Table of Contents

Countdown Begins for New UCR Data Collections and Initiatives Coming January 1

America's oldest time series of crime data is undergoing a great transformation. On January 1, a number of new and updated data collection and processing initiatives will move the FBI's Uniform Crime Reporting (UCR) Program closer to providing a better look at the scope and nature of crime in our nation. For the past few years, technical information specialists, analysts, statistical assistants, and other members of the UCR Redevelopment Program (UCRRP) team have been developing the standards by which law enforcement agencies can submit new, more detailed data. They have also been setting into motion better ways for the Bureau to process them. Together, these changes will make UCR more relevant to current issues and concerns and, in general, more efficient. Highlights of these changes include the following.

Human Trafficking Offenses and Arrests—In response to the *William Wilberforce Trafficking Victims Protection Reauthorization Act*, the UCR Program will collect data on human trafficking in two categories: commercial sex acts and involuntary servitude. Human trafficking/commercial sex acts and human trafficking/involuntary servitude will be Part I offenses in the Summary Reporting System (SRS) and Group A offenses in the National Incident-Based Reporting System (NIBRS). The offenses will be defined the same in both collection methods. In addition, another prostitution offense, purchasing prostitution, was added.

New Bias Categories of Gender and Gender Identity—With these two new categories, four new bias types were added to the FBI's hate crime data collection as a result of the *Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act*. Under the new bias category of Gender, Anti-Male and Anti-Female were included. Under the new bias category of Gender Identity, Anti-Transgender and Anti-Gender Non-Conforming were added. Under the bias category of Sexual Orientation, the category Anti-Homosexual was revised to Anti-Lesbian, Gay, Bisexual, or Transgender (Mixed Group). Both victim and offender collections were modified to account for bias-motivated crimes directed toward and perpetrated by juveniles in accordance with the Act.

New Rape Definition—Following the CJIS Advisory Policy Board's recommendations as approved by Director Robert S. Mueller, III, the UCR Program revised its definition of rape to include all victims (not just female victims as was the case in the SRS) and omit the requirement of physical force. In the SRS, rape is now defined as "Penetration, no matter how slight, of the vagina or anus with any body part or object, or oral penetration by a sex organ of another

person, without the consent of the victim." (The NIBRS sex offenses already capture the broader sex offense information reflected in the new SRS definition.) The term *forcible* has also been dropped from all sex offenses in both the SRS and NIBRS.

Updated Race and Ethnicity Collection Categories—To comply with the race and ethnicity designations specified by the U.S. Office of Management and Budget and to better reflect the changing composition of America, the UCR Program will now collect five race categories and two revised ethnicity categories. The race categories are White, Black or African American, American Indian or Alaska Native, Asian, and Native Hawaiian or Other Pacific Islander. The ethnicity categories are Hispanic or Latino, and Not Hispanic or Latino. These designations apply to all facets of the UCR Program in which race and ethnicity are captured for victims, offenders, arrestees, and racial bias types. These include the SRS, NIBRS, Law Enforcement Officers Killed and Assaulted (LEOKA), hate crime, cargo theft, and human trafficking data collections.

Although the FBI's national UCR Program will begin accepting the new, more detailed data beginning January 1, not all local, county, state, tribal, and federal agencies are necessarily equipped to report the modified records. The FBI anticipates a number of agencies will continue to make the required changes in the months to come.

In addition to expanding the UCR Program's data collection, the UCRRP aims to improve the overall methods by which the FBI accepts, processes, checks, and publishes data. For starters, the UCR Program is getting a new, more efficient system capable of relating and storing more data than ever before. To help streamline the submission process, the UCR Program will stop accepting paper submissions and Portable Document Format files in 2013 (except for agencies that have established a transition plan for a brief extension). This automation will include internal data quality checks sooner and enable staff to supply results back to contributors faster. Ultimately, the program will be able to provide a more timely, detailed, and relevant snapshot of crime in our nation that will help law enforcement in the allocation of resources.

Agencies with questions concerning these pending system changes should contact their state UCR Program managers or the UCR Program's Crime Statistics Management Unit by e-mail at cjis_comm@leo.gov or by telephone at (304) 625-4830.

UCR: More Than Meets the Eye

It takes the combined efforts of thousands of law enforcement agencies reporting data on the crimes brought to their attention before a news anchor says "New numbers released by the FBI report that the level of crime is on the move…." In its administrative role of the Uniform Crime Reporting (UCR) Program, the FBI collects, verifies, publishes, and audits crime data. The program's primary objective is to generate sound, useful information for law enforcement administration, operation, and management. Although the Summary Reporting System (SRS)—the traditional counting of eight violent and property crime offenses—represents UCR to most people, it is just one of two ways that agencies submit their offense and arrest data, as well as some of their data concerning law enforcement officers killed and assaulted. The other way agencies submit data is through the National Incident-Based Reporting System (NIBRS), which uses up to 58 data elements to collect details about incidents, offenses, and law enforcement officers killed and assaulted. NIBRS submissions also include data on other facets of UCR such as hate crime, cargo theft, and (beginning January 1) human trafficking. Agencies that report their offense and arrest data via the SRS must make separate electronic submissions for those other facets of data.

For more information about the UCR Program visit http://www.fbi.gov/about-us/cjis/ucr.

Image-Based Matching Technology Offers Identification and Intelligence Prospects

The FBI's Integrated Automated Fingerprint Identification System (IAFIS)—the largest criminal biometric database in the world—is steadily making way for the Next Generation Identification (NGI), which will extend automated biometric identification capabilities beyond fingerprints and palmprints. Although law enforcement has used photographs of scars, marks, and tattoos (SMTs) for several years to help identify or eliminate suspects, the NGI will automate that process. In 2014, investigators will be able to query the NGI with descriptive data about tattoos to find images of potential matches of SMTs associated with individuals' records. Equally notable, however, is that right now, the FBI's Biometric Center of Excellence (BCOE) and its partners are advancing image-matching technology that will enable investigators to use a probe, or query image—with *or without* descriptive data such as key words or characters—and find similar images.

The BCOE, headquartered at the Criminal Justice Information Services (CJIS) Division in Clarksburg, West Virginia, is the FBI's focal point for biometrics and identity management. It is an initiative of the Science and Technology Branch, which includes the Laboratory Division, the Operational Technology Division, and the CJIS Division. Together, scientists, technicians, and biometric experts from these divisions are supporting the BCOE's mission to "foster collaboration, improve information sharing, and advance the adoption of optimal biometric and identity management solutions within the FBI and across the law enforcement and national security communities." In short, the BCOE is exploring new and existing biometric modalities, or types, and maximizing their potentials.

With image-based matching technology, the BCOE's goal is to avoid the subjectivity inherent in text-based searches by using computer algorithms to search the features of other stored images and locate a potential match. An example of the subjectivity involved in labeling images, even when using the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) standards for classifying an image's class and subclass, follows.

When looking at the image shown above, some users might see the letter "D" in this image and label its ANSI/NIST class/sub-class as "Other/Wording." Other users might consider the image a logo for the Detroit Tigers and label it as "Symbol/Miscellaneous Symbol," based on what they think it represents. Still others, due to the image's orientation, might interpret the image as a face and label it as "Human/Abstract Face." Computerized labeling, or indexing, increases the likelihood of finding similar images.

The BCOE's academic partnership with Michigan State University facilitated the development of the TattooID prototype for the automated retrieval, indexing, and matching of SMTs. To use the TattooID prototype, an analyst enters a probe image, key words, or characters into the program that employs an image-matching algorithm. The algorithm runs against images stored in the database and provides any similar images, ranked with match scores. Such a search can be run for images of the same general design, or it can be limited to include only those images of tattoos on designated body areas, e.g., a person's shoulder. Although search results do not provide positive identifications at this point, they could help narrow a suspect list.

The BCOE recently finished building a tattoo dataset to test and evaluate the image-matching algorithms in the TattooID prototype. The testing will cover four basic scenarios: (1) tattoos from the same individual captured at different booking events; (2) similar tattoos on different individuals; (3) region of interest (matching small portions of an image to the larger image); and (4) matching across various media (drawings, stencils, photographs, etc.). To build the collection of images for testing, examiners analyzed tattoo images from the FBI Photo File and labeled the images according to ANSI/NIST classification standards. Furthermore, examiners ranked the similarities of images within the same class/sub-class, e.g., animal/bird. Once testing is completed, the BCOE will evaluate the prototype's performance and assess strengths and weaknesses of the current capability.

While the value of image-to-image matching technology is obvious from an identification perspective, the benefits of knowing the symbolism and background behind tattoos and graffiti can be equally valuable. From an intelligence standpoint, certain symbols or graffiti may be used to help establish whether an individual is associated with a particular gang, terrorist organization, or extremist group. This may help determine the extent to which the individual or gang poses a threat to law enforcement or the community, and possibly to recognize and link crimes across the country. This helps secure the safety of officers during investigations and arrests, and it can even possibly help with crime intervention strategies.

Applying its research with image-based matching technology with a bend toward relating the meaning of symbols, the BCOE recently collaborated with the Cryptanalysis and Racketeering Records Unit (CRRU) of the FBI's Laboratory Division on the development of the prototype

image-comparison system, Tattoo and Graffiti Image-Matching and Graphic Evaluation (TAG-IMAGE). This investigative tool was designed to help the CRRU match images within its database and to determine the significance of tattoos, graffiti, or other cryptic symbols for FBI investigative programs dealing with foreign or domestic terrorism, violent crime, or gangs. Rather than using metadata or text searches, TAG-IMAGE uses advanced image-to-image technology to match symbols based on actual appearances. It may also provide raw information on a symbol's actual use, rather than leaving speculation as to its meaning or origin.

With TAG-IMAGE, a contributor e-mails an image to the CRRU, where an analyst enters the probe image into the system, which compares it with images stored within the CRRU database. Once a search is completed, a CRRU analyst e-mails a response to the contributor that includes pictures of similar images as well as any associated details and contact information. The submitted image then becomes available for future comparisons by other agencies. The CRRU has begun a pilot program using the TAG-IMAGE prototype. After the pilot phase ends, TAG-IMAGE will become available to local, state, tribal, and federal law enforcement and correctional agencies.

The BCOE also plans to conduct a small operational pilot program with the National Gang Intelligence Center to assess the feasibility of image-based matching and to gain user feedback. Ultimately, the BCOE hopes to use this biometric research to enhance FBI operations.

Does your agency have a success story involving tattoos, symbols, or graffiti? If so, the BCOE would like to hear about it. Tell us your story by including a point of contact, agency name, name of database, and a brief description of how the tattoo, symbol, graffiti, or image of any of these helped to identify or eliminate a candidate, or how it provided information that aided an investigation. Send your e-mail to biometriccoe@leo.gov.

Law Enforcement Online Enterprise Portal Makes Access More Convenient

For more than 17 years, the Law Enforcement Online (LEO) system has been providing free, secure, Web-based communications to the law enforcement community. Over the years, LEO has continuously grown and modified to meet changing law enforcement requirements. In October 2012, LEO access was transformed with a "rehost" project that modernized both hardware and software and migrated LEO capabilities to the LEO Enterprise Portal (LEO-EP).

The new LEO-EP uses single sign-on technology. That means users can log on to one authorized Identity Provider (such as a state or local police network) and automatically gain access to the LEO-EP homepage. The page is personalized for each user and includes links to "portals" for the services the user is authorized to access via LEO, such as the Law Enforcement National Data Exchange (N-DEx), Joint Automated Booking System (JABS), or the Internet Crime Complaint Center (IC3).

The LEO program continues to work with its partners to add new services and link criminal justice customers to useful tools. Services currently available to authorized users via the LEO-EP include:

- **Regional Information Sharing System (RISS)—**A system that provides timely access to a variety of criminal intelligence databases.
- **Intelink—**A secure portal for integrated intelligence dissemination and collaboration efforts.
- **N-DEx—**A powerful, investigative tool that provides law enforcement agencies with the ability to search, link, analyze, and share criminal justice information.
- **JABS—**A repository of federal arrest information.
- **IC3—**A vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime.
- **National Gang Intelligence Center—**A multi-agency effort that integrates gang information from local, state, and federal law enforcement entities to serve as a centralized intelligence resource for gang information and analytical support.
- **US DOJ IDEA my FX—**A Web-based capability that allows files/folders to be securely transferred among cross-organizational teams.

All of LEO's original services are still available by clicking on the LEO icon in the LEO-EP. Some of these services include:

- E-mail
- News Highlights
- E-Learning
- Virtual Office
- Virtual Command Centers
- Special Interest Groups
- Forums
- Library

For now, new users still need to sign up for a LEO account to access the LEO services on the LEO-EP. However, work is underway to make LEO services available to all LEO-EP users, even those who do not have a LEO account. Users will be able to use their organization-based e-mail addresses making LEO e-mail optional.

The LEO-EP allows users to personalize their homepages with their most-used services.

For more information about the advantages of the LEO-EP, how to become an Identity Provider, or simply to sign up to use the services, contact the CJIS Division's LEO Program via e-mail at leoportal@leo.gov.

BUSTED…With an Assist from MC3 and RISC

Major Case Contact Center (MC3) takes tip that leads to abductor's arrest

FBI, Mobile (Alabama) Division and Ohio Authorities ★ At 6:45 p.m. on September 18, the National Instant Criminal Background Check System (NICS) activated the Major Case Contact Center (MC3) at the request of the FBI Mobile Division to assist with a child abduction case. Around 1 p.m. the day before, a 15-year-old girl was abducted from a medical center in Dothan, Alabama. Officials believed the abductor and his family traveled out of state with the victim. At 9:21 p.m. on September 21, the MC3 received a call advising that the abductor and his family had just shown up in Ohio. Immediately, the MC3 representative notified the Mobile Division, which worked with other law enforcement authorities to locate the 15-year-old girl. The abductors were arrested without incident.

Search of RISC leads to arrests of pair, including man wanted for cocaine smuggling

Ontario (California) Police Department ★ On November 2, an officer with the Ontario (CA) Police Department pulled over a vehicle because the driver was following the vehicle ahead of him too closely. Both the driver and passenger provided the officer with identification (ID) from Mexico; however, no records were found when the officer ran the names and dates of birth through the National Crime Information Center. Suspecting the IDs were forged, the officer ran the fingerprints of the driver on a rapid mobile ID device for a search of the FBI's Repository for Individuals of Special Concern (RISC) and the local Automated Fingerprint Identification System. Although the local system did not return a hit on the driver's biometrics, the RISC returned a "red" hit on them for cocaine smuggling from Missouri. After a "red" hit was found on the local system for the passenger, both men were arrested.

Need to Know

UCR State Program Bulletin and UCR Newsletter Available on the LEO

Law enforcement agencies that contribute data to the Uniform Crime Reporting (UCR) Program through a state program can access current and past editions of the UCR *State Program Bulletin* on the LEO Intranet at https://www.leo.gov/http://leowcs.leopriv.gov/legis/cjis/programs/crime_statistics/state_program_bulletins/state_program_bulletins.htm

Direct contributors can access current and past editions of the UCR Newsletter on the LEO Intranet at https://www.leo.gov/http://leowcs.leopriv.gov/lesig/cjis/programs/crime_statistics/newsletters/newsletters.htm.
Users with questions concerning access to the LEO should contact the LEO Operations Unit by telephone at (304) 625-5555.

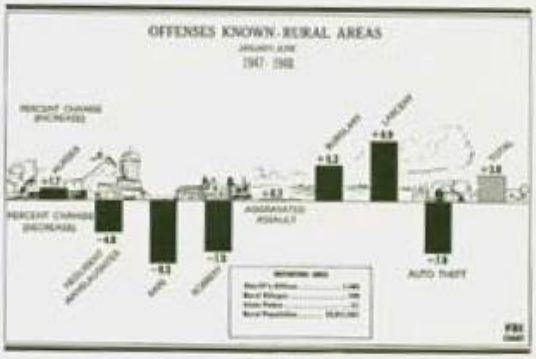
Stay Linked

Sign up for Your Alert Today!

Available exclusively online, *The CJIS Link* provides information about system enhancements, training opportunities, policy changes, and successes to CJIS system users across the law enforcement, national security, and intelligence communities. Be sure to visit www.fbi.gov/about-us/cjis to sign up for e-mail alerts that let you know when new editions become available.

To share your feedback, success stories, and article suggestions to make this newsletter even better, e-mail *The CJIS Link* staff at cjis_comm@leo.gov. Please be sure to put "CJIS Link" in the subject line.

Uniform Crime Reports:
Vintage to Virtual



public in useful and interesting ways. The vintage illustrations on this page show how crime was presented to the public in the 1940s. Today, UCR is available online as electronic publications at http://www.fbi.gov/about-us/cjis/ucr. With the upcoming UCR revitialization, scheduled for unveiling in 2013, even more data will be presented in a flexible, modern, and timely format. Get ready for UCR to enter the 21st century with a virtual splash!

PHOTO finish