath of the 1995 Oklahoma City bombing

Damage from Jordan hotel suicide bombing

The vest that failed to detonate in Jordan was slim and packed with ball bearings.

Schools appeal to terrorists as targets because of the emotional trauma that would be wrought by an attack on children. While most schools now have security measures in place to guard against shootings such as the Columbine, Colorado incident, most are relatively unguarded against larger terrorist strikes.

The most heinous school attack in recent history was an elementary school in Beslan, Russia during its first autumn-term day by a group of primarily Chechen terrorists. A three-day siege ended with the deaths of 344 civilians, 186 of them children. The terrorists were well armed with automatic weapons, rocket-propelled grenades, and improvised explosive devices (IEDs). They wired the gym, where the hostages were kept, and other parts of the school with explosives.

Obviously terrorists would love to carry out an attack on a stadium, conference, mass-transit sys-

tem, or other large-scale gathering to inflict massive casualties. Security measures for this sort of venue were already stringent, but have increased exponentially since the 9/11 attacks. Police and security officials must always be alert and assess all possible vulnerabilities in order to intervene in a terror plot, as terrorist methods change constantly, and security always has weaknesses to be guarded against.

Terrorists in Beslan, Russia packed hostages into the school's gym and wired it with explosives.

The gym at the Beslan shool after the explosions occurred.

EXPLOSIVES

Explosives are by far the preferred method for terror attacks. Of the total of 208 attacks worldwide in 2003, 134 were various types of bombings. This proportion is even higher in the U.S. due to a lack of other terror tactics such as armed attacks and political kidnappings.

Explosives are chosen by terrorists for several reasons: they are low risk but highly dramatic; low cost but high-yielding; components are readily available; few skills are needed; there are a variety of delivery options; large groups are not necessary; and forensic evidence is difficult to locate.

There are three types of explosions: chemical, mechanical, and nuclear. Detonations yield not only heat and fire, but also fragmentation—deadly flying debris; and extreme amounts of pressure, often strong enough to kill a person within proximity.

For a large explosive, there is a three-stage train consisting of an initiator, a booster, and a main charge. These elements increase in sensitivity. The initiator is very sensitive and thus easy to ignite, which then ignites the less sensitive but higher-energy booster, which ignites the insensitive and high-energy main charge.

Detonators and propellants, the respective second and third links in this chain, can be identified by trained police officers. Detonators typically have the appearance of a smaller metal or plastic shell and often a fuse is visible. Propellants can be anything from fertilizer-type bags to sticks of dynamite to large plastic-wrapped tubes. Five billion pounds of explosives are purchased each year in the U.S., most being ammonium nitrate, which is

An assortment of detonators

A variety of explosive materials

infamous for its use in the Oklahoma City bombing. However, it is rarely used in terror bombings; black powder is used in the majority of incidents. Other explosives include various forms of dynamite, commercial explosives, improvised varieties, pipe bombs, and military explosives.

Improvised explosives (fabricated using information from underground publications or the Internet) are usually more sensitive than other explosives and should be treated with a special degree of care. But officers should never handle an explosive or suspected explosive if it can be avoided at all. Extreme caution should be taken even in the inspection of what may be an explosive, as they are sensitive not only to fire and heat but also to vibrations coming from voices, radio waves, and footsteps. For example, an officer finding what appears to be old, leaky dynamite in a barn or warehouse would not want to use a radio near it, nor approach it for fear of vibrations in the ground setting off an explosion. When there is suspicion of an explosive, an officer should summon the bomb squad and clear the threatened area.

Tubes of dynamite

Tubes of explosive emulsions are a common propellant.

There are three types of explosive delivery methods. Type I is a package, such as a backpack, briefcase, or musical instrument. These can be easily placed and difficult to locate and can usually hold one to 11 pounds of explosives.

Type II deliveries, person-borne, are used by individuals planning a suicide bombing. The perpetrator's appearance is usually disguised to accommodate the explosive (which can be very slim), and not attract attention that could ruin a mission's success.

Vehicle bombs are the third type of delivery method. Vehicles usually hold 40 to 70 pounds of explosives or more.

BOMB THREATS

Bomb threats must be carefully evaluated from many different angles to determine the right course of action. Most bomb threats are simply that—a threat with no factual basis, but with so much at risk, one can't be too cautious. It is logical to have a plan in place to handle a bomb threat before one is received.

The first thing to consider is the type of facility under the threat. There is a vast difference in the number and type of possible casualties and access opportunities at a shopping mall versus a courthouse, for example. Officers need to know who a credible threat might come from and why, and where security might be lax.

Terrorists, former or current employees, the mentally disturbed, and children are the primary groups that make bomb threats. They do so for many different reasons, and if the identity of the threat maker can be ascertained, that information is very valuable to decision makers. Of course the frequency of threats and history will determine with what degree of seriousness authorities approach them. School children may make a threat in order to miss school, and employees may do so to get out of work for a while. A facility should evaluate their contingency plans to determine whether they encourage false threats. Terrorists usually hope to inflict as many casualties as possible, so a threat is illogical (it warns potential

victims) unless it lures responders in as targets or takes advantage of known evacuation routes. For example, if a high school facing a threat always evacuated to their stadium for a half-hour to allow any necessary procedures, not only would that plan offer students incentive for making a threat, but it would also concentrate potential casualties into a smaller area for a simpler, more effective terror strike.

A facility can best be prepared for bomb threats with measures such as a caller ID system; personnel ID system; package control system; strict control of keys and locks; and sufficient perimeter barriers and lighting.

Factors of motive, security, and possible consequences need to be weighed when determining whether an evacuation is necessary at all, and if so, whether it should be a full evacuation or partial evacuation. The likely size of a planted bomb would indicate its destructive limits and whether it could affect a large part of a facility or generate many casualties. All things considered, people may be safer staying inside a threatened structure.

If a threat is credible, police and bomb squads should be contacted immediately. Outside of their searches, searches by those who occupy a threatened area are most effective, but for them to search themselves means they must be informed of the threat, and thus there may be risk of panic.

One of the major difficulties in preventing a terror attack, especially a suicide bombing, is that it needs to be stopped in the planning phases (phase 1-6 in sidebar). Other crimes, such as robberies, are usually interdicted after the action has taken place. In the case of an attack, that point is much too late. Law enforcement must be on guard more than ever before, to perceive the threat while still in its planning stages for a successful intervention.

Any business or facility is a potential terrorist target. An area's threat level should be evaluated by what is known statistically, factually, and historically. For a suicide bombing, any area with a sizable crowd makes for a target. The concept of facility/ event security is simple: the more that is known about the potential target, the enemy, and the environment, the more possible it will be to avoid or evade an attack.

Prior to an attack, a terrorist will commence surveillance against a target with the goal of gathering information to assess vulnerabilities. The length of this process may vary widely. During this step in the attack process, the terrorist will be looking to exploit weaknesses in the access control measures of the facility, including physical barriers and procedural protocols. Physical security is exactly what it sounds like—locks, fences, bars, landscaping, shutters, dogs, etc. Procedural security features include any system put in place to enhance security, like alarms, lighting, identification-required access, cameras/closed-circuit television, guard or police presence, search dogs, etc.

The Nine Phases of a Suicide Attack

1. Identify potential targets
2. Recruit bomber(s)
3. Train bomber(s)
4. Target selection recon
5. Purchase materials
6. Construct device
7. Final preparation
8. Move to target
9. Detonate

SURVEILLANCE

Surveillance takes time, and puts offenders under threat of being noticed, thus identified and arrested. Surveillance detection is by facility security to determine if surveillance is being conducted in the area. This practice is of great importance because it keeps a structure's security watchful and gives a defender an opportunity to notice an observer's mistakes. An attacker doesn't mind being seen, but doesn't want to be noticed or remembered. Their location for surveillance must provide them with cover and concealment and be of tactical advantage.

There are many considerations when determining

whether surveillance is occurring. Anyone near the area should have a profile that matches their signature, i.e., what they look like they should be doing should match what they are doing. For example, a tourist will likely not be alone or taking pictures of government buildings, and a delivery truck would be making frequent stops, not be parked for long periods. Opportunities for surveillance to keep in mind would include parked vehicles (they could contain a camera), restaurants or parks near targets where attackers could easily sit and observe, and street vendors, among others. Every target will have a unique set of variables that can be exploited by those conducting surveillance. Officers must identify these variables.

Would-be attackers may give themselves away in various ways. A signature not matching a profile is one way. Others include an observer signaling, checking the time, or making a phone call when a security-related occurrence happens. Attackers will likely make themselves scarce at the pass of a traffic officer or security vehicle. Any repetition of movement or the same individual being sighted again and again for no apparent reason is a cause for concern. Attackers conducting surveillance are defeated by knowledge that they may be watched themselves.

Behavioral Indicators of Suicide Bombers

1. Threats
2. Anger, anxiety, fear
3. Shaking and/or sweating
4. Photos or surveillance of potential target
5. Indulgence in "worldly sins" that directly violate their religion
6. A trance-like state
7. Pale skin under a newly shaven beard
8. Clothing that could conceal a bomb
9. Uttering chants, shouting a religious phrase, or reaching upwards with the arms (likely indicates an imminent explosion)

Critical Infrastructure

- Agriculture
- Banking/finance
- Chemical and hazardous waste
- Defense industrial base
- Energy
- Emergency Services
- Food
- Government
- Information and telecommunications
- Transportation
- Postal and shipping services
- Public health
- Water

Key Assets

- National monuments and icons
- Nuclear power plants
- Dams
- Government facilities
- Commercial assets

Natural surveillance is defined as maximized visibility by design. It is a great advantage to a facility's defense because it allows anyone to notice suspicious activity. The more likely a criminal is to be under observation, the less likely they are to pose a threat.

Natural surveillance increases the risk for potential attackers by keeping them under observation more often. Strategies for increasing natural surveillance at a site might include maximizing the number of windows; having a very visible main entrance; raising the tree canopy level and minimizing landscaping brush; lighting access points, sidewalks, etc. well; and any other method suited to the potential target to make would-be attackers more visible.

The more changing elements there are in a facility's security plan, the more difficult it will be for a terrorist to carry out a successful attack. Terrorists thrive on knowing schedules and routines, so variation is key to combating them.

Sources

1. Col. Joel Leson. *Assessing and Managing the Terrorism Threat*. U.S. Dept. of Justice, Bureau of Justice Assistance.

2. Armor Group International Training Inc. *ITI Student Reference Handbook.* 2005.

3. The Virginia Crime Prevention Association. *Terrorism Threat Level Evaluation*. 2003.

4. The Virginia Crime Prevention Association. *CPTED and the Threat Assessment Process*. 2003.

5. Shaun Kelley. Arlington Co., VA Fire Department Assistant Chief and Building Official.

6. U.S. Department of State. “Patterns of Global Terrorism” www.state.gov. 2001-2004.

7. Steven Emerson. *American Jihad*. Free Press, 2002.

Special Research Reports by ROCIC Publications

Accessible to RISS member agencies on the ROCIC secure Intranet website. Complete listing of ROCIC Bulletins, Special Research Reports, User's Guides, and Training Conference Reports at http://rocic.riss.net/publications.htm

- Terrorism Threat Assessment for Large Facilities
- Check 21: New Banking Technology Challenges Law Enforcement
- ICE: Crystal Methamphetamine: Imported High-Purity Meth Replacing Domestic Lab Output
- Meth Lab Safety Issues: How to Protect Law Enforcement, First Responders, and the General Public from the Dangers of Clandestine Methamphetamine Labs
- CERT (Community Emergency Response Team): Civilian Support for First Responders
- Taxing Illegal Drugs: States Attacking Profit Motive of Dealers
- Diplomatic Immunity: Rules of Engagement for Law Enforcement
- Violence Against Law Enforcement: Law Enforcement Officers Murdered, Accidentally Killed, Assaulted in the Line of Duty
- Mara Salvatrucha (MS-13): Violent Street Gang with Military Background
- Indicators of Terrorist Activity: Stopping the Next Attack in the Planning Stages
- Internet Fraud: Techniques Used to Scam Online Consumers
- DXM: Teens Abusing Cough Medicine Risk Brain Damage, Death
- RISS Activity Report for G-8 Summit
- Mail Center Security
- Safety & Security for Electrical Infrastructure: Protecting Law Enforcement and the Public in Emergency Situations
- Crisis Response Report: Terrorist Attacks & Natural Disasters
- Eco Terrorism: Extremists Pose Domestic Threat
- Cold Case Units: Turning up the Heat
- Gypsies and Travelers
- User's Guide to ATIX: Automated Trusted Information Exchange
- DNA: Law Enforcement's New Investigative Tool
- False ID: National Security Threat
- Salvia Divinorum: Herbal Hallucinogen Raises Law Enforcement Concerns
- Smallpox: The Deadly Virus
- Human Trafficking: International Criminal Trade in Modern Slavery
- Network Security: Safeguarding Systems Against the Latest Threats
- Dirty Bombs: Radiological Dispersion Devices
- Ethics in Law Enforcement
- Law Enforcement Officers and Safety
- Computer Forensics: Following the Electronic Trail
- Huffing: Teens Abusing Inhalants
- RISSLeads Bulletin Board: Information in an Instant
- Bioterrorism
- Criminal Intelligence: Its Use in Law Enforcement in Our Changing World
- Terrorism: Defending the Homeland
- Law Enforcement and the Mentally Ill
- Civil Disorder: Preparing for the Worst
- Ecstasy: Harmless Party Drug Or Dangerous Trend?
- Heroin: More Purity For Less Money
- OxyContin Abuse Explodes In Southeast
- Just Say NO To Telemarketers
- School Security Crisis Response Manual
- XML: Communications Through Connectivity
- Credit Card Security Features
- Stop Phone Cramming: Check Your Phone Bill
- Shaken Baby Syndrome: What To Look For, What To Do
- Children and Internet Safety
- ROCIC's Illicit Drug Pricing: A Regional Comparison
- RAVES: When It's More Than A Party
- Identity Theft: From Low Tech to High Tech
- Hoaxes and Legends: How to Detect Hoaxes on the Internet
- Truce or Consequences: Motorcycle Gangs Talking to Each Other
- Child Pornography: Protecting the Innocent
- Meth Threat: Seizure of Labs by Untrained Personnel Recipe for Death and Destruction
- Illusion and Confusion: The Crime and Culture of Irish Travelers
- Date Rape Drugs: Rohypnol, GHB Gaining Popularity in Southeast, Southwest
- Security Threat Groups in Prison

ROCIC has been serving its criminal justice members since 1973, and served as the prototype for the modern RISS (Regional Information Sharing Systems) Centers.

ROCIC serves more than 180,000 sworn personnel in 1,727 criminal justice agencies located in 14 southeastern and southwestern states, Puerto Rico, and the U.S. Virgin Islands.

ROCIC provides a variety of services, free of charge, to its criminal justice member agencies:

- Centralized law enforcement databases with connectivity among law enforcement agencies and the RISS Centers using the RISS Nationwide Intelligence Network.
- Analytical processing of criminal intelligence, including phone tolls and document sorts
- Loaning of specialized, high-tech surveillance equipment and vehicles
- Publications, including criminal intelligence bulletin
- Specialized training and membership & information exchange
- Use of investigative funds
- On-site personal assistance by law enforcement coordinators