



UCR Program

Criminal Justice Information Services Division

Quarterly

Program News

JANUARY 2024

Section 1— Message to Program Participants

- Two new data collections launched January 13
- Data deadlines for 20246
- Timetable for releases of 2023 data.....7
- The Crime Data Explorer has two new features9
- CJIS APB recommendations from 2022 and 2023.....10
- Hate Crime Statistics Data Collection updates20
- Hate Crime Symposium.....20
- Quality Assurance Team formed.....21
- Infographics are available on LEEP.....22
- UCR Program now using a single telephone number and
single e-mail address23
- Check out the *CJIS Link* for the latest information on CJIS Division services
and programs.....23
- Electronic availability of the *UCR Program Quarterly*23

Section 2— Clarification to Policies and Procedures

- Two-year schedule for documentation updates.....24
- Trainer Talk.....25

Section 3— On the Audit Trail

Quality Assurance Review now the NIBRS Audit Program26

Auditors’ top findings from 2022 and early 2023.....27

NIBRS Team’s audit schedule for 2024.....30

Reminders regarding the proper use of the automatic weapon indicator and proper classification of cargo theft30

STATE PROGRAM MANAGERS ARE ENCOURAGED TO SHARE THE INFORMATION IN THIS DOCUMENT WITH THEIR LOCAL AGENCIES.

Section 1 – Message to Program Participants

Two new data collections launched January 1

On Monday, January 1, 2024, the FBI's Uniform Crime Reporting (UCR) Program began accepting data for two new data collections—the Law Enforcement Public Contact (LEPC) Data Collection and the Lawful Access Data Collection.

Law Enforcement Public Contact Data Collection

Representatives from several federal, state, local, and tribal law enforcement agencies across the nation, as well as the major law enforcement organizations, requested that the FBI develop and manage a national collection regarding law enforcement uses of force. During the subsequent development of the National Use-of-Force Data Collection, law enforcement leaders communicated that it was critically important to place use-of-force incidents in the context of the total number of law enforcement interactions with the public.



In response to this request, the FBI's UCR Program deployed a pilot project for the LEPC Data Collection in fall 2020 and launched the data collection on January 1, 2024. Therefore, agencies may now begin submitting annual counts for 2023.

The LEPC Data Collection collects the number of law enforcement contacts with the public in three categories:

- ❖ Citizen calls for service*
- ❖ Unit/officer-initiated contact
- ❖ Court/bailiff activities

*Note that the term *citizen* refers to any member of the general public.

Upon submitting the number of contacts for each of the three categories above, law enforcement can indicate what each number is based on:

- ❖ Actual records
- ❖ An estimated count
- ❖ The number of contacts with the public are not applicable
- ❖ The number of contacts with the public are unavailable

A law enforcement public contact is an incident or occurrence where a law enforcement officer is called to respond to a scene by a citizen(s) or initiates an activity which results in contact with a citizen(s). This count does not include the total number of people encountered at the incident or occurrence.

Agencies are not expected to create a data system to obtain this information. Instead, agencies are encouraged to use their computer-aided dispatch systems or other existing systems to obtain counts for law enforcement contacts with the public that fit into the listed categories.

All law enforcement agencies are eligible to participate in the LEPC Data Collection. The LEPC is housed on the Collection of Law Enforcement and Crime Tool (COLECT) platform that is accessible via the Law Enforcement Enterprise Portal (LEEP).

Agencies can use one of three methods to submit annual LEPC data:

- ❖ The LEPC Submission Page of COLECT in LEEP
- ❖ A flat file with a technical specification for bulk submission
- ❖ A web service option for bulk submission

LEPC data will be released on the Crime Data Explorer (CDE) and can be used to put context to the Use-of-Force Data Collection and the Law Enforcement Officers Killed and Assaulted (LEOKA) Data Collection.

Agencies with questions about the LEPC Data Collection should contact the FBI's UCR staff at UCR@fbi.gov.

Lawful Access Data Collection

The increased use of strong encryption inhibits law enforcement's ability to lawfully access data on electronic devices and platforms in connection with criminal and national security investigations. In response to law enforcement's description of these challenges to lawmakers, Congress routinely requests quantitative assessments of the issue. However, a nationally representative count of how many times encryption of an electronic device impedes a law enforcement investigation does not currently exist.



In collaboration with representatives from various law enforcement agencies and organizations throughout the nation, the FBI and Lawful Access Focus Group developed the framework for the scope, data elements, and reporting requirements of the Lawful Access Data Collection.

The goal of the data collection is to provide the law enforcement community with a method to quantify how often investigations are impacted by encrypted applications, devices, and software to better understand the impact of encryption on law enforcement investigations and provide valuable data to decision-makers to help mitigate these lawful access impacts.

The law enforcement and national security communities face challenges due to a phenomenon referred to as “warrant-proof encryption,” which is evidence or data vital to an ongoing investigation that cannot be accessed by criminal investigators, even when granted a lawful court order or warrant. An encounter with encryption for UCR purposes occurs when law enforcement seizes an encrypted device or a device with encrypted applications or software that impacts an investigation.

By contributing to the Lawful Access Data Collection, the law enforcement community can demonstrate its commitment to better data and assist in tracking the volume of affected investigations. Launched on January 1, the collection tracks the volume from law enforcement agencies, fusion centers, criminal forensic science and regional computer forensic laboratories, and other investigative agencies.

Data contributors may begin submitting incident information in the Lawful Access Data Collection centralized repository via COLECT, which is located within LEEP.

An informational flyer about the data collection is available on the UCR Community of Interest on JusticeConnect and, upon request, FBI staff can provide demonstrations for data submitters. For additional information, contact UCR@fbi.gov.

Data deadlines for 2024

Federal agencies and state UCR Program managers should note the following deadlines for the FBI's Crime and Law Enforcement Statistics Unit (CLESU) to receive data. State Program managers should also inform their local agencies of these deadlines.

All federal agencies and state UCR Programs must submit data by the established deadlines for their data to be included in releases. Data received after the deadlines will not be released in the current year's annual reports(s) or respective quarterly reports beginning with Quarter 1 data for 2024; however, it could be included in the CDE, which will be updated before the next release cycle.

Date	Information needed
January 31, 2024	The deadline for agencies to submit their 2023 police employee data (as of October 31, 2023) to the FBI.
February 5, 2024	The data submission deadline for inclusion in the <i>Quarterly Uniform Crime Report (Q4), January-December, 2023</i> .
February 12, 2024	The data submission deadline for inclusion in the <i>National Use-of-Force Data Collection Annual Report 2023</i> .
April 1, 2024	The data submission deadline for inclusion in: <ul style="list-style-type: none">❖ <i>Crime in the United States, 2023</i>❖ <i>NIBRS, 2023</i>❖ <i>NIBRS Estimates, 2023</i>❖ <i>Law Enforcement Officers Killed and Assaulted, 2023</i>❖ <i>Hate Crime Statistics, 2023</i>

Date	Information needed
April 15, 2024	The data submission deadline for inclusion in the <i>National Use-of-Force Data Collection Update, March 2024</i> .
May 6, 2024	The data submission deadline for inclusion in the <i>Quarterly Uniform Crime Report (Q1), January-March, 2024</i> .
July 15, 2024	The data submission deadline for inclusion in the <i>National Use-of-Force Data Collection Update, June 2024</i> .
August 5, 2024	The data submission deadline for inclusion in the <i>Quarterly Uniform Crime Report (Q2), January-June, 2024</i> .
October 7, 2024	The data submission deadline for inclusion in the <i>Quarterly Uniform Crime Report, (Q3), January-September, 2024</i> .
October 15, 2024	The data submission deadline for inclusion in the <i>National Use-of-Force Data Collection Update, September 2024</i> .
December 31, 2024	The deadline for making changes to an agency's current reporting status, name or address, or for adding new contributing agencies.

Timetable for releases of 2023 data

All 2023 data releases will appear exclusively on the CDE along with other data released for 2020 and later. Historical documents released for 2019 and earlier will continue to be available on the FBI's website at www.fbi.gov. Agencies are reminded that the data in the quarterly data releases are preliminary and are subject to change in subsequent releases.

Annual crime data releases

Name of data release	Tentative timeframe of data release
<i>Crime in the United States, 2023</i>	Fall 2024
<i>Hate Crime Statistics, 2023</i>	Fall 2024
<i>NIBRS, 2023</i>	Fall 2024
<i>NIBRS Estimates, 2023</i>	Fall 2024
<i>LEOKA, 2023</i>	Fall 2024

Quarterly Uniform Crime Report releases

Name of data release	Tentative date of data release
<i>Quarterly Uniform Crime Report (Q4), January-December, 2023</i>	March 2024
<i>Quarterly Uniform Crime Report (Q1), January-March, 2024</i>	June 2024
<i>Quarterly Uniform Crime Report (Q2), January-June, 2024</i>	September 2024
<i>Quarterly Uniform Crime Report (Q3), January-September, 2024</i>	December 2024

National Use-of-Force Data Collection releases

Name of data release	Tentative date of data release
<i>National Use-of-Force Data Collection Annual Report 2023</i>	March 2024
<i>National Use-of-Force Data Collection Update, March 2024</i>	June 2024
<i>National Use-of-Force Data Collection Update, June 2024</i>	September 2024
<i>National Use-of-Force Data Collection Update, September 2024</i>	December 2024

The Crime Data Explorer has two new features

The CDE has two new features: the Data Discovery Tool and the Special Reports area.

The Data Discovery Tool, which is accessible at <https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/explorer/crime/query>, allows users to customize the crime data they are looking for. Users can select desired timeframes, location levels (nation, state, or local law enforcement agencies), and offenses. The tool was added to the CDE in August 2023.

In addition, the Special Reports page area was created in October 2023 as a place for users to access special publications concerning UCR data. The link is accessible at <https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/home> and then clicking on the Special Reports tab.

The inaugural Special Reports area features the 37-page *UCR Summary of Crime in the Nation, 2022*, which contains a synopsis of UCR data for 2022.

Crime in the Nation, 2022, is comprised of the following components:

- ❖ *Crime in the United States, 2022*
- ❖ *NIBRS (National Incident-Based Reporting System), 2022*
- ❖ *NIBRS Estimates, 2022*
- ❖ *Hate Crime Statistics, 2022*
- ❖ *Law Enforcement Officers Killed and Assaulted, 2022*

Crime in the Nation, 2022, includes data from 15,724 agencies that represent 83.3 percent of agencies actively enrolled in the UCR Program and cover 93.5 percent of the nation's population.

Each component of *Crime in the Nation* provides multiple distinct tables that furnish details on various facets of crime and law enforcement data submitted to the UCR Program. Each component is available on the Documents & Downloads area of the CDE at <https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/downloads>.

CJIS APB recommendations from 2022 and 2023

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) had a productive 2022 and 2023 with meetings in June and December 2022 and in June and November 2023. Please note that modifications the APB recommended require approval from the FBI Director prior to implementation. The FBI Director has approved these recommendations. Although approved, changes may not be reflected in the next release of UCR documents. CJIS Division staff are incorporating them as quickly as possible.

June 2022

In its Cleveland meeting on June 8-9, 2022, the CJIS APB recommended multiple measures concerning the UCR Program. These measures included:

- ❖ Expanding the law enforcement officer victim type in NIBRS
- ❖ Clarifying the weapon type of *deadly disease* in NIBRS
- ❖ Modifying the forms used to report the felonious killings and accidental deaths of law enforcement officers
- ❖ Expanding the rules for agencies to collect stolen or recovered vehicle information in NIBRS
- ❖ Adding drone information in NIBRS

Expanding the law enforcement officer victim type in NIBRS

Currently, if a law enforcement officer is the victim of a crime, data contributors are limited to using the victim type of L = Law Enforcement Officer to the NIBRS offenses of 09A = Murder and Nonnegligent Manslaughter, 13A = Aggravated Assault, 13B = Simple Assault, and 13C = Intimidation. However, law enforcement officers are often victims of other crimes against persons and the crime against property of robbery.

This forces data contributors to choose between reporting the most accurate NIBRS offense or the most accurate victim type.

Examples of law enforcement officers being victims of assault with a lesser included offense are:

Rape—An undercover officer is compromised by a confidential informant, and as a result, is raped by members of the gang the officer infiltrated.

Fondling—A suspect gropes an officer's private body parts while the officer attempts to place the suspect under arrest.

Robbery—An offender takes a law enforcement officer's weapon.

Currently, agencies report these scenarios in one of two ways. The agency can report the most accurate NIBRS offense, but the agency must report the victim type as I = Individual because none of those offenses accept the victim type of L = Law Enforcement Officer. Or the agency can report the offenses using the victim type of L = Law Enforcement Officer but is limited to reporting the offense as assault, which is not as accurate in these cases.

Examples of law enforcement officers being victims of crimes against persons other than 09A, 13A, 13B, or 13C include:

Kidnapping/Abduction—A gang abducts an on-duty police officer and drives the officer to a secluded area.

Human Trafficking—During a sting operation, a police officer is portrayed as a minor and is solicited or coerced into participating in a commercial sex act.

Negligent Manslaughter—A drunk driver veers off the road, striking and killing an officer conducting a traffic stop.

In these cases, agencies may report the appropriate offense, but must use the victim code of I = Individual. If an agency tries to report a victim code of L = Law Enforcement Officer with an offense code of 09B (Negligent Manslaughter), the incident will receive an error code of 482 - *(Type of Victim) cannot be L = Law Enforcement Officer unless Data Element 24 (Victim Connected to UCR Offense Code) is one of the following: 09A = Murder & Nonnegligent Manslaughter 13A = Aggravated Assault 13B = Simple Assault 13C = Intimidation.*

Currently, the structure of reporting law enforcement officers as victims is limiting and does not provide a true picture of how often police are crime victims. Also, if an agency opts to report the most accurate NIBRS offense when assault is a lesser included offense, data about law enforcement officers killed and assaulted is lost.

The CJIS APB recommended that the victim type of L = Law Enforcement Officer be expanded to include all crimes against persons and robbery.

Clarifying the weapon type of *deadly disease* in NIBRS

Currently, guidance does not exist to assist NIBRS data contributors on reporting a weapon type of *deadly disease*. A weapon type of *deadly disease* may be present in cases when the offender is aware he or she is infected with a deadly disease and deliberately exposes or attempts to expose another to the disease by biting, spitting, etc.

Examples include an offender who deliberately coughs and spits while threatening to infect another person with a deadly disease or an offender raping an individual and knowingly infecting the victim with a deadly disease.

NIBRS data contributors are directed to report a weapon type of *deadly disease* as data value 90 = Other in Data Element 13 (Type Weapon/Force Involved). This guidance had been documented in the August 2000 *NIBRS Volume 1: Data Collection Guidelines* manual stating: “90 = Other (any weapon or force, including [deadly/dangerous/communicable diseases], not fitting the above specifically coded weapons/force).”

However, the 2023.0 edition of the *NIBRS User Manual*, dated June 30, 2023, states “90 = Other (BB guns, pellet guns, Tasers, pepper spray, stun guns, etc.)” on page 94 and does not include disease as an example for data value 90 = Other for Data Element 13 (Type Weapon/Force Involved).

The APB recommended to change the list of examples in data value 90 = Other for Data Element 13 (Type Weapon/Force Involved) to include the words “deadly/dangerous/communicable diseases.”

Expanding the rules for agencies to collect stolen or recovered vehicle information in NIBRS

Currently, the use of Data Element 18 (Number of Stolen Motor Vehicles) and Data Element 19 (Number of Recovered Motor Vehicles) is limited solely to the offense of 240 = Motor Vehicle Theft. Therefore, when data is requested on the number of stolen motor vehicles, only the number of stolen and recovered motor vehicles reported with

the offense code of 240 = Motor Vehicle Theft. These totals do not take into consideration the number of motor vehicles stolen or recovered from robbery (carjacking), burglary (vehicles stolen from within the burglarized structure), fraud (vehicles acquired through deceit), and embezzlement (vehicles that have been entrusted to someone's care and are stolen). Because these totals do not include motor vehicles stolen through the other offenses, they do not accurately represent these thefts. In addition, researchers may not know that stolen motor vehicles are not counted when stolen through other offenses.

The APB moved to accept Option 1: Allow stolen and recovered motor vehicles to be reported in Data Element 18 = Number of Stolen Motor Vehicles and Data Element 19 = Number of Recovered Motor Vehicles, respectively, for the offenses of 240 = Motor Vehicle Theft, 120 = Robbery, 220 = Burglary, 26A = False Pretenses/Swindle/Confidence Game, 26B = Credit Card Fraud, 26C = Impersonation, 26E = Wire Fraud, 26F = Identity Theft, 26G = Computer Hacking/Invasion, and 270 = Embezzlement.

Adding drone information in NIBRS

In May 2021, staff with the UCR Program met with other FBI units and federal agencies to discuss a possible consolidated solution between law enforcement agencies across the nation into a centralized place to capture data on drone/unmanned aircraft systems (UAS) incidents.

During the meeting, participants furnished background on the increasing number of instances of drones being used to commit crimes, including to harass individuals and damage property. Currently, there is no centralized location to track criminal incidents involving drone/UAS incidents; participants discussed the possibility of collecting this information in NIBRS.

Because the task of adding a new numbered offense in NIBRS can be complicated and burdensome to law enforcement agencies, it was suggested that a data value be added to a current data element in NIBRS to capture if a drone/UAS was involved in an incident.

The CJIS APB voted to create a new data value, R = Drone/Unmanned Aircraft System to Data Element 8 (Offender Suspected of Using) with options of Y = Yes or N = No within the new data value. The UCR Program began collecting this data in 2023.

December 2022

The CJIS APB met December 7-8, 2022, in Oklahoma City, Oklahoma, and recommended two modifications to UCR data:

- ❖ Capturing firearm information in Data Element 14 (Type Property Loss/Etc.) and the ability to report property information for all NIBRS offenses
- ❖ Modifying several definitions used within the LEOKA data collection

Capturing firearm information in Data Element 14 (Type Property Loss/Etc.) and the ability to report property information for all NIBRS offenses

Agencies complete Data Element 14 (Type Property Loss/Etc.) as part of the property segment of an incident. The property segment is used to describe the type, value, and (for drugs and narcotics seized in drug cases) quantity of property involved in an incident. Historically, the property segment has been submitted only for kidnapping/abduction, crimes against property, drug/narcotic offenses, and gambling offenses. However, the law enforcement community is concerned that restraining agencies in terms of what can be submitted is limiting the view of crime in the nation. The concern has to do with the inability to quantify when weapons, specifically firearms, are seized for offenses other than those currently permitted within NIBRS.

Law enforcement agencies can report the data value 6 = Seized in Data Element 14 (Type Property Loss/Etc.) for the offenses of:

250 = Counterfeiting/Forgery

35A = Drug/Narcotic Violations

35B = Drug Equipment Violations

39A = Betting/Wagering

39B = Operating/Promoting/Assisting Gambling

39C = Gambling Equipment

39D = Sports Tampering

521 = Violation of National Firearms Act of 1934*

522 = Weapons of Mass Destruction*

526 = Explosives*

58A = Import Violations*

58B = Export Violations*

61A = Federal Liquor Violations*

61B = Federal Tobacco Violations*

620 = Wildlife Trafficking*

*Denotes offenses for federal and tribal law enforcement agencies reporting only.

The UCR Program is examining whether some established NIBRS business rules should be relaxed or removed to allow for a more robust view of crime in the United States. Relaxing the NIBRS business rules governing the reporting of property offenses can allow for additional context to be reported with all offenses. This allows a law enforcement agency that reports property for any offense within its record management system to submit data to the UCR Program without having to remove information from its system before submitting data via NIBRS.

Also, relaxing the business rules to allow for the reporting of property with violent offenses can give flexibility to determine the extent of the presence of firearms when an offense occurs. This will not provide a national picture of how often a firearm is used in the commission of an incident, but it will provide insight into the number of times a firearm was seized.

However, any modifications to NIBRS business rules affects both the UCR Program and data contributors. Modifying business rules not only impacts the rules that were modified but has a ripple effect of affecting business rules associated with other NIBRS segments, offenses, and data elements.

The CJIS APB recommended that the FBI relax the business rules surrounding the reporting of property so that agencies can report property information for all NIBRS offenses.

Modifications to LEOKA Data Collection Definitions

Currently, line-of-duty assault data is reported exclusively via NIBRS using Data Elements 25A (Type of Officer Activity/Circumstance), 26B (Officer Assignment Type), and 25C (Officer-ORI Other Jurisdiction).

Data Element 25A (Type of Officer Activity/Circumstance) provides an option to report an ambush, but the category of ambush does not have an option to report the unprovoked attack of an officer. Incident details surrounding an assault by an unprovoked attack do not contain the granularity advantageous for data collection and the enhancement of officer training.

Currently, ambush (entrapment/premeditation) is defined as “Situation in which an unsuspecting officer was targeted or lured into danger as the result of an offender’s conscious consideration and planning,” and unprovoked attack is defined as “An attack on an officer not prompted by official contact at the time of the incident between the officer and offender.”

However, ambush and unprovoked attack are often not mutually exclusive, and elements of both can be incorporated within the same incident in which an officer is killed or assaulted. An officer may be attacked without warning as part of a premeditated or a spontaneous attack by the offender. Both spontaneous and premeditated actions are considered by the public, the law enforcement community, and media representatives to be potential variables within an ambush situation.

To address this, at its June 2022 meeting, the APB recommended changing the LEOKA Collection Tool 1-701 for Felonious Killings to include stand-alone questions pinpointing unprovoked attack and ambush from other circumstance options. In addition, the Beyond 2021 LEOKA Task Force has endorsed further breaking down the ambush circumstance to include two subcategories—premeditated attack and unprovoked attack—and including updated definitions for ambush and unprovoked attack.

The recommended updates are:

Ambush—Situation in which an officer is intentionally killed without warning during a premeditated or unprovoked attack in which the offender who has not yet engaged with the officer executes the attack.

Premeditated attack (entrapment)—Situation in which an unsuspecting officer was targeted or lured into danger as a result of an offender’s conscious consideration and planning.

Unknown Planning of Attack (spontaneous)—An attack on an officer that was spontaneous in nature, with insufficient facts indicating planning by the offender.

This change requires modifications to the LEOKA Collection Tool 1-701 for Felonious Killings, updates to NIBRS business rules and processes, updates to NIBRS documentation, and updates to the FBI’s training curriculum and audit process.

To remain compliant with NIBRS standards, data contributors will need to modify their systems within 2 years of the release of updated documentation.

In addition, in 2005, the following definitions for felonious killing and accidental death were provided in the LEOKA publication:

- ❖ A felonious killing is an incident type in which the willful and intentional actions of an offender results in the fatal injury of an officer who is performing his or her official duties.
- ❖ An accidental death is an incident type in which an officer was fatally injured as a result of an accident or negligence that occurred while the officer was acting in an official capacity. Due to the hazardous nature of the law enforcement profession, deaths of law enforcement officers are considered accidental if the cause of death is found not to be a willful and intentional act of murder.

For a killing to be categorized as felonious under existing definitions, a law enforcement officer must have suffered a fatal injury, as the result of both a willful and intentional action of the offender while the officer was performing his or her official duties. However, for a killing to be accidental, it must be shown that an officer acting in his or her official capacity was fatally injured due to an accidental or negligent act.

As an example, when a law enforcement officer dies as a result of an intoxicated driver’s choice to operate a vehicle, there must exist a willful and intentional action by the offender to harm the officer for the killing to be classified as a felonious killing. According to the current LEOKA classifications, the offense of driving under the

influence is not an intentional action; rather, it is a reckless or negligent act. Therefore, such an incident falls within the definition of accidental death.

However, the use of these definitions has resulted in continued subjectivity and inconsistency surrounding the classification of line-of-duty deaths of law enforcement officers. The Beyond 2021 LEOKA Task Force recommended that agencies use classification options more in line with NIBRS since assault details of law enforcement officers are now captured exclusively via NIBRS.

The Beyond 2021 LEOKA Task Force has recommended classification options for line-of-duty deaths be modified to provide a more objective framework for classification of incidents. The modifications would minimize subjectivity resulting from inconsistent interpretations of felonious killing and accidental death definitions. This provides the granularity needed to enhance officer safety, ensure consistency between submitting agencies, and support the use of common language among the UCR Program's data collections.

The task force recommended creating two subcategories within the category of felonious killing to include incidents involving murder and nonnegligent manslaughter and incidents of negligent manslaughter. The categories are:

Felonious killing—An incident type in which the willful, intentional, or unlawful actions of an offender results in the fatal injury of an officer who is performing his or her official duties.

Murder and nonnegligent manslaughter—The willful (nonnegligent) killing of a law enforcement officer by another individual.

Negligent manslaughter—The killing of a law enforcement officer through another person's gross negligence.

Accidental death—An incident type in which an officer dies due to an accident while the officer was acting in an official capacity. An accident is an incident in which was not voluntary, intended, expected, or foreseeable.

Members of the task force assert that including negligent manslaughter will provide an option for the reporting of line-of-duty deaths in which an agency cannot initially or definitively establish the offender's intent or when an investigation is pending but may

reveal the offender's willfulness and intent to kill an officer once the investigation is completed.

By including both murder and nonnegligent manslaughter and negligent manslaughter as subcategories within felonious killings, the law enforcement agency would complete incident details via the LEOKA Collection Tool 1-701 for Felonious Killings. This modification provides the granular details useful for training and analysis in situations such as an officer's death resulting from an intoxicated driver or when an offender kills an officer while using force when attempting to flee. This minimizes ambiguity and postponement of reporting incident details until the completion of any type of investigation, as each manslaughter subcategory constitutes a felonious killing classification and prompts completion of the LEOKA Collection Tool 1-701 for Felonious Killings.

June 2023

At its meeting in June 2023 in Glendale, Arizona, the APB recommended additional refinements to the LEOKA Collection Tool 1-701 for Felonious Killings.

These refinements include condensing the information from five sections into four sections: Preliminary Information, Victim Officer, Incident Details, and Offender. In addition, the collection tool will include the victim officer's name and date of birth. Because the inclusion of such personally identifiable information (PII) in LEOKA supports multiple programs, the FBI needs to continue collecting that data to mitigate any potential data gaps. Incorporating this PII in the LEOKA Data Collection Tool allows the LEOKA Data Collection to employ technical solutions that will automate current manual processes and increase operational efficiencies.

Also, in its efforts to focus on officer safety, the FBI has an initiative to increase the number of records in the Violent Person File (VPF) of the National Crime Information Center (NCIC) System. Records in the VPF warn law enforcement officers that a subject they are encountering may have a propensity of violence against law enforcement. In coordination with the NCIC Operations and Policy Unit at the CJIS Division, at the request of the agency, the FBI will extract fields from the LEOKA Data Collection Tool and put that information into a record in the VPF on the agency's behalf. The FBI will modify the LEOKA Data Collection Tool to reflect this initiative. Although the FBI would create the initial entry at the agency's request, the agency will be responsible for all subsequent record maintenance such as second-party checks, validation

requirements, packing the record, and maintaining documentation to support the entry of the individual's information in the VPF.

November 2023

During the November 2023 meeting in Savannah, Georgia, the APB opted to make no changes affecting the UCR Program.

Hate Crime Statistics Data Collection updates

Hate Crime Statistics Task Force

The Hate Crime Statistics Task Force held its first in-person meeting on June 6, 2023, during the CJIS APB meeting in Glendale, Arizona.

The task force created an action item to be voted on by the APB achieving recognition of hate crime awareness week. In June 2023, the APB recommended to memorialize an annual week dedicated to combatting hate crime across the nation through information sharing beginning in 2023. The event name will be forthcoming and will relate to sharing information on hate crime.

The task force will be working on a best practices document for reporting, exploring data values, and producing a marketing video to assist in explaining the purpose of hate crime statistics and encouraging participation.

Hate Crime Symposium

The CJIS Division hosted a NIBRS Train-the-Trainer and Hate Crime Symposium, August 8-10, 2023, at the CJIS Division in Clarksburg, WV. The agenda included opening remarks, keynote addresses, instructional presentations, hands-on break-out sessions, and informational booths.

The attendees included state-level NIBRS trainers, State Program Managers, Department of Justice (DOJ) representatives, FBI Headquarters staff, FBI Criminal Investigations Division, FBI Pittsburgh Field Office, FBI's CJIS Division, Hate Crime Statistics Task Force members, law enforcement agencies, and representatives from the top ten most-in-population nontransitioned NIBRS agencies.

The symposium facilitated networking, collaboration, and exchange of ideas with the law enforcement community, CJIS Management, and DOJ partners. The symposium enhanced law enforcement agencies' understanding of UCR hate crime statistics and the bias motivations that are reportable to the UCR Program. Attendees gained a better understanding of how local law enforcement utilizes UCR data from local and state program managing perspective and gained more “tools in their toolbox.”

Eradicate Hate Global Summit, 2023

The Eradicate Hate Global Summit was formed as a response to the largest anti-Semitic attack in U.S. history. On October 27, 2018, a gunman motivated by hate ideologies murdered 11 Jews and injured others worshipping at the Tree of Life synagogue in Pittsburgh. The Eradicate Hate Global Summit now stands as the most comprehensive anti-hate conference in the world.

The UCR Program hate crime coordinator presented on the State of Hate panel. This panel addressed recent incidents and trends involving hate precipitated by actors motivated by various kinds of hate—anti-Semitic, anti-Black, anti-Asian, anti-Muslim, anti-LGBTQ+, anti-Asian, anti-women, and more. They spoke about the *2021 Hate Crime Report*, the *Supplemental Hate Crime Statistics, 2021* report, provided victim information statistics, and information about the Hate Crime Statistics Task Force. In addition, it was announced that the Hate Crime Statistics Task Force, along with the UCR Program, will be launching the Hate Crime Awareness Week in 2024. More details will be provided in the future.

Quality Assurance Team formed

Staff in the CLESU at the CJIS Division created the Quality Assurance Team in the spring of 2023 to find inefficiencies and ensure that UCR products are timely, frequent, and of high quality. The team consists of:

Data quality examiners serve as points of contacts to states and assist with submissions for crime and law enforcement data collections.

Program analysts conduct analytical studies related to program controls, productivity/management improvement, and workforce planning. They work toward improving the accuracy and adequacy of information systems.

Management and program analysts prepare various quantitative and qualitative analyses with information systems and present studies to conduct constructive changes.

Infographics are available on LEEP

Staff in the UCR Program maintain infographics on the LEOKA Data Collection and the Law Enforcement Suicide Data Collection (LESDC) on the CDE.

The one-page LEOKA infographic, accessible at <https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/le/leoka>, includes such data as accidental and felonious deaths of law enforcement officers by month for 2022 and 2023. It also provides information on officers' accidental and felonious deaths by region, the demographics of officers killed, and the circumstances surrounding accidental and felonious deaths. The infographic, which is updated monthly, also provides information about the types of weapons offenders used and the location of fatal firearm wounds.

The two-page LESDC infographic is accessible at <https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/le/lesdc> and collects data on suicides and attempted suicides among current and former law enforcement officers, corrections officers, 911 operators, and legal system personnel. The graphic provides information on the methods used in suicides and attempted suicides, the number of attempted suicides and the number of suicides reported, the locations of the incidents, and the employment status and occupational categories of those who died by suicide or attempted suicide.

The graphic also furnishes the numbers of attempted suicides and suicides by race, gender, and military service and the number of incidents by agency wellness program when available.

UCR Program now using a single telephone number and single e-mail address

To assist our external partners in contacting the FBI's UCR Program, the program is now using a single telephone number, 304-625-4830, and a single email address, UCR@fbi.gov, for all general UCR-related topics, information, and questions.

If you are a state program manager, please contact your state's data quality examiner for specific issues regarding UCR data.

Check out the *CJIS Link* for the latest information on CJIS Division services and programs

Visit the *CJIS Link* webpage at <https://le.fbi.gov/cjis-division/cjis-link> to learn how the programs and services administered by the FBI's CJIS Division can help your agency fight crime.

Electronic availability of the *UCR Program Quarterly*

All editions of the *UCR Program Quarterly* are available on JusticeConnect within LEEP.

To access the *UCR Program Quarterly* on JusticeConnect, you must have a LEEP account and be a member of the UCR Program community. To obtain a LEEP account, apply at www.cjis.gov. Once on LEEP, apply to the UCR Program community by clicking on the magnifying glass and searching for "Uniform Crime Reporting Program." Scroll down and click on the UCR Program logo to request joining the community. Members of the UCR Program community should:

- ❖ Log on to the LEEP portal at www.cjis.gov.
- ❖ Click on the JusticeConnect link, read the terms and conditions, and select "I Agree" to continue.
- ❖ Select UCR Program Quarterly under the Publications and Files section.

Users with questions concerning access to LEEP should contact the Data Sharing Services Unit by telephone at 304-625-5555.

Section 2— Clarification to Policies and Procedures

Two-year schedule for documentation updates

The FBI has adopted a 2-year schedule for updating UCR documentation. Data contributors will have 2 calendar years from the date the documentation is released to implement any modifications to UCR Program data unless mandated by law.

Each release will occur biennially and include all enhancements made within the previous 2 calendar years. The UCR Program released the 2023.0 versions of the *NIBRS User Manual*, *NIBRS Technical Specification*, and *NIBRS XML Developer's Guide* in November. The next updated documents are slated for release in 2025 and will include any enhancements recommended by the CJIS APB in 2023 and 2024 that have received approval from the FBI Director.

If the FBI makes enhancements to the UCR Program more quickly than the 2-year schedule, the FBI will release documentation updates to our data contributors.

Currently, at a minimum, data contributors must comply with the 2019.2.1 versions of the *NIBRS User Manual*, the *NIBRS Technical Specification*, and the *NIBRS XML Developer's Guide*.

Data contributors have until November 2025 to comply with the 2023.0 versions of the *NIBRS User Manual*, the *NIBRS Technical Specification*, and the *NIBRS XML Developer's Guide*. These documents are available on the FBI's website at <https://le.fbi.gov/informational-tools/ucr/ucr-technical-specifications-user-manuals-and-data-tools>.

Trainer Talk

Each quarter, Trainer Talk features questions the trainers from the UCR Program have received about classifying offenses in UCR. The information the UCR trainers provide is for UCR Program reporting purposes only and may not reflect the charges filed against an offender(s).

When requesting assistance with the classification of offenses, the UCR trainers ask law enforcement agencies and state Program personnel to provide the entire incident report so that UCR trainers can provide the most accurate assessment. Agencies may submit incident reports by e-mail to UCRtrainers@leo.gov. Agency staff with questions should contact the trainers' e-mail at UCRtrainers@leo.gov.

Question

What is the correct reportable offense for Till Tapping, which involves a distraction of the individual at the till (the drawer of a cash register where the money is kept) while accomplices steal from the till itself?

Answer

The agency should use the offense code 26A = False Pretenses/Swindle/Confidence Game in Data Element 6 (UCR Offense Code). False Pretenses/Swindle/Confidence Game is "the intentional misrepresentation of existing fact or condition or the use of some other deceptive scheme or device to obtain money, goods, or other things of value." (page 25, *NIBRS User Manual*, version, 2023.0, dated June 30, 2023). However, if there is any type of confrontation (physical struggle) taking place when the money is taken, the offense could be classified as a robbery.

Question

How should an agency report 3D printed/replicate guns?

Answer

The agency should report the type of 3D printed/replicate weapon in Data Element 13 (Type Weapon Involved). For example, a facsimile pistol should be reported as a 12 = Handgun. A homemade gun (zip gun or something that functions like a firearm but is not actually replicating another type) would be reported as 15 = Other Firearm in Data Element 13 (Weapon Type Involved).

Section 3— On the Audit Trail

Quality Assurance Review now the NIBRS Audit Program

With the transition of collecting crime data via NIBRS, the CJIS Audit Unit (CAU) has opted to change the name of the Quality Assurance Review to the NIBRS Audit Program.

Beginning with audits that occurred on or after October 1, 2022, audit staff present findings of the NIBRS Audit Program to each respective state's UCR Program Manager and CJIS Systems Officer as well as the Compliance Evaluation and UCR Subcommittees of the CJIS APB. This change aligns all CJIS audit programs and provides more transparency about audit results.

The objective of the NIBRS Audit Program is to assess and ensure that each federal/state UCR Program and its local agencies adheres to incident-based reporting methods that are consistent with UCR standards set forth in the *National Incident-Based Reporting System User Manual* to achieve uniform crime reporting nationwide.

The FBI's UCR Program provides a nationwide view of crime based on the submission of crime information by law enforcement agencies throughout the country. Accurate crime reporting is essential to the credibility of the UCR Program. Designed to enhance the UCR Program, the NIBRS audit is an assessment of a UCR Program and its compliance to the national Program's standards and definitions.

The FBI's CAU conducts a NIBRS audit of UCR Programs with local law enforcement agencies reporting NIBRS data. Reviews of UCR Programs occur on a triennial cycle and are administered remotely from the CJIS Division. The goal is to assess the UCR Program, which involves the local law enforcement agency, in its compliance with the FBI's UCR Program standards of reporting. The objective of the audit is to assist UCR contributors to collect and report accurate and dependable statistics to the FBI's UCR Program.

The three phases of the NIBRS audit are:

- ❖ Administrative Interview: CAU staff ascertain how the UCR Program and/or local agency manages incidents and whether data submitted to the FBI's UCR Program comply with the national standards of reporting.

- ❖ Data Quality Review: CAU staff review officer case file documentation to include the officer's narrative and any information deemed supplemental to determine if the agency appropriately applied national standards and definitions. The CAU staff document any discrepancies.
- ❖ Exit Briefing: CAU staff provide a briefing to the UCR Program manager and/or local agency point of contact, which is a summarization of the NIBRS audit findings based on the administrative interview and the data quality review.

The NIBRS Audit Program is an assessment of a federal or state UCR Program's compliance with the FBI's UCR Program standards and definitions. CAU staff administer them remotely from the CJIS Division of federal or state programs that submit data specified by UCR Program resource materials.

Agencies with questions about the NIBRS Audit Program should contact the CAU by telephone at 304-625-3020 or by e-mail at cjisaudit@fbi.gov.

Auditors' top findings from 2022 and early 2023

The CAU NIBRS Audit Program compiled its top findings from audits conducted during fiscal year 2022 and early 2023. The top findings included issues with 23H = All Other Larceny, the separation of time and place, classifying hate crime biases as 99 = Unknown after the case was closed, misclassification of frauds, and submitting incorrect victim and offender information.

Issues with 23H = All Other Larceny

The definition of 23H = All Other Larceny is "All thefts which do not fit any of the Larceny/Theft or specific subcategories identified in UCR." (2023.0 *NIBRS User Manual* dated June 30, 2023, page 36). However, auditors found several instances in which agencies reported 23H = All Other Larceny when they should have used a more specific subcategory such as 23C = Shoplifting or 23D = Theft From Building. One reason for this is that 23H = All Other Larceny may be the first option programmed into an agency's computers, thus potentially skewing the findings.

Law enforcement officers should use the most specific subcategory of larceny-theft possible to describe the incident.

Issues with the separation of time and place

Auditors found that agencies often combined thefts into one incident instead of correctly reporting them as multiple incidents based on the time and day the incidents occurred. The same problem exists for fraud offenses. For example, an individual steals items from three cars on the same street in a residential area. Shortly after, the individual travels to a different residential area several blocks away and stole items from two cars on the same street. The agency should report two incidents of 23F = Theft From Motor Vehicle because the thefts occurred at locations that were several blocks apart.

In another example, an offender stole a wallet from a convenience store. Later that day, the offender used credit cards from the stolen wallet to make purchases at a different location. The agency should submit two separate reports—one for theft and one for fraud.

Classifying hate crime biases as 99 = Unknown after the case was closed

In NIBRS, offenses not involving any facts indicating bias motivation on the part of the offender are to be reported as 88 = None, whereas offenses involving ambiguous facts (some facts are present but are not conclusive) should be reported as data value 99 = Unknown. When an offense is initially classified as bias motivation 99 = Unknown and subsequent investigation reveals the crime was motivated by bias or no bias was found, the agency must update its original submission. The incident should not be closed and submitted with the data value 99 = Unknown.

The protocols that agencies use to indicate whether an offense is a hate crime (Data Element 8A – Bias Motivation) receive significant attention during most of the NIBRS Audits and training sessions. It would benefit all agencies to emphasize these areas in training when communicating with your agency personnel.

Misclassification of frauds

Auditors have found that agencies are not selecting the most accurate type of fraud for relevant incidents. Agencies should report the most specific subcategory of fraud whenever the circumstances fit the definition of more than one of the subcategories listed below.

For example, many frauds may would fit the definition of 26A = False Pretenses/Swindle/Confidence Game. However, if the offender used a credit card to

perpetrate the Fraud, the agency should classify the offense as 26B = Credit Card/Automated Teller Machine Fraud.

Also, both 26A = False Pretenses/Swindle/Confidence Game and 250 = Counterfeiting/Forgery should be submitted when both are present in an incident. A common finding is that agencies are often submitting only a 250 = Counterfeiting/Forgery and not providing a report of 26A= False Pretenses/Swindle/Confidence Game, when the fraud accompanied the forgery.

Incorrect victim and offender information

Auditors have found that agencies have been improperly reporting the number of victims and offenders and their appropriate demographics, even when the information is present in the incident report and officer narrative. In addition, agencies are reporting zero offenders for incidents when individuals were seen fleeing from the scene of an incident. If an individual sees people fleeing from the scene of a crime, the agency should report the information in Data Element 34 (Offender Number to be Related) and use Data Elements 37 through 39A to indicate if anything is known about the offenders (an approximate age, sex, race, or ethnicity) or 00 = Unknown in Data Element 34 (Offender Number to be Related) to indicate that offenders were present, but nothing was known about the offenders.

Audit findings

Auditors' findings are provided to the state CJIS Systems Officer (CSO) and UCR Program Manager in a draft findings letter, the Findings and Response Template, and the Supplemental Review Document. The NIBRS Team is available to discuss findings, errors, and provide feedback to support the resolution of the issues. Once a response is received from the state, the audit will be finalized, and the results will be provided to the CSO, UCR Program Manager, the Compliance Evaluation Subcommittee, and the UCR Subcommittee.

NIBRS Team’s audit schedule for 2024

Date	State
January	Arizona
January/February	Louisiana
February/March	California
March	Georgia and South Carolina
April	Rhode Island
May	Idaho and Montana
June	Alaska, Wyoming, and Utah
July	Massachusetts, DOJ, Department of State, and U.S. Forestry Service
August	U.S. Capitol Police and Connecticut
September	Maryland and Nevada

Reminders regarding the proper use of the automatic weapon indicator and proper classification of cargo theft

Members of the CAU have noted two issues that frequently arise during the audit process: the improper use of Automatic Weapon Indicator “A” in Data Element 13 (Type of Weapon/Force Involved) and Data Element 46 (Arrestee Was Armed With) and misclassifying incidents as cargo theft.

Use of Automatic Weapon Indicator “A” in Data Elements 13 and 46

Reporting agencies should insert the letter “A” in Data Element 13 (Type of Weapon/Force Involved) and Data Element 46 (Arrestee Was Armed With) to indicate a fully automatic weapon was involved in an incident. Reporting agencies should not enter the letter “A” in the data element when an automatic weapon was not involved in the incident.

The UCR Program defines a fully automatic weapon as:

“Any firearm which shoots, or is designed to shoot, more than one shot at a time by a single pull of the trigger without manual reloading,” (*NIBRS Technical Specification*, Version 2023.0, dated June 30, 2023, p. 61).

Many firearms, especially handguns, are called “automatic,” which means it is an automatic self-loader or, as it is more commonly referred, semi-automatic. This means that as a round is fired, the spent cartridge is expelled from the weapon and another round is automatically chambered but does not fire without another pull of the trigger. Therefore, these types of weapons do not meet the UCR definition of a fully automatic weapon. Actually, a very small number of firearms manufactured for the civilian market, especially handguns, are fully automatic weapons by UCR standards.

The UCR Program staff asks state program managers and direct contributors to review incident reports with an “A” in Data Elements 13 and/or 46 to ensure that the firearms involved meet the Program’s definition of fully automatic firearms.

Proper classification of cargo theft

Agencies are reminded to consult the *Cargo Theft User Manual*, Version 3.0, dated April 7, 2023, (<https://le.fbi.gov/file-repository/cargo-theft-user-manual.pdf/view>) for assistance in reporting incidents of cargo theft to the FBI. The document addresses policy, types of offenses that constitute a cargo theft incident, how to identify cargo theft, and guidelines for reporting cargo theft.

Cargo theft is the criminal taking of any cargo including, but not limited to, goods, chattels, money, or baggage that constitutes, in whole or in part, a commercial shipment of freight moving in commerce, from any pipeline system, railroad car, motortruck, or other vehicle, or from any tank or storage facility, station house, platform, or depot, or from any vessel or wharf, or from any aircraft, air terminal, airport, aircraft terminal or air navigation facility, or from any intermodal container, intermodal chassis, trailer, container freight station, warehouse, freight distribution facility, or freight consolidation facility. For purposes of this definition, cargo shall be deemed as moving in commerce at all points between the point of origin and the final destination, regardless of any temporary stop while awaiting transshipment or otherwise. (*Cargo Theft User Manual*, Version 3.0, dated April 7, 2023, p. 4).

Agencies report cargo theft using Data Element 2A (Cargo Theft) in the Administrative Segment.

In the UCR Program, cargo theft is not considered an offense by itself; cargo theft should be reported in conjunction with at least 1 of the 15 offenses to indicate that cargo was taken. The 15 offenses (and their UCR Offense Codes) are:

120 = Robbery

210 = Extortion/Blackmail

220 = Burglary/Breaking & Entering

23D = Theft From Building

23F = Theft From Motor Vehicle

23H = All Other Larceny

240 = Motor Vehicle Theft

26A = False Pretenses/Swindle/Confidence Game

26B = Credit Card/Automatic Teller Machine Fraud

26C = Impersonation

26E = Wire Fraud

26F = Identity Theft

26G = Hacking/Computer Invasion

270 = Embezzlement

510 = Bribery

The UCR Program has furnished the following guidelines regarding the classification and reporting of cargo theft incidents and arrests.

- ❖ Two key phrases in the classification of cargo theft are “commercial shipment” and “in the supply chain.” To be considered cargo, the items must be part of a commercial shipment and must be in the supply chain (that is, moving in commerce).

- ❖ Thefts from United Parcel Service (UPS), Federal Express (FedEx), the U.S. mail, etc., are considered to be cargo until items are received at a final distribution point. Once the business receives the items (that is, personnel at the company sign for the goods), the goods are no longer considered cargo because they are outside of the supply chain. Therefore, **deliveries from UPS, FedEx, to individuals or other businesses (e.g., flowers, pizza, electronics, and appliances) are not considered to be cargo because they are outside the supply chain.** (Emphasis added.)

Below are some scenarios of cargo theft. It is assumed that all cargo is moving in commerce, i.e., commercial shipment and in the supply chain, at all points between the point of origin and the final destination (exchange bill of lading), regardless of any temporary stop while awaiting transshipment or otherwise.

- ❖ An armed suspect hijacked an 18-wheeler and kidnapped the driver (UCR Offense Codes 100 = Kidnapping/Abduction and 120 Robbery). The suspect then transferred the stolen cargo to another trailer.
- ❖ Four men wearing ski masks conducted an armed robbery at a trucking facility (UCR Offense Code 120 = Robbery). Two of the men held the guards at gunpoint while the other two men jumped into an idling truck nearby and drove off with the cargo.
- ❖ A suspect was employed at a wholesale tobacco warehouse. After hours, the employee gained entry into the warehouse and removed 4,000 cartons of cigarettes, inventory that was slated for shipment to local retailers (UCR Offense Code 220 = Burglary).
- ❖ A delivery driver stopped at a truck stop for a short break and exited, leaving the vehicle unattended. A short time later, the driver returned to the vehicle and discovered the cargo missing from the box truck (UCR Offense Code 23F = Theft From Motor Vehicle).
- ❖ Unknown suspects entered the terminal grounds of Carrier XYZ by cutting a section of fence. The suspects then broke into a loaded unattached trailer and

removed the cargo (UCR Offense Code 23H = All Other Larceny).

- ❖ The driver of an 18-wheeler accepted a bribe to “look the other way” (UCR Offense Code 510 = Bribery) while his load of cargo was being “stolen” (UCR Offense Code 23F = Larceny From a Motor Vehicle).

- ❖ Two individuals worked for Company Y, loading and unloading cargo. Employee A discovered that Employee B was using drugs on the job. Employee A threatened to reveal his drug use to their employer. As payment for keeping silent, Employee A demanded a partial shipment of plasma TVs (UCR Offense Code 210 = Extortion/Blackmail).

- ❖ The owner/driver of a tractor trailer stopped at a post office to check his mail, leaving the vehicle running and unlocked. When he returned, both the rig and the cargo were gone (UCR Offense Code 240 = Motor Vehicle Theft).

- ❖ An air cargo worker stole a shipment of military supplies from an all-cargo aircraft, which was scheduled for delivery to military personnel overseas (UCR Offense Code 270 = Embezzlement).

- ❖ A man, posing as an indirect air carrier employee (UCR Offense Code 26C Impersonation) picked up a truck and trailer from a consolidation facility, which was slated for delivery to an airport sorting center (UCR Offense Code 240 = Motor Vehicle Theft).

- ❖ Five suspects entered a slow-moving freight train, which was transporting cargo from the freight yard to numerous destinations. The suspects used various tools to break into the shipping containers. The merchandise was then thrown off the train, and accomplices on the ground gathered the stolen merchandise. (UCR Offense Code 220 = Burglary/Breaking and Entering).

- ❖ A suspect worked on the dock at a port facility, loading and unloading cargo containers. After hours, the suspect entered the shipping yard and stole a chassis and intermodal container loaded with automobile tires (UCR Offense Code 23H = All Other Larceny).

- ❖ An employee used the internet to gain unauthorized access to the shipping records for Company ABC (UCR Offense Code 270 = Embezzlement). The employee then obtained corporate credit card information and pre-paid the freight fees for a shipment of imported wines (UCR Offense Code 26B = Credit Card/Automated Teller Machine Fraud). Via computer, the suspect then illegally diverted the shipment to an alternate address (UCR Offense Code 26E = Wire Fraud).

The following scenarios do not meet the definition of cargo theft because the shipments are no longer a commercial shipment or in the supply chain:

- ❖ A letter carrier was delivering mail in a neighborhood when the mail was stolen from the carrier's vehicle. This is **not** cargo theft. Once the U.S. mail left the final distribution point, it was no longer considered cargo because it was no longer in the supply chain. The agency should report the incident as a Theft From a Motor Vehicle (UCR Offense Code 23F = Larceny From a Motor Vehicle), but the incident is not considered to be cargo theft.

- ❖ A truck was delivering a refrigerator for installation into an individual's home. The driver of the truck was carjacked while stopped at a traffic light. The agency should report the incident as Robbery (UCR Offense Code 120 = Robbery); however, the incident is **not** considered cargo theft because the refrigerator is not in the supply chain.

Agencies with questions regarding cargo theft should contact the UCR trainers by email at UCRtrainers@leo.gov.