CITY OF URBANA

CITY OF URBANA
CITY COUNCIL REGULAR MEETING

DATE: Monday, November 23, 2026
TIME: 7:00 PM
PLACE: 400 South Vine Street, Urbana, IL 61801

AGENDA

A. Call to Order and Roll Call

B. Approval of Minutes of Previous Meeting

1. **11-04-2026 Special City Council Meeting Minutes**

2. **11-09-2026 City Council Meeting Minutes**

C. Additions to the Agenda

D. Presentations and Public Input

E. Council Input and Communications

F. Reports of Standing Committees

G. Committee of the Whole (*Council Member Shirese Hursey, Ward 3*)

1. Consent Agenda

a. **Resolution No. 2026-11-063R:** A Resolution Approving an Intergovernmental Agreement (Edward Byrne Memorial Justice Assistance Grant) – PD

b. **Resolution No. 2026-11-064R:** A Resolution Approving an Intergovernmental Agreement Providing for Reimbursement of Completed Storm Sewer Repair on Crystal Lake Drive – PW

c. **Resolution No. 2026-11-065R:** A Resolution Amending Resolution No. 2023-02-013R A Resolution Adopting the City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List (#3) – Exec

2. Regular Agenda

a. **Ordinance No. 2026-11-028:** An Ordinance Amending Urbana City Code Article VIII – Recycling Tax, Chapter 22 – Taxation, Section 102 – Residential Recycling Tax Imposed – PW

H. Reports of Special Committees

All City meetings are broadcast on Urbana Public Television and live-streamed on the web. Details on how to watch are found on the UPTV webpage located at https://www.urbanail.gov/executive-department/page/urbana-public-television

I. Reports of Officers

1. **Surveillance Technologies Policy and Use Reports**

J. Adjournment

PUBLIC INPUT

The City of Urbana welcomes Public Input during open meetings of the City Council, the City Council's Committee of the Whole, City Boards and Commissions, and other City-sponsored meetings. Our goal is to foster respect for the meeting process, and respect for all people participating as members of the public body, city staff, and the general public. The City is required to conduct all business during public meetings. The presiding officer is responsible for conducting those meetings in an orderly and efficient manner. Public Input will be taken in the following ways:

Email Input
Public comments must be received prior to the closing of the meeting record (at the time of adjournment unless otherwise noted) at the following: citycouncil@urbanail.gov. The subject line of the email must include the words "PUBLIC INPUT" and the meeting date. Your email will be sent to all City Council members, the Mayor, City Administrator, and City Clerk. Emailed public comments labeled as such will be incorporated into the public meeting record, with personal identifying information redacted. Copies of emails will be posted after the meeting minutes have been approved.

Written Input
Any member of the public may submit their comments addressed to the members of the public body in writing. If a person wishes their written comments to be included in the record of Public Input for the meeting, the writing should so state. Written comments must be received prior to the closing of the meeting record (at the time of adjournment unless otherwise noted).

Verbal Input
Protocol for Public Input is one of respect for the process of addressing the business of the City. Obscene or profane language, or other conduct that threatens to impede the orderly progress of the business conducted at the meeting is unacceptable.

Public comment shall be limited to no more than five (5) minutes per person. The Public Input portion of the meeting shall total no more than two (2) hours, unless otherwise shortened or extended by majority vote of the public body members present. The presiding officer or the city clerk or their designee, shall monitor each speaker's use of time and shall notify the speaker when the allotted time has expired. A person may participate and provide Public Input once during a meeting and may not cede time to another person, or split their time if Public Input is held at two (2) or more different times during a meeting. The presiding officer may give priority to those persons who indicate they wish to speak on an agenda item upon which a vote will be taken.

The presiding officer or public body members shall not enter into a dialogue with citizens. Questions from the public body members shall be for clarification purposes only. Public Input shall not be used as a time for problem solving or reacting to comments made but, rather, for hearing citizens for informational purposes only.

In order to maintain the efficient and orderly conduct and progress of the public meeting, the presiding officer of the meeting shall have the authority to raise a point of order and provide a verbal warning to a speaker who engages in the conduct or behavior proscribed under "Verbal Input". Any member of the public body participating in the meeting may also raise a point of order with the presiding officer and request that they provide a verbal warning to a speaker. If the speaker refuses to cease such conduct or

behavior after being warned by the presiding officer, the presiding officer shall have the authority to mute the speaker's microphone and/or video presence at the meeting. The presiding officer will inform the speaker that they may send the remainder of their remarks via e-mail to the public body for inclusion in the meeting record.

Accommodation

If an accommodation is needed to participate in a City meeting, please contact the City Clerk's Office at least 48 hours in advance so that special arrangements can be made using one of the following methods:

- Phone: 217.384.2366
- Email: CityClerk@urbanail.gov

CITY OF URBANA

City of Urbana
400 S. Vine Street, Urbana, IL 61801
www.urbanail.gov

MEMORANDUM TO THE MAYOR AND CITY COUNCIL

Meeting: November 16, 2026 Committee of the Whole
Subject: Approval of an Intergovernmental Agreement **(**Edward Byrne Memorial Justice Assistance Grant**)**

Summary

Action Requested

City Council as being asked to approve the resolution to accept a grant award through an Intergovernmental Agreement (IGA). Appropriating the accepted grant would occur in the forthcoming budget amendment.

Brief Background

The U.S. Department of Justice annually awards the Edward Byrne Memorial Justice Assistance Grant to various law enforcement agencies throughout the United States. The Urbana Police Department applies jointly with the Champaign Police Department. The City of Champaign is the lead agency, therefore, the City of Urbana would be classified as sub-grantee.

Relationship to City Services and Priorities

Impact on Core Services

The Urbana Police Department will utilize $23,022 to purchase virtual reality (VR) training equipment, upgraded monitors, and resources to support officer wellness initiatives. These purchases will enhance the department's training capabilities, provide officers with opportunities to improve their skills, and support their overall well-being. This investment will help ensure officers are better equipped to serve the community safely and effectively.

Strategic Goals & Plans

N/A

Previous Council Actions

City Council has accepted the Edward Byrne Memorial Justice Assistance Grant on multiple occasions in the past.

Discussion

Fiscal and Budget Impact

This grant offsets expenditures the City already planned on incurring, but for which there is insufficient funding. In the event that this IGA is not approved, the Police Department will seek a budget amendment to allocate fund balance to complete this installation project. There is no local match in order to accept or receive this award. The grant is intended to supplement funding to local and county law enforcement agencies.

Recommendation
Staff recommends that City Council approve the resolution accepting the grant award.

Next Steps
If approved, staff will use the grant funds to aid in the purchase of squad car camera installation and comply with all required financial reporting requirements.

Attachments

1. A Resolution Approving and Intergovernmental Agreement (JAG)
2. Intergovernmental Agreement (JAG)

Originated by: Zachery Mikalik, Deputy Chief of Police
Reviewed: Larry Boone, Chief of Police
Approved: Darius L. White, City Administrator

RESOLUTION NO. _____

A RESOLUTION APPROVING AN INTERGOVERNMENTAL AGREEMENT
(to Accept a Justice Assistance Grant)

WHEREAS, each of the parties to the Intergovernmental Agreement between the City of Urbana, City of Champaign and the County of Champaign is a body politic organized, operating, and maintaining offices within the boundaries of Champaign County, Illinois; and

WHEREAS, the City of Urbana (the "City") is an Illinois home rule unit of local government pursuant to Section 6 of Article VII of the Illinois Constitution of 1970 and the statutes of the State of Illinois; and

WHEREAS, Section 10 of Article VII of the Illinois Constitution of 1970 and the Illinois Intergovernmental Cooperation Act, 5 ILCS 220/1 *et seq.* enable the parties to enter into and execute agreements among themselves and provide authority for intergovernmental cooperation; and

WHEREAS, the City recognizes that it is appropriate and beneficial for the City and its departments to apply for and receive grants from private, state, and federal agencies; and

WHEREAS, the U.S. Department of Justice, Office of Justice Programs has created and operates the Edward Byrne Memorial Justice Assistance Grant Program for local units of government that maintain and operate law enforcement departments; and

WHEREAS, in the past, the City has joined with one or more other communities as allocated by the U.S. Department of Justice, Office of Justice Programs, in applying for and receiving grant funding from the said Edward Byrne Memorial Justice Assistance Grant Program; and

WHEREAS, the City of Champaign, as lead agency, has been awarded a Justice Assistance Grant, of which $23,022 has been allocated to the City of Urbana; and

WHEREAS, the City Council finds it desirable and in the best interests of the City to accept this allocation of funds.

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Urbana, Illinois, as follows:

Section 1.

The Intergovernmental Agreement among the Cities of Champaign and Urbana and the County of Champaign for the Edward Byrne Memorial Justice Assistance Grant (JAG) Program, in substantially the form of the Exhibit appended hereto and made a part hereof, shall be and hereby is authorized and approved.

Section 2.

The Mayor of the City of Urbana, Illinois, shall be and hereby is authorized to execute and deliver and the City Clerk of the City of Urbana, Illinois, shall be and hereby is authorized to attest to said execution of said Agreement as so authorized and approved for and on behalf of the City of Urbana, Illinois.

PASSED BY THE CITY COUNCIL this _____ day of _____, 2026.

AYES:

NAYS:

ABSTENTIONS:

_____
Darcy E. Sandefur, City Clerk

APPROVED BY THE MAYOR this ____ day of _____, 2026.

_____
DeShawn Williams, Mayor

INTERGOVERNMENTAL AGREEMENT
JAG PROGRAM

(City of Champaign, City of Urbana, and Champaign County)

THIS AGREEMENT is made and entered by and among the City of Champaign, an Illinois Municipal Corporation ("Champaign"), City of Urbana, an Illinois Municipal Corporation ("Urbana"), and Champaign County, an Illinois Unit of Local Government ("County"), - (herein after collectively referred to as "the parties"), effective on the last date signed by a party hereto.

WHEREAS, Section 10 of Article VII of the Illinois Constitution of 1970 and the Illinois Intergovernmental Cooperation Act, 5 ILCS 220/1 et seq. enables the parties to enter into agreements among themselves and provide authority for intergovernmental cooperation; and

WHEREAS, The Edward Byrne Memorial Justice Assistance Grant Program (JAG) is a partnership among federal, state, and local governments to create safer communities by improving the functioning of the criminal justice system; and

WHEREAS, the City of Champaign and Champaign County desire to apply for JAG funds to fund individual projects in the City of Champaign and Champaign County.

NOW, THEREFORE, the parties agree as follows:

Section 1. The Funds. The parties acknowledge, as of the date of this Agreement, the total anticipated grant available to all parties is ONE HUNDRED AND EIGHTEEN THOUSAND TWO HUNDRED SIXTY DOLLARS ($118,260.00).

Section 2. Grant Disposition. Proceeds from the grant shall be distributed by Champaign to Champaign County for funding individual local projects fitting into the JAG guidelines, in the amounts set forth in Exhibit A.

Section 3. Lead Agency. The City of Champaign is hereby designated the Lead Agency for this Agreement. Responsibilities shall include leading the application process for the JAG funds, accepting any and all funds awarded through the JAG program, establishing a trust fund in which to deposit the funds received through the JAG program, and preparing required reports.

Section 4. Representative; Information Requirements. The City of Champaign shall designate one representative to fulfill the requirements of this Agreement. The representative shall exercise due diligence in providing any and all information necessary or convenient for the performance of the duties required by Champaign in Section 3 above, including submitting the JAG application and preparation of performance measures and program assessment data.

Section 5. Fund Restriction. The parties agree that no funds will be used directly or indirectly for security enhancements or equipment to nongovernmental entities not engaged in criminal justice or public safety, and that the funds will not supplant existing budgeted funds.

Section 6. Liability. Nothing in the performance of this Agreement shall impose any liability for claims against any party other than claims for which liability may be imposed by the Illinois Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/1-

101 *et seq*. Each party to this Agreement shall be responsible for its own actions in providing services under this Agreement and shall not be liable for any civil liability that may arise from the furnishing of the services by the other party. The parties to this Agreement do not intend for any third party to obtain any rights by virtue of this Agreement.

Section 7. Amendments. Amendments to this Agreement shall be made in writing and signed by all parties. In the event the amount of funds received is different from the amount set forth in Section 1, the parties shall exercise principles of good faith and fair dealing to amend Exhibit A in a manner consistent with the principles of this Agreement and in accordance with all JAG program requirements. Such amendments may be entered into by the chief administrative officers of Champaign, Urbana, and County.

Section 8. Signatures. This Agreement may be executed in any number of counterparts, each of which shall be deemed to be an original. Facsimile, pdf, or other digital signature (e.g. Docusign) shall be deemed to have the same legal effect as an original ink signature.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed on the date and year indicated herein.

CITY OF CHAMPAIGN

By: Christopher Walton
Acting City Manager

Date: 10/20/2026

ATTEST: Shannon Myers

APPROVED AS TO FORM:
Thomas Yu
City Attorney CB 2026-**152**

CHAMPAIGN COUNTY

By: _____

Date: _____

ATTEST: _____

APPROVED AS TO FORM:
_____
State's Attorney

CITY OF URBANA

By: _____

Date: _____

ATTEST: _____

APPROVED AS TO FORM:
_____
City Attorney CB 2026-_____

EXHIBIT A
(City of Champaign, City of Urbana, and Champaign County)

JAG AWARD DISPOSITION

The 2025 JAG funds will be distributed to the Champaign Police Department to fund individual projects meeting the guidelines of the JAG grant.

City of Champaign Police Department		$76,471.00
City of Urbana Police Department		$29,364.00
Champaign County Sheriff's Office		$12,425.00
	TOTAL	$118,260.00

CITY OF URBANA

City of Urbana
400 S Vine Street, Urbana, IL 61801
www.urbanaillinois.us

MEMORANDUM TO THE MAYOR AND CITY COUNCIL

Meeting: November 16, 2026, Committee of the Whole
Subject: A Resolution Approving and Authorizing the Execution of an Intergovernmental Agreement Providing for Reimbursement of Completed Storm Sewer Repair on Crystal Lake Drive

---

Summary

Action Requested

City Council is being asked to pass the attached resolution to approve and authorize the execution of an Intergovernmental Agreement between the City of Urbana and the Urbana & Champaign Sanitary District (UCSD) that provides for the reimbursement of a completed repair of the City's storm sewer on Crystal Lake Drive in Urbana.

Brief Background

During construction of UCSD's Crystal Lake Drive Interceptor Sewer Improvements, it was determined that a repair of the City's storm sewer was necessary. For the sake of timeliness and coordination with the UCSD project, the contractor for the project performed the storm sewer repair work and charged those fees to UCSD through the project contract.

Relationship to City Services and Priorities

Impact on Core Services N/A
Strategic Goals & Plans N/A
Previous Council Actions N/A

Discussion

Additional Background

Sewer conflicts and repairs are not uncommon during construction of underground utilities. Typically, the project owner absorbs the costs of sewer repairs. However, in this case, the poor quality of the materials used for the original construction of the City's storm sewer required additional repair work and the addition of a storm sewer structure. It would be unreasonable for the City to expect that the project owner would pay for this repair work. Therefore, UCSD and City staff agreed that the work should be completed as part of the UCSD project but paid for by the City. This coordination allowed for the project to continue in a timely manner, which reduced the impact on residents in the area. Because UCSD is a government body, an intergovernmental agreement is required for this payment.

Fiscal and Budget Impact
The City will reimburse UCSD for the construction costs associated with the storm sewer repair, totaling $15,454.62. The City budgets annually for storm sewer repairs in the Stormwater Utility Fund and those funds will be used for this reimbursement.

Recommendation
Staff recommends approval of the Resolution Approving and Authorizing the Execution of an Intergovernmental Agreement Providing for Reimbursement of Completed Storm Sewer Repair on Crystal Lake Drive.

Next Steps
If the attached resolution is passed, the Mayor will execute the intergovernmental agreement. Then, the City will process payment for the reimbursement of the storm sewer repair costs.

Attachments

1. Resolution No. 2026-11-___R: A Resolution Approving and Authorizing the Execution of an Intergovernmental Agreement Providing for Reimbursement of Completed Storm Sewer Repair on Crystal Lake Drive
2. An Intergovernmental Agreement Providing for Reimbursement of Completed Storm Sewer Repair on Crystal Lake Drive

Originated by: Justin Swinford, Interim City Engineer
Reviewed: Vince Gustafson, Public Works Director
Approved: Darius White, City Administrator

RESOLUTION NO. 2026- 11 - R

A RESOLUTION APPROVING AN INTERGOVERNMENTAL AGREEMENT PROVIDING FOR REIMBURSEMENT OF COMPLETED STORM SEWER REPAIR ON CRYSTAL LAKE DRIVE

WHEREAS, Section 10 of Article VII of the Illinois Constitution of 1970 and the Illinois Intergovernmental Cooperation Act, 5 ILCS 220/1 et seq., authorize units of local government to enter into agreements by and between themselves and provide authority for intergovernmental cooperation; and,

WHEREAS, the City Council, after due consideration, finds that approving the agreement as herein provided is in the best interests of the residents of the City and is desirable for the welfare of the City's government and affairs.

NOW, THEREFORE, BE IT RESOLVED by the City Council, of the City of Urbana, Illinois, as follows:

An intergovernmental agreement providing for reimbursement of completed storm sewer repair on Crystal Lake Drive, in substantially the form of the copy of said agreement attached hereto and hereby incorporated by reference, is hereby authorized and approved. The Mayor of the City of Urbana is hereby authorized to execute and deliver said agreement as so authorized and approved for and on behalf of the City of Urbana.

PASSED BY THE CITY COUNCIL this ____ day of _____, 2026.

AYES:

NAYS:

ABSTENTIONS:

_____
Darcy E. Sandefur, City Clerk

APPROVED BY THE MAYOR this _____ day of _____, 2026.

_____
DeShawn B. Williams, Mayor

Attachment #1

AN INTERGOVERNMENTAL AGREEMENT PROVIDING FOR REIMBURSEMENT OF COMPLETED STORM SEWER REPAIR ON CRYSTAL LAKE DRIVE

This Intergovernmental Agreement (hereinafter, the "Agreement"), including any exhibits and attachments appended hereto and incorporated herein, is made and entered into as of this _____ day of _____, 2026 by and between the Urbana & Champaign Sanitary District, an Illinois Municipal Corporation (hereinafter, the "Sanitary District") and the City of Urbana, an Illinois Municipal Corporation (hereafter, the "City").

WHEREAS, Section 10 of Article VII of the Illinois Constitution of 1970 and the Illinois Intergovernmental Cooperation Act, 5 ILCS 220/1 *et seq*. enable the parties hereto to make and enter into agreements by and between themselves and provide authority for intergovernmental cooperation; and,

WHEREAS, during its Crystal Lake Drive Interceptor Sewer Improvements project (the "Project"), the Sanitary District discovered a City-owned storm sewer pipe in a non-functional condition; and,

WHEREAS, in order to avoid delay to the Project and with the City's knowledge and consent, the Sanitary District, through its Project contractor, Ezell Excavating, repaired the non-functional storm sewer pipe (the "Repair Work"), and the City has inspected and accepted the Repair Work as complete and to the City's satisfaction; and,

WHEREAS, the Sanitary District has paid Ezell Excavating for the Repair Work in accordance with the Project contract, at a cost of Fifteen Thousand Four Hundred Fifty-Four and 62/100 Dollars ($15,454.62) (the "Repair Costs"); and,

WHEREAS, the City and its constituents benefit directly from the repaired storm sewer pipe, and the parties desire to enter into this Agreement to document the City's reimbursement of the Repair Costs to the Sanitary District.

NOW therefore, in consideration of the exchange of good, valuable and mutual consideration which each party hereto acknowledges as having in hand received and for the exchange of the terms, provisions and conditions contained in this Agreement, the parties hereto agree as follows:

1. Notwithstanding anything to the contrary provided for in this Agreement, the City shall reimburse the Sanitary District for the Repair Costs in the fixed amount of Fifteen Thousand Four Hundred Fifty-Four and 62/100 Dollars ($15,454.62), which amount shall constitute full and complete payment for the Repair Work.

2. The parties acknowledge that the Sanitary District has paid Ezell Excavating in full for the Repair Work. Following execution of this Agreement, the Sanitary District shall submit an invoice for the the City's share of the Repair Costs, together with reasonable supporting documentation. The City shall pay the invoiced amount to the Sanitary District within sixty (60) days of its receipt of the invoice.

3. Notice given hereunder shall be given to:

	City at:	The Sanitary District at:
Delivery:	City Engineer Urbana Public Works Department 706 South Glover Avenue Urbana, IL 61802	Executive Director Urbana & Champaign Sanitary District 1100 East University Avenue Urbana, IL 61802
Mail:	(same as above)	Executive Director Urbana & Champaign Sanitary District P.O. Box 669 Urbana, IL 61803

Notice shall be deemed effective:

a. If given by First Class Mail, four (4) days after placement with the U.S. Postal Service if placed in a properly addressed and stamped envelope.

b. If given by courier service, the day after delivery if the courier service provides, whether in hardcopy or electronically, a receipt stating that delivery was made.

c. If sent by certified mail, return receipt requested, upon mailing.

4. In the event either party to this Agreement defaults (the "Defaulting Party") on any of its obligations provided in this Agreement, the other party (the "Non-Defaulting Party") shall give the Defaulting Party notice of any such default. All Notices of Default shall be in writing, describe the nature of the default and specify the paragraph of this Agreement or the exhibit designation and paragraph therein claimed to be in default. The Defaulting Party shall have seven (7) calendar days in which to (i) cure the default, (ii) provide a written statement to the Non-Defaulting Party which explains why the Defaulting Party is not in default; or (iii) provide the Non-Defaulting Party with a reasonable timetable in which it will cure the default if the same cannot reasonably be cured within the said seven (7) calendar-day period.

5. In the event of a dispute between the parties regarding the withholding of any approval, any terms provided for in this Agreement or any exhibit attached hereto and made a part hereof, or the performance of any obligation provided for in this Agreement, the parties shall meet face-to-face in an effort to resolve their dispute. If such face-to-face resolution effort fails, the parties to this Agreement shall agree to and shall participate in good faith in mediation. Should mediation fail, either party shall have the right to file and maintain an action in the Circuit Court for the Sixth Judicial Circuit, Champaign County, Illinois seeking the relief which the filing party deems appropriate. Any dispute regarding the construction, interpretation or application of

any term contained in this Agreement or any exhibit appended hereto and any breach hereof shall be governed by the laws of the State of Illinois and Sanitary District ordinances.

.

IN WITNESS WHEREOF, the City and the District have executed this Agreement.

CITY OF URBANA

By_____
DeShawn Williams– Mayor

Date:_____

URBANA & CHAMPAIGN SANITARY DISTRICT

By_____ 11/5/2026
Charles Nerone – Board President

Date: 11/5/2026

CITY OF URBANA

City of Urbana
400 S. Vine Street, Urbana, IL 61801
www.urbanaillinois.us

MEMORANDUM TO THE MAYOR AND CITY COUNCIL

Meeting: November 16, 2026, Committee of the Whole
Subject: A Resolution Amending Resolution No. 2023-02-013R A Resolution Adopting the City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List (#3)

Summary

Action Requested

City Council is asked to approve the reallocation of up to $70,000 in American Rescue Plan Act (ARPA) State and Local Fiscal Recovery Funds (SLFRF), or "ARPA funds," from certain subrecipient projects which may have available balances that will not be expended by the program deadline of December 31, 2026. Because the exact available balances and reallocation amounts cannot yet be determined, we are requesting that the City Council grant City staff one-time, limited flexibility to reallocate funds to the Sanitary Sewer Lateral Lining (SSLL) project, administered by the City of Urbana Public Works Department. In the unlikely event that SSLL cannot absorb the reallocated funds, there are three backup reallocation recipients. This grant of flexibility expires on December 31, 2026. City staff will provide Council with a final exact-dollar reallocation schedule no later than April 30, 2027.

The proposed resolution would amend Resolution No. 2023-02-013R A Resolution Adopting the City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List and authorize the action requested above.

Brief Background

Following a review conducted in collaboration with the Champaign County Regional Planning Commission (CCRPC or RPC), it was determined that up to four subrecipient projects could not fully expend their ARPA funds by the December 31, 2026, spending deadline:

Subrecipient	Project Name	Estimated available balance
Justine Petersen	Urbana Small Business Microloan Fund	Up to $42,000
CCRPC	ARPA Project and Fiscal Management	Up to $16,000

Subrecipient	Project Name	Estimated available balance
City of Urbana Public Works Department	Equality and Quality of Life (EQL)	Up to $12,000
FirstFollowers	Urbana Community Peace Hub	$1.51

Relationship to City Services and Priorities

Impact on Core Services

There are no known or anticipated impacts on core City services. The recommended reallocation will support the City of Urbana's Sanitary Sewer Lateral Lining (SSLL) project, a municipal infrastructure initiative managed by the City of Urbana Public Works Department to rehabilitate aging residential sewer connections using trenchless technology.

Strategic Goals & Plans

The requested reallocation plan supports the following elements of Mayor-Council goals:

- **Strategic Area #1: Public Safety and Well-Being.**
  - **Action Step 3a: Promote community well-being**.
- **Strategic Area #3: Infrastructure.**
  - **Strategy 1: Improve quality of current infrastructure assets.**
  - **Strategy 2: Increase investments in infrastructure equity.**

The requested reallocation plan also aligns with multiple "Big Moves" from the 2025 Comprehensive Plan, including:

- **Big Move 3:** Address the Needs of Individual Areas
- **Big Move 8:** Invest in Financially and Environmentally Resilient Infrastructure
- **Big Move 10:** Support Community Health, Safety, and Well-Being

Previous Council Actions

In February 2023, the Council voted to adopt Resolution_2023-02-013R, obligating the original ARPA SLFRF grant. In May 2026, the Council voted to adopt Resolution No. 2026-05-018R to reallocate a total of $40,037 in ARPA funds. In September 2026, the Council also voted to adopt Resolution_2026-09-051R to reallocate a total of $45,000 in ARPA funds.

Discussion

Additional Background Information

The City of Urbana was the recipient of about $13 million in American Rescue Plan Act (ARPA) State and Local Fiscal Recovery Funds (SLFRF), or "ARPA funds." Urbana City Council voted to allocate about $10 million to 26 different subrecipient projects in Resolution_2023-02-013R.

Twenty-three (23) subrecipient projects are fully closed out or have completed over 97% of scheduled spending. Over 99% of Urbana's ARPA subrecipient project funds have already been spent or credibly allocated (e.g., for regular recurring payments into future months).

Obligation Deadline: Although no new subrecipient projects can be started after the December 31, 2024, obligation deadline, U.S. Department of the Treasury guidance and FAQs anticipated that some recipient and subrecipient projects would not be able to expend their ARPA funds by the December 31, 2026, spending deadline (for a variety of reasons: recipient capacity, project timeline, availability of other funds, etc.). In that case, ARPA funds may be reallocated to other existing subrecipient projects already obligated or funded by December 31, 2024.

Operations Impact
The reallocation process requires staff time and effort in coordination with RPC to analyze subrecipient expenditures, schedules, and forecasts – and then to develop approaches to reallocation.

Policy or Statutory Impacts
There are no known or anticipated policy or statutory impacts.

Fiscal and Budget Impact
The reallocation request is intended to increase the likelihood that all ARPA funds are fully expended so that no unspent ARPA funds are returned to the U.S. Treasury.

Community Impact
The reallocation request is intended to increase the likelihood that all ARPA funds are completely spent to maximize the community impact of those funds. There are no known or anticipated impacts that would negatively affect members of traditionally under-represented racial or ethnic groups.

Recommendation
City Council is asked to approve the reallocation of up to $70,000 in ARPA funds to the Sanitary Sewer Lateral Lining (SSLL) project.

Next Steps
Upon Council approval, RPC and City staff will prepare the appropriate documents and obtain required approvals to implement the approved reallocation(s). RPC and City staff will continue to monitor progress toward full expenditure of all ARPA subrecipient project grants.

Attachments

1. Resolution No. 2023-02-013R A Resolution Adopting the City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List (as a link)
2. Resolution No. 2026-05-018R A Resolution Amending Resolution No. 2023-02-013R A Resolution Adopting The City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List (as a link)
3. Resolution_2026-09-051R A Resolution Amending Resolution No. 2023-02-013R A Resolution Adopting the City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List (#2) (as a link)
4. Resolution _____ A Resolution Amending Resolution No. 2023-02-013R A Resolution Adopting the City of Urbana American Rescue Plan Act (ARPA) Concept Plan Project List (#3)

Originated by: Tarek Arthur Azim, Management Analyst
Reviewed: Matt Roeschley, City Attorney
Approved: Darius L. White, City Administrator

RESOLUTION NO. _____

A RESOLUTION AMENDING RESOLUTION NO. 2023-02-013R A RESOLUTION ADOPTING THE CITY OF URBANA AMERICAN RESCUE PLAN ACT (ARPA) CONCEPT PLAN PROJECT LIST (#3)

WHEREAS, the City of Urbana adopted the American Rescue Plan Act (ARPA) Concept Plan Project List through Resolution No. 2023-02-013R, as previously amended by Resolution No. 2026-05-018R and Resolution No. 2026-09-051R, allocating ARPA State and Local Fiscal Recovery Funds (SLFRF) to designated subrecipient projects; and

WHEREAS, the City previously approved ARPA SLFRF funding for the subrecipient projects identified in Exhibits A and B through prior Council action; and

WHEREAS, the City desires to ensure all ARPA SLFRF funds are spent down for maximum community impact before the December 31, 2026, deadline; and

WHEREAS, although no new subrecipient projects can be started after the December 31, 2024, obligation deadline, U.S. Department of the Treasury guidance and FAQs allow ARPA SLFRF awards to be reallocated to other existing subrecipient projects obligated or funded by December 31, 2024; and

WHEREAS, certain subrecipient projects identified in Exhibit A may have available balances that will not be expended for their originally approved activities; and

WHEREAS, the City wishes to authorize the reallocation of up to $70,000 in such available balances to the existing subrecipient projects identified in Exhibit B, without changing their approved scope; and

WHEREAS, the exact available balances and allocation among destination projects cannot yet be determined;

NOW, THEREFORE, BE IT RESOLVED by the City Council, of the City of Urbana, Illinois, as follows:

Section 1. Limited reallocation authority

Resolution No. 2023-02-013R, as previously amended, is further amended to authorize the City Administrator or designee (hereafter, the "designated city official") to reallocate available, previously obligated ARPA SLFRF balances from the "source" subrecipient awards identified in **Exhibit A** to one or more of the existing "destination" subrecipient projects identified in **Exhibit B**.

The combined amount of all reallocations authorized by this resolution shall not exceed $70,000. This dollar limitation applies to all transfers collectively, not separately to each source or destination award.

This resolution does not establish or retroactively establish a federal obligation. It authorizes the administrative reclassification of funds previously obligated by the City.

The authority to approve reallocations under this resolution expires as of December 31, 2026. The designated city official will provide Council with a final exact-dollar allocation schedule no later than April 30, 2027.

Section 2. Determination of final amounts and allocation

The determination of final amounts and allocation shall be based on available balances, eligible project needs, and the destination subrecipient's ability to expend the additional funds within the City's deadline.

While the combined amount of all reallocations authorized by this resolution shall not exceed $70,000, no minimum allocation to any destination award is required. The total amount reallocated may be less than $70,000, including zero dollars. Estimated available balances in **Exhibit A** are planning figures only. No fixed split is established by **Exhibit B**.

Section 3. That the City Clerk of the City of Urbana, Illinois, be and the same is hereby authorized to attest to the Mayor's signature as so authorized for and on behalf of the City of Urbana, Illinois.

PASSED BY THE CITY COUNCIL this _____ day of _____, _____.

AYES:

NAYS:

ABSTENTIONS:

_____

Darcy E. Sandefur, City Clerk

APPROVED BY THE MAYOR this _____ day of _____, _____.

_____

DeShawn B. Williams, Mayor

EXHIBITS

Exhibit A: Authorized source awards

Subrecipient	Project Name	Estimated available balance
Justine Petersen	Urbana Small Business Microloan Fund	Up to $42,000
Champaign County Regional Planning Commission	ARPA Project and Fiscal Management	Up to $16,000
City of Urbana Public Works Department	Equality and Quality of Life (EQL)	Up to $12,000
FirstFollowers	Urbana Community Peace Hub	$1.51

Actual adjustments shall be determined under Sections 1 and 2.

Exhibit B: Authorized destination awards

Subrecipient	Project Name
City of Urbana Public Works Department	Ward 3 Sanitary Sewer Lateral Lining (SSLL)
University YMCA	New American Welcome Center (NAWC)
Cunningham Township Supervisor's Office (CTSO)	Bridge to Home
Urbana Park District	Health & Wellness Center (HAWC)

CITY OF URBANA

City of Urbana
400 S. Vine Street, Urbana, IL 61801
www.urbanaillinois.us

MEMORANDUM TO THE MAYOR AND CITY COUNCIL

Meeting: November 16, 2026, Committee of the Whole
Subject: U-Cycle Recycling Tax

Summary

Action Requested
Establish a new set of U-Cycle taxes to fund recycling services.

Brief Background
Current U-Cycle fees have not kept pace with inflation and are insufficient to fund recycling services.

Relationship to City Services and Priorities

Impact on Core Services
Recycling is a component of waste management which is a core City duty.

Previous Council Actions

- The City of Urbana established U-Cycle curbside recycling service in September 1986. Urbana was one of the first communities in the State to establish a municipal curbside recycling program.
- In 1999, the City of Urbana expanded its recycling to include multifamily and dormitory properties.
- City Council has annually approved a Fee Schedule including recycling fees since 1995. The service was funded by property taxes prior to 1995.
- At the Committee of the Whole Meeting December 02, 2024, staff brought an ordinance to committee and council that removed the U-Cycle tax from the fee schedule on the premise that it is a tax, not a fee, and then set new U-Cycle tax rates for several years.

Discussion

Additional Background Information
U-Cycle service was provided by a single vendor for seven (7) years with limited tax rate increases. As such, when the contract and extensions ran out, seven years' worth of inflation was priced in the competitive bids, including significant post-COVID inflation. Additionally, since implementation of current contracts, diesel price increases have led to bill surcharges due to international conflict. Urbana is also within a limited waste industry market. At the start of the most recent contract negotiations in 2024, the curbside recycling service bid received two responses, while the multifamily

recycling service bid received only one response. Licensed haulers were personally contacted in an effort to garner as many competitive bids as possible.

Operations Impact
Without sufficient funding, U-Cycle will have to breach contract and discontinue service.

Fiscal and Budget Impact
U-Cycle fees are billed to all residents through the Urbana and Champaign Sanitary District (UCSD) bill. Funds are managed separate from the General Fund.

Proposed rate adjustments take into consideration the differing cost to provide Curbside service compared to the combined Multifamily and Dormitory service, equal rate growth over time for all payer types, and sufficient revenue to rebuild a safe fund balance.

	Current	**CY 27**	**CY 28**	**CY 29**	**CY 30**
Curbside	$6.25	$9.74	$10.03	$10.34	$10.65
Multifamily (per unit)	$3.75	$4.95	$5.10	$5.25	$5.41
Dormitory (per bed)	$3.00	$4.07	$4.20	$4.32	$4.45

	FY 27	**FY 28**	**FY 29**	**FY 30**
Ending Fund Balance	15%	18%	20%	23%

Community Impact
Impacts include a fee increase for residents or a discontinuation of recycling services for residents.

Recommendation
Next Steps
It is recommended that Council approve an ordinance establishing new U-Cycle rates.

Originated by: Scott Tess, Sustainability & Resilience Officer
Reviewed: Vince Gustafson, Public Works Director
Approved: Darius L. White, City Administrator

ORDINANCE NO. 2026- -

AN ORDINANCE AMENDING URBANA CITY CODE CHAPTER 22, SECTION 22-102 (Recycling Tax)

WHEREAS, the City of Urbana is a home rule unit of local government pursuant to Article VII, Section 6, of the Illinois Constitution, 1970, and may exercise any power and perform any function pertaining to its government and affairs, including the power to regulate for the protection of the public health, safety, and welfare; and

WHEREAS, the City Council heretofore enacted the Urbana City Code Section 14-7 to establish a schedule of fees for the various licenses, permits, fines, and other fees required under the Urbana City Code; and

WHEREAS, the City Council heretofore enacted Urbana City Code Section 22-102 to establish a Recycling Tax; and

WHEREAS, the City Council, after due consideration, finds that increasing the recycling tax as provided in this Ordinance will protect the public health, safety, and welfare; and

NOW, THEREFORE, BE IT ORDAINED by the City Council of the City of Urbana, Illinois, as follows:

Section 1. Urbana City Code Chapter 14, "Licenses and Permits," Section 14-7, "Schedule of Fees," Subsection (I), "Waste Management," Part 4, "Residential Recycling Tax," Part 5, "Dormitory Recycling Tax," and Part 6, "Multifamily Dwelling Recycling Tax," are hereby rescinded.

Section 2. Urbana City Code, Chapter 22, "Taxation," Section 22-102, "Residential Recycling Tax Imposed," subsection (a), is hereby amended and shall read as follows:

"Sec. 22-102. – Residential recycling tax imposed."

(a) A residential recycling tax is hereby imposed upon the use and privilege of occupying a dwelling

unit in a residential dwelling in the City of Urbana. The amount of the tax shall be:

(i) The monthly recycling tax for a dwelling unit in a residential dwelling shall be nine dollars and seventy-four cents ($9.74) effective January 1, 2027; ten dollars and three cents ($10.03) effective January 1, 2028; ten dollars and thirty-four cents ($10.34) effective January 1, 2029; and ten dollars and sixty-five cents ($10.65) effective January 1, 2030. Beginning January 1, 2031, and on January 1 of each year thereafter, the rates provided in this Section shall be adjusted based on the rate of inflation, determined by the change in the Consumer Price Index for All Urban Consumers (CPI-U) for a twelve (12) month period as of the end of June of the prior calendar year. The rate increase in a single year shall be limited to a maximum of five percent (5%), regardless of the calculated amount. The resulting rate shall be rounded to the nearest one-tenth of one cent ($0.001).

(ii) The monthly recycling tax for each unit in a multifamily dwelling shall be four dollars and ninety-five cents ($4.95) effective January 1, 2027; five dollars and ten cents ($5.10) effective January 1, 2028; five dollars and twenty-five cents ($5.25) effective January 1, 2029, and five dollars and forty-one cents ($5.41) effective January 1, 2030. Beginning January 1, 2031, and on January 1 of each year thereafter, the rates provided in this Section shall be adjusted based on the rate of inflation, determined by the change in the Consumer Price Index for All Urban Consumers (CPI-U) for a twelve (12) month period as of the end of June of the prior calendar year. The rate increase in a single year shall be limited to a maximum of five percent (5%), regardless of the calculated amount. The resulting rate shall be rounded to the nearest one-tenth of one cent ($0.001).

(iii) The monthly recycling tax for a dormitory shall be four dollars and seven cents ($4.07) times the residential capacity of the dormitory effective January 1, 2027; four dollars and twenty cents ($4.20) effective January 1, 2028; four dollars and thirty-two cents ($4.32) effective

January 1, 2029; and four dollars and forty-five cents ($4.45) effective January 1, 2030. Beginning January 1, 2031, and on January 1 of each year thereafter, the rates provided in this Section shall be adjusted based on the rate of inflation, determined by the change in the Consumer Price Index for All Urban Consumers (CPI-U) for a twelve (12) month period as of the end of June of the prior calendar year. The rate increase in a single year shall be limited to a maximum of five percent (5%), regardless of the calculated amount. The resulting rate shall be rounded to the nearest one-tenth of one cent ($0.001).

Section 3. Those sections, paragraphs, and provisions of the Urbana City Code that are not expressly amended or repealed by this Ordinance are hereby re-enacted, and it is expressly declared to be the intention of this Ordinance not to repeal or amend any portions of the Urbana City Code other than those expressly set forth as amended or repealed in this Ordinance. The invalidity of any section or provision of this Ordinance hereby passed and approved shall not invalidate other sections or provisions thereof.

Section 4. This Ordinance shall not be construed to affect any suit or proceeding pending in any court, or any rights acquired, or a liability incurred, or any cause or causes of action acquired or existing prior to the effective date of this Ordinance; nor shall any right or remedy of any character be lost, impaired, or affected by this Ordinance.

Section 5. The City Clerk is directed to publish this Ordinance in pamphlet form by authority of the corporate authorities, and this Ordinance shall be in full force and effect on January 1, 2027, after its passage and publication in accordance with Section 1-2-4 of the Illinois Municipal Code.

This Ordinance is hereby passed by the affirmative vote, the "ayes" and "nays" being called, of a majority of the members of the Council of the City of Urbana, Illinois, at a meeting of said Council.

PASSED BY THE CITY COUNCIL this _____ Day of _____, 2026.

AYES:

NAYS:

ABSTAINS:

_____
Darcy Sandefur, City Clerk.

APPROVED BY THE MAYOR this ____ Day of _____, 2026.

_____
DeShawn Williams, Mayor.

Bucket 1 - Police Records, Reporting & Case Management

Purpose: Systems used to document police activity, manage cases, issue citations, receive reports, and maintain official Department records.

- **L22** – DepartmentWare
- **L14** – CAD & RMS
- **L19** – CrimeStoppers
- **L51** – Stolen Bike Search

Bucket 2 - Criminal Justice Information Systems

Purpose: Systems providing access to criminal justice, offender, warrant, missing persons, and public safety information maintained by governmental agencies.

- **L16** – Champaign County Warrants Database
- **L18** – Concealed Carry License Database
- **L35** – Illinois Department of Corrections Inmate Search
- **L44** – NamUs (National Missing and Unidentified Persons System)
- **L46** – N-DEx (National Data Exchange)
- **L55** – Winols Sex Offender Registry

Bucket 3 - Intelligence Sharing & Information Exchange Systems

Purpose: Systems that facilitate intelligence sharing and coordination among public safety and law enforcement agencies.

- **L25** – El Paso Intelligence Center (EPIC)
- **L37** – Illinois Statewide Terrorism and Intelligence Center (STIC)
- **L23** – DHS (Department of Homeland Security)

Bucket 4 - Investigative Research & Open-Source Intelligence (OSINT)

Purpose: Tools used to locate, verify, analyze, and investigate publicly available information, commercial records, and social media content.

Investigative Research Tools

- **L15** – Carfax for Police
- **L33** – IDIcore
- **L41** – LexisNexis Accurint

Social Media & Social Media Analysis

- **L28** – Geofeedia
- **L50** – Social Media Analysis Tools (e.g., X1 Social Discovery)

Bucket 5 - Biometric Identification Systems

Purpose: Systems used to identify or verify individuals through fingerprints, DNA, and other biometric identifiers.

- **L30** – IAFIS (Integrated Automated Fingerprint Identification System)
- **L32** – IDENT (Automated Biometric Identification System)

Bucket 6 - Covert Video & Thermal Surveillance Systems

Purpose: Devices used to support lawful criminal investigations and public safety operations.

- Temporarily Deployed Covert Surveillance Cameras
- Thermal Imaging Device

Bucket 7 - Digital Forensics & Mobile Device Investigation Systems

Purpose: Systems used to lawfully extract, analyze, preserve, and manage digital evidence obtained from mobile devices, computers, digital storage media, and telecommunications providers.

- Cellebrite
- Magnet AXIOM
- Cellular Provider Records
- Cell Site Location Information (CSLI)

Bucket 8 - Specialized Investigative Systems

Purpose: Systems supporting specialized investigative functions such as firearms tracing, ballistic analysis, and travel document verification.

- **L13** – ATF E-Trace
- **L43** – Lost and Stolen Passport Database

Excluded Category: Data Analytics, Communications & Information Storage Systems

Analytics & Reporting

- VICAP – Violent Criminal Apprehension Program (L70)
- Data Analytic Tools (L76)
    - LE Analytics
    - LE Explorer
    - Citizen Connect
    - Public Safety Analytics
    - Dynamic Reporting
    - Decision Support Systems
    - ArcGIS

Communications

- Internal & External Communication (L78)
    - Evertel

Information Storage

- File Storage (L82)
    - Crime Drive

Administrative Systems

- Data Collection on Employees (L83)
    - Background Investigation Files

Police Records, Reporting & Case Management Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Police Records, Reporting & Case Management Systems.

Systems governed by this policy include DepartmentWare, Computer-Aided Dispatch and Records Management System (CAD & RMS), CrimeStoppers, and Stolen Bike Search Tool (Project529).

The purpose of this policy is to:

• Define authorized and prohibited uses.

• Protect privacy, civil liberties, and constitutional rights.

• Ensure accountability and oversight.

• Establish standards governing access to, retention of, and dissemination of information maintained within these systems.

• Maintain the integrity, security, and accuracy of Department records.

2. Authorized Uses

Police Records, Reporting & Case Management Systems may be used only for legitimate law enforcement, criminal justice, public safety, administrative, and records-management purposes consistent with applicable law and Department policy.

Authorized uses include:

• Documenting calls for service, incidents, arrests, and investigations.

• Maintaining official police records and case files.

• Tracking investigative case activity and workflow.

• Managing property, evidence, and associated records.

• Receiving information submitted by members of the public through authorized reporting mechanisms.

• Supporting information sharing among Department personnel.

• Assisting supervisors with records review and case oversight.

• Supporting records retention and records-management requirements.

• Enhancing operational efficiency and accountability.

• Supporting criminal investigations and public safety operations.

All use must be related to an official Department purpose.

3. Prohibited Uses

Police Records, Reporting & Case Management Systems shall not be used for:

• Accessing records without a legitimate law enforcement, criminal justice, or governmental purpose.

• Accessing records relating to friends, family members, coworkers, elected officials, public figures, or other individuals absent a documented official purpose.

• Conducting searches based on personal curiosity.

• Disseminating information to unauthorized persons.

• Accessing information for private, political, commercial, or personal purposes.

• Altering, deleting, concealing, or modifying records without authorization.

• Using Department records to monitor lawful First Amendment activity absent a legitimate law enforcement purpose.

• Accessing records in a manner that violates Department policy or applicable law.

4. Approval and Oversight

Access to Police Records, Reporting & Case Management Systems is limited to authorized personnel whose official duties require such access.

Supervisors are responsible for ensuring that:

• Personnel utilize systems only for authorized purposes.

• User permissions are appropriate for assigned responsibilities.

• Apparent misuse is investigated and addressed.

• Records-management practices comply with Department policy and legal requirements.

User activity may be logged, reviewed, and audited to ensure compliance with policy and law.

5. Exigent Circumstances

Exigent circumstances involving Police Records, Reporting & Case Management Systems may arise when immediate access to Department records, case information, calls for service, investigative information, or other operational records is necessary to protect life, prevent serious bodily injury, locate endangered persons, respond to active threats, or support rapidly evolving public safety incidents.

Examples may include:

• Locating a missing, abducted, suicidal, or endangered person using available records and historical law enforcement contacts.

• Identifying suspects, victims, witnesses, or associated individuals during an ongoing violent crime investigation.

• Accessing calls for service, incident reports, or case information during an active shooter, hostage situation, barricaded subject incident, or other critical public safety event.

• Reviewing prior incident reports or investigative records to identify known safety concerns during an active incident.

• Obtaining information necessary to coordinate emergency response efforts with other public safety agencies.

In exigent circumstances, authorized personnel may access available records and systems consistent with their assigned access privileges and official duties. Such access does not eliminate the requirement to comply with applicable law, Department policy, audit requirements, or records-management standards.

6. Data Retention, Access, and Dissemination

Records maintained within these systems shall be retained in accordance with:

• Applicable records-retention schedules.

• Department policy.

• State and federal law.

• Court orders and evidentiary requirements.

Access is limited to authorized personnel.

Information may be disseminated only as authorized by law, Department policy, court order, interagency agreement, or other official governmental purpose.

7. Third-Party Data Handling

Where Department records are maintained, supported, stored, or processed by third-party vendors, contractual safeguards shall govern access, maintenance, and security.

The City retains ownership and control of Department-generated records, subject to applicable law.

Third-party providers shall not access Department information except as necessary to provide authorized services or as otherwise required by law.

8. Training and Authorized Users

Only authorized personnel may access Police Records, Reporting & Case Management Systems.

Personnel granted access shall receive training appropriate to their assigned responsibilities, including:

• System operation.

• Privacy and confidentiality requirements.

• Records-management obligations.

• Information-security requirements.

• Applicable legal restrictions.

• Audit and accountability standards.

9. Auditing, Accountability, and Discipline

System use is subject to:

• Supervisory review.

• Audit logging.

• Internal compliance reviews.

• Investigation of suspected misuse.

Violations of this policy may result in disciplinary action, loss of system access, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements regarding the use of Police Records, Reporting & Case Management Systems.

Information regarding the use of these systems may be included in annual surveillance technology reporting, subject to applicable legal restrictions and operational considerations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, technology changes, operational needs, and community expectations.

Revisions will be submitted and approved as required by applicable ordinance requirements and Department policy.

Police Records Reporting & Case Management Systems Use Report

1. Description of the Surveillance Technology and How It Works

The Urbana Police Department utilizes Police Records, Reporting & Case Management Systems to document law enforcement activities, maintain official Department records, manage investigative and administrative workflows, and receive information submitted by members of the public.

Systems within this category include:

- DepartmentWare - $5,000/yr
- Computer-Aided Dispatch and Records Management System (CAD & RMS) - 14,777.25/qt. $59,109.00/yr
- CrimeStoppers
- Stolen Bike Search Tool (Project529) - $25/yr

These systems collect, store, organize, retrieve, and manage information generated through Department operations and public interactions. Information may be entered by Department personnel, submitted by members of the public, received from other governmental agencies, or generated during law enforcement activities.

Records maintained in these systems may include incident reports, calls for service, case information, property information, bicycle registration information, investigative records, and other official Department records.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to assist officers, investigators, and other authorized personnel in carrying out law enforcement and public safety responsibilities.

Authorized uses include:

- Documenting calls for service, incidents, arrests, and investigations.
- Maintaining official police records and case files.
- Tracking investigative case activity and workflow.
- Managing property, evidence, and associated records.
- Receiving information submitted by members of the public.
- Supporting information sharing among Department personnel.
- Assisting supervisors with records review and case oversight.

- Supporting records retention and records-management requirements.
- Enhancing operational efficiency and accountability.
- Supporting criminal investigations and public safety operations.

These systems may only be used for official law enforcement purposes consistent with applicable law and policy.

3. Deployment Authorization and Operational Oversight

Access to Police Records, Reporting & Case Management Systems is restricted to authorized personnel who have a demonstrated business need and have received required training.

User credentials are assigned individually and may not be shared. Access levels are based upon job responsibilities and operational necessity.

Supervisors, system administrators, and governing agencies may monitor system use and conduct audits to ensure compliance with applicable policies, security requirements, and legal standards.

Unauthorized access, dissemination, or misuse of information may result in disciplinary action, revocation of system access, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

- Annual access and subscription costs: $64,134
- State or federal user fees: NA
- Required training costs: NA
- Administrative support costs: NA
- Funding source(s): PD Budget

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Police Records, Reporting & Case Management Systems could result in a disparate impact on protected classes.

Safeguards include:

- Purpose-based access restrictions
- Supervisor oversight
- Required user training

- Audit logging and review
- Documentation requirements
- Compliance with applicable laws and policies

The Department does not access or use these systems for discriminatory purposes or based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Information obtained through these systems is utilized in connection with legitimate public safety, investigative, and criminal justice functions.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that police records and case-management systems may contain sensitive personal information regarding victims, witnesses, complainants, suspects, arrested persons, and other individuals whose information is documented as part of law enforcement operations.

Safeguards include:

Restricted Access
Only authorized personnel with a legitimate law enforcement or criminal justice purpose may access these systems.

Information Security
Access credentials, user permissions, and security controls are designed to prevent unauthorized access and disclosure.

Audit and Accountability Measures
System activity may be recorded and audited by the Department, state agencies, federal agencies, or system administrators.

Information Sharing Limitations
Information obtained through these systems may only be shared as permitted by law, policy, court order, or authorized criminal justice purposes.

Protection of Constitutional Rights
The Department does not use Police Records, Reporting & Case Management Systems to monitor, track, or investigate individuals solely because they engage in lawful First Amendment activities.

7. Data Storage, Retention, and Third-Party Access

Some systems within this category are owned or maintained by the Department, vendors, or partner organizations that provide records-management, case-management, or information-reporting services.

The Department may retain information obtained through these systems when incorporated into official police reports, investigative files, case records, intelligence products, or evidentiary records as permitted by law and policy.

Third-party access is governed by the policies of the originating agency, vendor agreements, and applicable laws concerning criminal justice information.

8. Exigent Circumstances Use

Exigent circumstances involving Police Records, Reporting & Case Management Systems may arise when immediate access to information is necessary to protect life, prevent serious bodily injury, locate endangered persons, apprehend dangerous offenders, respond to active threats, or address rapidly evolving public safety emergencies.

Examples may include:

- Locating a missing, abducted, suicidal, or endangered person.
- Identifying a suspect involved in a violent crime who presents an imminent threat to public safety.
- Determining whether an individual involved in an active incident is the subject of an outstanding warrant or protection order.
- Confirming the identity of an individual when accurate identification is necessary to protect officers or the public.
- Obtaining information needed to support an active criminal investigation involving an immediate threat of violence.
- Assisting another law enforcement agency responding to an ongoing emergency or active public safety threat.

In exigent circumstances, authorized personnel may access available Police Records, Reporting & Case Management Systems consistent with their assigned access privileges and official duties.

Exigent circumstances do not eliminate the requirement to comply with applicable laws, user agreements, audit requirements, security standards, or Department policies.

Information obtained through these systems remains subject to all restrictions governing access, retention, dissemination, and disclosure.

9. Compliance With State and Federal Law

The use of Police Records, Reporting & Case Management Systems will comply with all applicable state and federal laws, regulations, user agreements, and security requirements.

Such requirements may include:

- Criminal history record dissemination laws
- State and federal privacy laws
- Records retention requirements
- Information security requirements
- Court orders and judicial directives
- Governing agency policies and procedures

Personnel authorized to access these systems are required to comply with all applicable restrictions on access, use, disclosure, and dissemination of information.

10. Summary

Police Records, Reporting & Case Management Systems provide authorized personnel with tools to document law enforcement activities, manage case information, maintain official Department records, receive information from the public, and support criminal investigations and public safety operations.

Access to these systems is restricted, audited, and governed by legal and policy safeguards designed to protect privacy, civil rights, and civil liberties while supporting legitimate law enforcement objectives.

Criminal Justice Information Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Criminal Justice Information Systems.

The purpose of this policy is to:

- Define authorized and prohibited uses.
- Protect privacy, civil liberties, and constitutional rights.
- Ensure accountability and oversight.
- Promote lawful access to criminal justice information.
- Establish standards for access, use, retention, and dissemination of information obtained through these systems.

2. Authorized Uses

Criminal Justice Information Systems may be used only for legitimate law enforcement, criminal justice, and public safety purposes consistent with applicable law, user agreements, and Department policy.

Authorized uses include:

- Conducting criminal investigations.
- Verifying warrants, protection orders, offender status, and other criminal justice information.
- Locating missing, endangered, or wanted persons.
- Identifying individuals, vehicles, and property.
- Identifying registered sex offenders.
- Verifying correctional, inmate, or offender information.
- Supporting officer safety.
- Supporting public safety operations.
- Assisting other criminal justice agencies with legitimate investigations.
- Fulfilling other authorized criminal justice functions.

All use must be connected to an official law enforcement or criminal justice purpose.

3. Prohibited Uses

Criminal Justice Information Systems shall not be used for:

- Accessing information without a legitimate law enforcement or criminal justice purpose.
- Conducting searches based on personal curiosity.
- Accessing records relating to friends, family members, coworkers, public officials, public figures, or other individuals absent a documented official purpose.
- Conducting background inquiries for personal, political, commercial, or non-governmental purposes.
- Accessing, retaining, or disseminating information in violation of law, policy, or user agreements.
- Using criminal justice information to monitor individuals based solely on race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.
- Monitoring lawful First Amendment activities absent a legitimate law enforcement purpose.
- Sharing criminal justice information with unauthorized individuals or organizations.

4. Approval and Oversight

Access to Criminal Justice Information Systems is restricted to authorized personnel whose official duties require access.

Supervisors are responsible for ensuring that:

- Personnel have a legitimate business need before access is granted.
- Access permissions remain appropriate to assigned duties.
- Users complete any required certifications or training.
- Potential misuse is investigated and addressed.
- Department personnel comply with all applicable user agreements, security requirements, and Department policies.

User activity may be monitored, reviewed, and audited by the Department and by the agencies responsible for administering the systems.

5. Exigent Circumstances

Exigent circumstances involving Criminal Justice Information Systems may arise when immediate access to criminal justice information is necessary to protect life, prevent serious bodily injury, locate endangered persons, apprehend dangerous offenders, respond to active threats, or address rapidly evolving public safety emergencies.

Examples may include:

- Locating a missing, abducted, suicidal, or endangered person.
- Identifying a suspect involved in a violent crime who presents an imminent threat to public safety.
- Determining whether an individual involved in an active incident is associated with an outstanding warrant, protection order, missing person record, offender record, or other criminal justice information relevant to the incident.
- Confirming the identity of an individual when accurate identification is necessary to protect officers or the public.
- Obtaining information needed to support an active criminal investigation involving an immediate threat of violence.
- Assisting another law enforcement agency responding to an ongoing emergency or active public safety threat.

In exigent circumstances, authorized personnel may access available Criminal Justice Information Systems consistent with their assigned access privileges and official duties. Exigent circumstances do not eliminate the requirement to comply with applicable laws, user agreements, audit requirements, security standards, or Department policies.

Information obtained through these systems remains subject to all restrictions governing access, retention, dissemination, and disclosure.

6. Data Retention, Access, and Dissemination

Many Criminal Justice Information Systems are owned and maintained by state, federal, regional, or other governmental entities.

Information accessed through these systems may be incorporated into official police reports, investigative files, evidentiary records, or other Department records when authorized and necessary for official purposes.

Access is restricted to authorized users.

Information obtained through these systems may be disseminated only as permitted by applicable law, governing agency requirements, user agreements, court order, or Department policy.

7. Third-Party Data Handling

Most Criminal Justice Information Systems are operated by governmental entities outside the control of the City of Urbana.

The Department will comply with applicable user agreements, operational requirements, and security standards established by the agency responsible for maintaining each system.

Where vendors or contractors provide technical support or administrative services, access shall be limited to authorized functions and governed by applicable contracts, agreements, and legal requirements.

8. Training and Authorized Users

Only authorized personnel may access Criminal Justice Information Systems.

Personnel granted access shall complete any required training or certification before receiving access and shall maintain any required credentials.

Training may include:

- System operation and security requirements.
- Privacy and confidentiality requirements.
- Authorized and prohibited uses.
- Information dissemination restrictions.
- Audit and accountability requirements.
- Applicable legal and regulatory obligations.

9. Auditing, Accountability, and Discipline

Use of Criminal Justice Information Systems is subject to:

- Supervisory review.
- Audit logging.
- Internal compliance reviews.
- Audits conducted by governing agencies.
- Investigation of suspected misuse.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Criminal Justice Information Systems.

Information regarding system usage, compliance activities, and operational impacts may be included in annual surveillance technology reporting, subject to applicable legal restrictions and security considerations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, criminal justice information requirements, technological changes, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Criminal Justice Information Systems Use Report

1. Description of the Surveillance Technology and How It Works

Criminal Justice Information Systems

The Urbana Police Department utilizes Criminal Justice Information Systems that provide authorized access to criminal justice records, offender information, warrant information, missing persons records, public safety notifications, and other law enforcement information maintained by local, state, and federal agencies.

Systems within this category include:

- Champaign County Warrants Database
- Concealed Carry License Database
- Illinois Department of Corrections Inmate Search
- National Missing and Unidentified Persons System (NamUs)
- National Data Exchange (N-DEx)
- Winols Sex Offender Registry

These systems allow authorized personnel to search, retrieve, and review records maintained by governmental agencies. Information is generally entered and maintained by the originating agency and made available to authorized users for law enforcement, criminal justice, and public safety purposes. The Urbana Police Department generally accesses information contained within these systems but is not the owner or custodian of the underlying databases.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to assist officers, investigators, and other authorized personnel in carrying out law enforcement and public safety responsibilities.

Authorized uses include:

• Identifying persons, vehicles, and property

• Determining the existence of warrants or court orders

• Verifying criminal justice status information

• Locating missing persons

• Identifying registered sex offenders

• Supporting criminal investigations

• Enhancing officer safety

• Supporting criminal investigations and public safety operations

• Facilitating information sharing among criminal justice agencies

These systems may only be used for official law enforcement purposes consistent with applicable law and policy.

3. Deployment Authorization and Operational Oversight

Access to Criminal Justice Information Systems is restricted to authorized personnel who have a demonstrated business need and have received required training.

User credentials are assigned individually and may not be shared. Access levels are based upon job responsibilities and operational necessity.

Supervisors, system administrators, and governing agencies may monitor system use and conduct audits to ensure compliance with applicable policies, security requirements, and legal standards.

Unauthorized access, dissemination, or misuse of information may result in disciplinary action, revocation of system access, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

• Annual access and subscription costs: No known cost.

• State or federal user fees: NA

• Required training costs: NA

• Administrative support costs: NA

• Funding source(s): NA

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Criminal Justice Information Systems could result in a disparate impact on protected classes.

Safeguards include:

• Purpose-based access restrictions

• Supervisor oversight

• Required user training

• Audit logging and review

• Documentation requirements

• Compliance with applicable laws and policies

The Department does not access or use these systems for discriminatory purposes or based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Information obtained through these systems is utilized in connection with legitimate public safety, investigative, and criminal justice functions.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that criminal justice databases can contain sensitive personal information regarding individuals who may be victims, witnesses, subjects of investigations, registrants, incarcerated persons, missing persons, or individuals otherwise involved in governmental processes.

Safeguards include:

Restricted Access

Only authorized personnel with a legitimate law enforcement or criminal justice purpose may access these systems.

Information Security

Access credentials, user permissions, and security controls are designed to prevent unauthorized access and disclosure.

Audit and Accountability Measures

System activity may be recorded and audited by the Department, state agencies, federal agencies, or system administrators.

Information Sharing Limitations

Information obtained through these systems may only be shared as permitted by law, policy, court order, or authorized criminal justice purposes.

Protection of Constitutional Rights

The Department does not use Criminal Justice Information Systems to monitor, track, or investigate individuals solely because they engage in lawful First Amendment activities.

7. Data Storage, Retention, and Third-Party Access

Many systems within this category are owned and maintained by state, federal, regional, or other governmental entities. Information accessed through these systems remains subject to the policies, retention schedules, security requirements, and legal authorities established by the owning agency.

The Department may retain information obtained through these systems when incorporated into official police reports, investigative files, case records, intelligence products, or evidentiary records as permitted by law and policy.

Third-party access is governed by the policies of the originating agency and applicable laws concerning criminal justice information.

8. Exigent Circumstances Use

Exigent circumstances involving Criminal Justice Information Systems may arise when immediate access to criminal justice information is necessary to protect life, prevent serious bodily injury, locate endangered persons, apprehend dangerous offenders, respond to active threats, or address rapidly evolving public safety emergencies.

Examples may include:

• Locating a missing, abducted, suicidal, or endangered person.

• Identifying a suspect involved in a violent crime who presents an imminent threat to public safety.

• Determining whether an individual involved in an active incident is the subject of an outstanding warrant or protection order.

• Confirming the identity of an individual when accurate identification is necessary to protect officers or the public.

• Obtaining information needed to support an active criminal investigation involving an immediate threat of violence.

• Assisting another law enforcement agency responding to an ongoing emergency or active public safety threat.

In exigent circumstances, authorized personnel may access available Criminal Justice Information Systems consistent with their assigned access privileges and official duties. Exigent circumstances do not eliminate the requirement to comply with applicable laws, user agreements, audit requirements, security standards, or Department policies.

Information obtained through these systems remains subject to all restrictions governing access, retention, dissemination, and disclosure.

9. Compliance With State and Federal Law

The use of Criminal Justice Information Systems will comply with all applicable state and federal laws, regulations, user agreements, and security requirements.

Such requirements may include:

• Criminal history record dissemination laws

• State and federal privacy laws

• Records retention requirements

• Information security requirements

• Court orders and judicial directives

• Governing agency policies and procedures

Personnel authorized to access these systems are required to comply with all applicable restrictions on access, use, disclosure, and dissemination of information.

10. Summary

Criminal Justice Information Systems provide officers and investigators with access to critical public safety information maintained by authorized governmental entities. These systems support investigations, warrant verification, missing person investigations, offender identification, information sharing, and officer safety functions. Access is restricted, audited, and governed by legal and policy safeguards designed to protect privacy, civil rights, and civil liberties while supporting legitimate law enforcement objectives.

Intelligence Sharing & Information Exchange Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Intelligence Sharing and Information Exchange Systems.

The purpose of this policy is to:

- Define authorized and prohibited uses.
- Protect privacy, civil liberties, and constitutional rights.
- Ensure accountability and oversight.
- Establish standards for the sharing, retention, and dissemination of intelligence information.
- Promote lawful and responsible information exchange with authorized public safety and law enforcement partners.

2. Authorized Uses

Intelligence Sharing and Information Exchange Systems may be used only for legitimate law enforcement, investigative, intelligence, and public safety purposes consistent with applicable law and Department policy.

Authorized uses include:

- Supporting criminal investigations.
- Sharing investigative leads and intelligence information.
- Identifying criminal activity patterns, trends, and connections.
- Enhancing officer safety.
- Assisting with multi-jurisdictional investigations.
- Supporting public safety operations and threat assessments.
- Identifying relationships between criminal incidents occurring in different jurisdictions.
- Coordinating investigative efforts with authorized law enforcement partners.
- Supporting intelligence analysis related to criminal activity and public safety threats.

All use must be connected to a legitimate law enforcement, investigative, or public safety objective.

3. Prohibited Uses

Intelligence Sharing and Information Exchange Systems shall not be used for:

- Collecting, maintaining, or disseminating information without a legitimate law enforcement or public safety purpose.
- Creating intelligence files based solely upon race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.
- Monitoring, recording, or maintaining information regarding lawful First Amendment activities absent a legitimate law enforcement purpose.
- Sharing unverified, speculative, or knowingly inaccurate information.
- Accessing systems for personal, political, commercial, or non-governmental purposes.
- Disseminating information to unauthorized individuals or organizations.
- Retaining information in violation of applicable law, policy, or governing agency requirements.
- Conducting inquiries based on personal curiosity or non-official interests.

4. Approval and Oversight

Access to Intelligence Sharing and Information Exchange Systems is restricted to authorized personnel whose official duties require such access.

Supervisors are responsible for ensuring that:

- Personnel use these systems only for authorized purposes.
- Information entered into or shared through these systems meets applicable standards.
- Access privileges remain appropriate to assigned duties.
- Potential misuse is investigated and addressed.
- Personnel comply with applicable laws, information-sharing agreements, and Department policies.

System use may be monitored, audited, and reviewed by the Department, governing agencies, or system administrators.

5. Exigent Circumstances

Exigent circumstances involving Intelligence Sharing and Information Exchange Systems may arise when immediate access to, or dissemination of, intelligence information is necessary to protect life, prevent serious bodily injury, locate dangerous individuals, respond to active threats, or address rapidly evolving public safety emergencies.

Examples may include:

- Responding to an active shooter, hostage situation, or other critical public safety incident.
- Sharing time-sensitive threat information regarding a credible threat to the public, critical infrastructure, schools, or government facilities.
- Assisting in the location and apprehension of a violent offender believed to present an immediate danger to the community.
- Coordinating investigative information with local, state, federal, or international law enforcement partners during an ongoing emergency.
- Identifying intelligence information needed to support officer safety during a critical incident.
- Obtaining or disseminating information necessary to prevent imminent criminal activity or violence.

In exigent circumstances, authorized personnel may access available Intelligence Sharing and Information Exchange Systems or disseminate information through those systems consistent with their assigned access privileges and official duties.

Exigent circumstances do not eliminate the requirement to comply with applicable laws, Department policy, documentation requirements, information-sharing standards, or privacy protections. Information shared during exigent circumstances shall be limited to what is reasonably necessary to address the immediate public safety need.

6. Data Retention, Access, and Dissemination

Information obtained through Intelligence Sharing and Information Exchange Systems may be retained when incorporated into official police reports, investigative files, intelligence products, or other authorized Department records.

Access is restricted to authorized personnel.

Information may be disseminated only to authorized agencies, officials, or individuals as permitted by law, Department policy, information-sharing agreements, or official law enforcement purposes.

Information retained by external systems remains subject to the retention schedules, security requirements, and legal authorities established by the agencies responsible for maintaining those systems.

7. Third-Party Data Handling

Most Intelligence Sharing and Information Exchange Systems are operated and maintained by state, federal, international, or multi-agency entities.

The Department will comply with all applicable operating rules, information-sharing requirements, user agreements, and security standards established by the agencies responsible for administering those systems.

The Department does not control the internal storage, architecture, retention schedules, or auditing mechanisms of systems maintained by external entities.

8. Training and Authorized Users

Only authorized personnel may access Intelligence Sharing and Information Exchange Systems.

Personnel granted access shall complete any required training and maintain any required certifications or credentials.

Training may include:

- Authorized and prohibited uses.
- Intelligence sharing standards.
- Privacy and civil liberties protections.
- Constitutional considerations.
- Information security requirements.
- Audit and accountability requirements.
- Applicable laws and regulations.

9. Auditing, Accountability, and Discipline

Use of Intelligence Sharing and Information Exchange Systems is subject to:

- Supervisory review.
- Audit logging.
- Internal compliance reviews.
- Audits conducted by governing agencies.
- Investigation of suspected misuse.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Intelligence Sharing and Information Exchange Systems.

Information regarding system usage, compliance efforts, and operational impacts may be included in annual surveillance technology reporting, subject to legal, security, and investigative limitations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, evolving technology, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Intelligence Sharing & Information Exchange Systems Use Report

1. Description of the Surveillance Technology and How It Works

Intelligence Sharing & Information Exchange Systems

The Urbana Police Department utilizes Intelligence Sharing and Information Exchange Systems that facilitate the lawful sharing of investigative information, criminal intelligence, threat information, and public safety information between authorized law enforcement agencies and public safety partners.

Systems within this category include:

- El Paso Intelligence Center (EPIC)
- Europol Information System (EIS)
- Illinois Statewide Terrorism and Intelligence Center (STIC)
- Evertel Genasys $7,560

These systems allow authorized users to access, receive, review, and share information relevant to criminal investigations, public safety threats, organized criminal activity, officer safety concerns, and regional or multi-jurisdictional investigations. Information available through these systems is generally maintained by participating agencies and shared with authorized users for legitimate law enforcement and public safety purposes.

The Urbana Police Department may access information from these systems and, when authorized, may contribute information that supports criminal investigations, public safety initiatives, or intelligence-sharing efforts.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to facilitate information sharing among authorized law enforcement, intelligence, and public safety agencies.

Authorized uses include:

• Supporting criminal investigations

• Sharing investigative leads and intelligence information

• Enhancing officer safety

• Identifying criminal activity patterns and trends

• Assisting with multi-jurisdictional investigations

• Supporting public safety operations

• Identifying connections between criminal incidents occurring in different jurisdictions

• Coordinating information exchange among law enforcement partners

• Supporting threat assessments and intelligence analysis

These systems may only be used for authorized law enforcement and public safety purposes consistent with applicable law and Department policy.

3. Deployment Authorization and Operational Oversight

Access to Intelligence Sharing and Information Exchange Systems is restricted to authorized personnel who have a legitimate operational need and have received any required training.

User accounts are assigned individually, and access levels are governed by Department policy, system requirements, and governing agency standards. Personnel granted access must comply with all applicable user agreements, information-sharing requirements, security standards, and Department policies.

System activity may be monitored or audited by the Department, system administrators, or the agencies responsible for maintaining the systems.

Unauthorized access, use, dissemination, or disclosure of information may result in disciplinary action, loss of access privileges, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

• Annual subscription or access costs: $7,560

• Membership fees: NA

• Training costs: NA

• Administrative support costs: NA

• Funding source(s): PD Budget

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Intelligence Sharing and Information Exchange Systems could result in a disparate impact on protected classes.

Safeguards include:

• Purpose-based access restrictions

• Supervisor oversight

• User training requirements

• Auditing and accountability measures

• Compliance with applicable laws and policies

• Information-sharing standards established by participating agencies

The Department does not collect, access, or share information through these systems based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Information is exchanged only for legitimate law enforcement, investigative, and public safety purposes.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that intelligence-sharing systems may contain sensitive information concerning criminal investigations, public safety threats, criminal organizations, suspects, victims, witnesses, and other individuals associated with law enforcement activities.

Safeguards include:

Restricted Access

Access is limited to authorized personnel with a legitimate law enforcement, investigative, or public safety purpose.

Information Validation Standards

Information shared through these systems should be based upon documented observations, investigations, official records, intelligence products, or other authorized sources consistent with applicable standards and policies.

Audit and Accountability Measures

System activity may be monitored and audited to detect unauthorized access, dissemination, or misuse.

Information Sharing Limitations

Information may only be disseminated to authorized agencies and individuals consistent with system rules, applicable law, and official law enforcement purposes.

Protection of Constitutional Rights

The Department does not utilize Intelligence Sharing and Information Exchange Systems to monitor, collect, maintain, or disseminate information regarding individuals solely because they

engage in lawful activities protected by the United States Constitution or the Illinois Constitution.

Investigative activity must be based upon legitimate law enforcement objectives and not solely on an individual's protected beliefs, viewpoints, associations, or activities.

7. Data Storage, Retention, and Third-Party Access

Most systems within this category are operated and maintained by state, federal, international, or multi-agency entities. Information contained within these systems remains subject to the policies, retention schedules, legal authorities, and security requirements established by the system owner.

Information obtained through these systems may be incorporated into official police reports, investigative files, intelligence products, or other Department records when authorized and necessary for legitimate law enforcement purposes.

Third-party access is governed by applicable laws, information-sharing agreements, and policies established by the agencies responsible for maintaining the systems.

8. Exigent Circumstances Use

Exigent circumstances involving Intelligence Sharing and Information Exchange Systems may arise when immediate access to, or dissemination of, intelligence information is necessary to protect life, prevent serious bodily injury, locate dangerous individuals, respond to active threats, or address rapidly evolving public safety emergencies.

Examples may include:

• Responding to an active shooter, hostage situation, or other critical public safety incident.

• Sharing time-sensitive threat information regarding a credible threat to the public, critical infrastructure, schools, or government facilities.

• Assisting in the location and apprehension of a violent offender believed to present an immediate danger to the community.

• Coordinating investigative information with local, state, federal, or international law enforcement partners during an ongoing emergency.

• Identifying intelligence information needed to support officer safety during a critical incident.

• Obtaining or disseminating information necessary to prevent imminent criminal activity or violence.

In exigent circumstances, authorized personnel may access available Intelligence Sharing and Information Exchange Systems or disseminate information through those systems consistent with their assigned access privileges and official duties.

Exigent circumstances do not eliminate the requirement to comply with applicable laws, Department policy, documentation requirements, information-sharing standards, or privacy protections. Information shared during exigent circumstances shall be limited to what is reasonably necessary to address the immediate public safety need.

9. Compliance With State and Federal Law

The use of Intelligence Sharing and Information Exchange Systems will comply with all applicable federal, state, and local laws, information-sharing agreements, user requirements, and governing agency policies.

Such requirements may include:

• Privacy and civil liberties protections

• Information security requirements

• Criminal intelligence standards

• Records retention requirements

• Information dissemination restrictions

• Applicable state and federal confidentiality laws

Personnel authorized to access these systems are required to comply with all restrictions governing access, use, sharing, retention, and disclosure of information.

10. Summary

Intelligence Sharing and Information Exchange Systems provide authorized personnel with the ability to receive, review, analyze, and share information that supports criminal investigations, public safety operations, officer safety, and coordination among law enforcement partners. Access to these systems is restricted, audited, and governed by legal, operational, and policy safeguards intended to protect privacy, civil rights, and civil liberties while supporting legitimate law enforcement and public safety objectives.

Investigative Research & Open-Source Intelligence (OSINT) Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Investigative Research and Open-Source Intelligence (OSINT) Systems.

The purpose of this policy is to:

- Define authorized and prohibited uses.
- Protect privacy, civil liberties, and constitutional rights.
- Ensure accountability and oversight.
- Establish standards for the collection, use, retention, and dissemination of information obtained through OSINT and investigative research tools.
- Promote lawful and responsible investigative practices.

2. Authorized Uses

Investigative Research and OSINT Systems may be used only for legitimate law enforcement, investigative, and public safety purposes consistent with applicable law and Department policy.

Authorized uses include:

- Conducting criminal investigations.
- Identifying individuals, businesses, addresses, vehicles, and associated records.
- Locating victims, witnesses, suspects, and missing persons.
- Verifying information obtained during investigations.
- Reviewing publicly available information relevant to authorized investigations.
- Accessing information through authorized investigative research and social media analysis tools.
- Developing investigative leads.
- Corroborating information obtained through other lawful investigative methods.
- Supporting threat assessments related to specific criminal investigations or documented public safety concerns.
- Assisting other law enforcement agencies in legitimate investigations.

All use must be connected to a legitimate law enforcement, investigative, or public safety objective.

3. Prohibited Uses

Investigative Research and OSINT Systems shall not be used for:

- Accessing information without a legitimate law enforcement purpose.
- Conducting inquiries based on personal curiosity.
- Researching individuals for personal, political, commercial, or non-governmental purposes.
- Monitoring individuals or groups solely based on race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.
- Monitoring, collecting, or retaining information regarding lawful First Amendment activity absent a legitimate law enforcement purpose.
- Collecting or retaining information unrelated to an authorized investigation or public safety function.
- Accessing information in violation of vendor agreements, platform terms of service, applicable law, or Department policy.
- Disseminating information to unauthorized persons or organizations.
- Using deceptive or fictitious online identities except as specifically authorized by law, Department policy, and supervisory approval.

4. Approval and Oversight

Access to Investigative Research and OSINT Systems is restricted to authorized personnel whose official duties require such access.

Supervisors are responsible for ensuring that:

- Personnel use these systems only for authorized purposes.
- Investigative activity is tied to a legitimate law enforcement objective.
- Access permissions remain appropriate to assigned duties.
- Potential misuse is investigated and addressed.
- Personnel comply with Department policy, legal requirements, and vendor restrictions.

System use may be monitored, reviewed, and audited to ensure compliance with Department requirements.

5. Exigent Circumstances

Exigent circumstances involving Investigative Research and OSINT Systems may arise when immediate access to publicly available information is necessary to protect life, prevent serious bodily injury, locate endangered persons, identify dangerous suspects, or respond to rapidly evolving public safety incidents.

Examples may include:

- Locating a missing, abducted, suicidal, or endangered person.
- Identifying a suspect involved in a violent crime who presents an immediate threat to public safety.
- Obtaining time-sensitive information during an active shooter, hostage situation, barricaded subject incident, or similar critical event.
- Reviewing publicly available information regarding credible threats of violence directed at specific individuals, schools, public events, or critical infrastructure.
- Identifying information necessary to support emergency response operations.
- Confirming identities, locations, associations, or other information needed to address an immediate public safety threat.

In exigent circumstances, authorized personnel may access available Investigative Research and OSINT Systems consistent with Department policy, applicable law, and the requirements governing each platform or system.

Exigent circumstances do not eliminate constitutional protections, documentation requirements, vendor restrictions, privacy safeguards, or Department policies. Information obtained during exigent circumstances remains subject to the same restrictions governing retention, dissemination, and use that apply during routine operations.

6. Data Retention, Access, and Dissemination

Information obtained through Investigative Research and OSINT Systems may be retained when incorporated into official police reports, investigative files, evidentiary records, intelligence products, or other authorized Department records.

Access is restricted to authorized personnel.

Information obtained through these systems may be disseminated only as permitted by applicable law, Department policy, court order, or legitimate law enforcement purpose.

Information retained by external platforms or vendors remains subject to the retention schedules, privacy policies, and operating requirements established by those entities.

7. Third-Party Data Handling

Many Investigative Research and OSINT Systems are operated and maintained by commercial vendors, data providers, investigative research platforms, social media analysis providers, or other third parties.

The Department will comply with applicable vendor agreements, platform terms of service, legal requirements, and operational restrictions governing the use of such systems.

The Department does not control the internal storage, retention schedules, auditing mechanisms, or system architecture of third-party platforms or vendors.

8. Training and Authorized Users

Only authorized personnel may access Investigative Research and OSINT Systems.

Personnel granted access shall complete any required training before receiving access and shall maintain any required credentials.

Training may include:

- Authorized and prohibited uses.
- Constitutional and civil liberties considerations.
- Privacy protections.
- Vendor and platform restrictions.
- Documentation requirements.
- Information security requirements.
- Audit and accountability standards.

9. Auditing, Accountability, and Discipline

Use of Investigative Research and OSINT Systems is subject to:

- Supervisory review.
- Audit logging where available.
- Internal compliance reviews.
- Investigation of suspected misuse.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Investigative Research and OSINT Systems.

Information regarding system usage, compliance efforts, and operational impacts may be included in annual surveillance technology reporting, subject to legal, security, and investigative limitations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, evolving technology, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Investigative Research & Open-Source Intelligence (OSINT) Systems Use Report

1. Description of the Surveillance Technology and How It Works

The Urbana Police Department utilizes Investigative Research and Open-Source Intelligence (OSINT) Systems that assist authorized personnel in locating, reviewing, analyzing, and verifying publicly available information and commercially available records relevant to criminal investigations and public safety operations.

Systems within this category include:

- Carfax for Police
- Geofeedia
- IDIcore - $260/mo - $3,120/yr
- LexisNexis Accurint – $600/mo $7,200/yr
- Social Media Analysis Tools (e.g., X1 Social Discovery)

These systems provide access to information from public records, commercially available data sources, publicly accessible online content, and social media platforms. Information may be searched, reviewed, and analyzed by authorized personnel to support investigations, verify information, identify individuals, locate involved parties, and develop investigative leads.

The Department may utilize these systems to collect information that is publicly available or otherwise lawfully accessible. Information obtained through these systems may be used independently or in conjunction with other investigative resources.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to assist officers and investigators in conducting lawful investigations, gathering information from publicly available or commercially available sources, and developing investigative leads.

Authorized uses include:

• Identifying individuals, businesses, addresses, vehicles, and associated records

• Locating witnesses, victims, missing persons, and suspects

• Verifying information obtained during investigations

• Reviewing publicly available records and commercially available information

• Supporting analysis conducted through authorized investigative research platforms

• Supporting criminal investigations

• Corroborating information obtained through other lawful investigative methods

• Identifying potential relationships between people, businesses, vehicles, addresses, and events

• Collecting information relevant to public safety concerns and criminal activity

These systems may only be used for legitimate law enforcement purposes consistent with applicable law and Department policy.

3. Deployment Authorization and Operational Oversight

Access to Investigative Research and OSINT Systems is restricted to authorized personnel whose duties require their use.

User permissions are assigned based on job responsibilities and operational necessity. Personnel utilizing these systems may be required to complete training provided by the Department or system vendor.

Use of these systems is governed by Department policy, applicable law, vendor terms of service, and supervisory oversight. User activity may be audited or reviewed to ensure compliance with established requirements and authorized uses.

Unauthorized access, misuse, or dissemination of information may result in disciplinary action, revocation of access privileges, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

• Annual subscription costs: $10,320

• Licensing fees: NA

• Vendor support costs: NA

• Training costs: NA

• Administrative support costs: NA

• Funding source(s): PD Budget

5. Assessment of Potential Disparate Impact

The Department has assessed whether Investigative Research and OSINT Systems could result in a disparate impact on protected classes.

Safeguards include:

• Purpose-based use restrictions

• Supervisory oversight

• Required training

• Audit and accountability measures

• Documentation of investigative activity

• Compliance with applicable laws and policies

The Department does not utilize these systems to target individuals or groups based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Investigative activity must be based on legitimate law enforcement objectives, articulable facts, or authorized investigative purposes.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that publicly available information, commercial data sources, investigative research platforms, and public records may contain personal information regarding individuals who are not involved in criminal activity.

Safeguards include:

Restricted Access

Access is limited to authorized personnel conducting official law enforcement duties.

Purpose-Based Use Requirements

Users must have a legitimate investigative, public safety, or law enforcement purpose before accessing available information.

Verification of Information

Information obtained from online sources may not always be accurate, complete, or current. Investigators are expected to independently assess and verify information before relying upon it for investigative or enforcement decisions.

Audit and Accountability Measures

System use may be logged and reviewed to detect unauthorized access or misuse.

Information Sharing Restrictions

Information obtained through these systems may be shared only as permitted by law, Department policy, court order, or legitimate law enforcement purpose.

Protection of Constitutional Rights

The Department does not collect, maintain, or monitor information about individuals solely because they engage in lawful activities protected by the United States Constitution or the Illinois Constitution.

The Department recognizes that online activity may include lawful political, religious, social, labor, educational, or advocacy-related expression. Such activity alone does not provide a basis for investigative monitoring or collection.

7. Data Storage, Retention, and Third-Party Access

Many systems within this category are operated by commercial vendors, data providers, or other third parties. Information accessed through these systems remains subject to the terms, conditions, retention schedules, and privacy practices of the originating source.

Information obtained through these systems may be retained when incorporated into official police reports, investigative case files, evidentiary records, intelligence products, or other Department records as authorized by law and policy.

Retention of Department records is governed by applicable records retention schedules and Department policy.

Third-party access is governed by the policies of the originating platform or vendor and applicable law.

8. Exigent Circumstances Use

Exigent circumstances involving Investigative Research and OSINT Systems may arise when immediate access to publicly available information is necessary to protect life, prevent serious bodily injury, locate endangered persons, identify suspects involved in ongoing violent crimes, or respond to rapidly evolving public safety incidents.

Examples may include:

• Locating a missing, abducted, suicidal, or endangered person.

• Identifying a suspect involved in a violent crime who presents an immediate threat to the public.

• Obtaining time-sensitive information during an active shooter, hostage situation, barricaded subject, or similar critical incident.

• Identifying individuals making credible threats of violence against specific persons, locations, schools, or public events.

• Reviewing publicly available information needed to support emergency response operations.

• Confirming identities, associations, locations, or other information necessary to address an immediate public safety threat.

In exigent circumstances, authorized personnel may access available investigative research and OSINT resources consistent with Department policy, applicable law, and the terms governing the use of each system.

Exigent circumstances do not eliminate the requirement to comply with constitutional protections, privacy safeguards, vendor restrictions, documentation requirements, or Department policies. Information obtained during exigent circumstances remains subject to the same restrictions governing retention, dissemination, and use that apply during routine operations.

9. Compliance With State and Federal Law

The use of Investigative Research and OSINT Systems will comply with all applicable federal, state, and local laws governing privacy, records management, information security, public records, and law enforcement activities.

Personnel utilizing these systems are required to comply with Department policy, vendor agreements, applicable laws, and constitutional protections governing the collection, use, retention, dissemination, and disclosure of information.

10. Summary

Investigative Research and OSINT Systems provide authorized personnel with access to publicly available and commercially available information that may assist with criminal investigations, public safety operations, threat assessments, and locating individuals. The Department's use of these systems is governed by supervisory oversight, policy requirements, legal standards, and privacy safeguards designed to protect civil rights and civil liberties while supporting legitimate law enforcement objectives.

Biometric Identification Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Biometric Identification Systems.

The purpose of this policy is to:

• Define authorized and prohibited uses.
• Protect privacy, civil liberties, and constitutional rights.
• Ensure accountability and oversight.
• Establish standards for the use of biometric identification systems and information.
• Promote lawful and responsible use of biometric resources supporting criminal investigations and public safety operations.

2. Authorized Uses

Biometric Identification Systems may be used only for legitimate law enforcement, criminal justice, and public safety purposes consistent with applicable law and Department policy.

Authorized uses include:

• Identifying unknown individuals.
• Verifying the identity of arrested persons.
• Supporting criminal investigations.
• Identifying missing, deceased, injured, or incapacitated persons.
• Comparing fingerprint or other biometric information obtained through lawful law enforcement activities.
• Linking individuals to criminal justice records where authorized by law.
• Supporting identification and investigative functions.
• Assisting fugitive investigations.
• Protecting officer and public safety.

All use must be connected to a legitimate law enforcement, investigative, forensic, or public safety objective.

3. Prohibited Uses

Biometric Identification Systems shall not be used for:

• Accessing information without a legitimate law enforcement or criminal justice purpose.
• Conducting searches based on personal curiosity.
• Researching individuals for personal, political, commercial, or non-governmental purposes.
• Using biometric information in violation of applicable law, court order, user agreement, or Department policy.

• Disseminating biometric information to unauthorized persons or organizations.
• Identifying, monitoring, or tracking individuals solely because of race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.
• Monitoring lawful First Amendment activity absent a legitimate law enforcement purpose.
• Retaining or disseminating information beyond what is authorized by law or policy.

4. Approval and Operational Oversight

Access to Biometric Identification Systems is restricted to authorized personnel whose official duties require such access.

User permissions are assigned based upon job responsibilities, operational necessity, and any requirements established by the agency operating the system. Personnel granted access must comply with all applicable Department policies, user agreements, security requirements, and governing agency rules.

Supervisors are responsible for ensuring that:

• Personnel use these systems only for authorized purposes.
• Access privileges remain appropriate to assigned duties.
• Investigative activity is tied to a legitimate law enforcement objective.
• Potential misuse is investigated and addressed.
• Personnel comply with applicable laws, user agreements, and Department policies.

System activity may be monitored or audited by the Department, the system owner, or other authorized oversight entities.

Unauthorized access, misuse, dissemination, or disclosure of information may result in disciplinary action, loss of access privileges, criminal penalties, or civil liability.

5. Exigent Circumstances

Exigent circumstances involving Biometric Identification Systems may arise when immediate identification is necessary to protect life, prevent serious bodily injury, locate endangered persons, identify victims, apprehend dangerous offenders, or support emergency response operations.

Examples may include:

• Identifying an unconscious, injured, deceased, or otherwise incapacitated individual when immediate identification is necessary.
• Identifying a suspect involved in a violent crime who presents an imminent threat to public safety.
• Assisting in the identification of a missing, abducted, or endangered person.
• Supporting emergency response efforts during mass casualty incidents, natural disasters, or other large-scale emergencies.

• Confirming the identity of an individual when delays could materially impact officer safety or public safety.
• Comparing available biometric information during a rapidly evolving criminal investigation involving an imminent threat of harm.

In exigent circumstances, authorized personnel may access available biometric identification resources consistent with applicable law, Department policy, and system-specific requirements.

Exigent circumstances do not eliminate legal restrictions, documentation requirements, court orders, user agreement obligations, audit requirements, or Department policies. Information obtained during exigent circumstances remains subject to the same protections governing access, retention, dissemination, and disclosure that apply during routine operations.

6. Data Retention, Access, and Dissemination

Most Biometric Identification Systems utilized by the Department are owned and maintained by state or federal governmental agencies.

Biometric information obtained through authorized queries may be incorporated into official police reports, investigative files, evidentiary records, or other Department records when authorized and necessary for law enforcement purposes.

Access is restricted to authorized personnel.

Information obtained through these systems may be disseminated only as permitted by applicable law, governing agency requirements, user agreements, court order, or legitimate law enforcement purpose.

Retention schedules, security requirements, access controls, and disclosure restrictions are governed by the policies and legal authorities applicable to each system.

7. Third-Party Data Handling

Most Biometric Identification Systems are owned and maintained by governmental entities outside the control of the City of Urbana.

The Department will comply with all applicable user agreements, operational requirements, and security standards established by the agencies responsible for administering those systems.

The Department does not control the internal storage, retention schedules, auditing mechanisms, or system architecture maintained by external entities.

Where vendors or contractors provide technical support or administrative services, access shall be limited to authorized functions and governed by applicable contracts, agreements, and legal requirements.

8. Training and Authorized Users

Only authorized personnel may access Biometric Identification Systems.

Personnel granted access shall complete any required training and maintain any required certifications or credentials.

Training may include:

• Authorized and prohibited uses.
• Applicable legal requirements.
• Information security obligations.
• Privacy and civil liberties protections.
• Information dissemination restrictions.
• Audit and accountability standards.
• System-specific operating requirements.

9. Auditing, Accountability, and Discipline

Use of Biometric Identification Systems is subject to:

• Supervisory review.
• Audit logging.
• Internal compliance reviews.
• Audits conducted by governing agencies.
• Investigation of suspected misuse.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Biometric Identification Systems.

Information regarding system usage, compliance efforts, and operational impacts may be included in annual surveillance technology reporting, subject to legal, security, and investigative limitations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, evolving technology, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Biometric Identification Systems Use Report

1. Description of the Surveillance Technology and How It Works

Biometric Identification Systems

The Urbana Police Department utilizes Biometric Identification Systems that assist authorized personnel in identifying or verifying individuals through unique biological or physical characteristics. These systems compare fingerprint, DNA, or other biometric information against records maintained in authorized governmental databases.

Systems within this category include:

- Integrated Automated Fingerprint Identification System (IAFIS)
- ITouch Biometrics - $1,980

These systems allow authorized personnel to compare biometric information collected during lawful law enforcement activities against records maintained by local, state, or federal agencies. The Department generally accesses information maintained by other governmental entities and does not independently operate or maintain the underlying biometric databases.

Biometric identification systems are used to support criminal investigations, confirm identities, identify unknown individuals, and assist with public safety functions.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to assist in identifying individuals, supporting criminal investigations, and enhancing public safety.

Authorized uses include:

• Identifying unknown individuals

• Verifying the identity of arrested persons

• Supporting criminal investigations

• Identifying missing, deceased, or incapacitated persons

• Linking individuals to criminal justice records where authorized by law

• Assisting with fugitive investigations

• Supporting forensic examinations and evidence analysis

• Confirming identities when necessary for public safety purposes

These systems may only be used for authorized law enforcement and criminal justice purposes consistent with applicable law and Department policy.

3. Deployment Authorization and Operational Oversight

Access to Biometric Identification Systems is restricted to authorized personnel with a legitimate law enforcement or criminal justice purpose.

User permissions are assigned based upon job responsibilities and operational necessity. Personnel must complete any required training before receiving access to applicable systems.

Use of Biometric Identification Systems is governed by Department policy, applicable law, system-specific user agreements, and agency requirements established by the system owner.

System use may be subject to audits, reviews, and oversight by the Department and governing agencies.

Unauthorized access, use, dissemination, or misuse of biometric information may result in disciplinary action, loss of system access, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

• Annual access costs: $1,980

• Equipment costs: NA

• Maintenance costs: NA

• Training costs: NA

• Administrative support costs: NA

• Funding source(s): PD Budget

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Biometric Identification Systems could result in a disparate impact on protected classes.

Safeguards include:

• Authorized-use restrictions

• Supervisor oversight

• User training requirements

• Audit and accountability measures

• Compliance with applicable laws and policies

• Established forensic and identification standards

The Department does not utilize Biometric Identification Systems to target individuals based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Biometric information is used for identification and investigative purposes consistent with authorized law enforcement objectives and applicable legal requirements.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that biometric information is sensitive personal information that may present privacy concerns if improperly collected, used, retained, or disclosed.

Safeguards include:

Restricted Access

Access is limited to authorized personnel with a legitimate criminal justice, investigative, identification, or forensic purpose.

Verification and Quality Controls

Biometric identifications are evaluated using established forensic, investigative, and evidentiary standards. Biometric information is considered one component of an investigation and may be supplemented by additional evidence when appropriate.

Audit and Accountability Measures

System use may be logged and subject to review or audit by the Department and governing agencies.

Information Sharing Limitations

Biometric information may only be shared as authorized by law, court order, criminal justice information-sharing agreements, or official law enforcement purposes.

Protection of Constitutional Rights

The Department does not use Biometric Identification Systems to monitor, identify, or track individuals solely because they engage in lawful activity protected by the United States Constitution or the Illinois Constitution.

The Department does not use Biometric Identification Systems to identify individuals based solely upon protected characteristics.

7. Data Storage, Retention, and Third-Party Access

Most Biometric Identification Systems utilized by the Department are owned, maintained, and administered by state or federal governmental agencies.

Retention schedules, security requirements, access controls, and disclosure restrictions are governed by the policies and legal authorities applicable to each system.

Biometric information obtained through authorized queries may be incorporated into official reports, investigative files, evidentiary records, or other Department records when authorized and necessary for law enforcement purposes.

Third-party access is governed by applicable laws, system requirements, and agreements established by the agency operating the system.

8. Exigent Circumstances Use

Exigent circumstances involving Biometric Identification Systems may arise when rapid identification is necessary to protect life, respond to an active threat, identify victims, locate endangered persons, or support an ongoing emergency response.

Examples may include:

• Identifying an unconscious, injured, deceased, or otherwise incapacitated individual when immediate identification is necessary.

• Identifying a suspect involved in a violent crime who poses an imminent threat to public safety.

• Assisting in the identification of a missing, abducted, or endangered person.

• Supporting emergency response efforts during mass casualty incidents, natural disasters, or other large-scale emergencies.

• Confirming the identity of an individual when delays could materially impact officer safety or public safety.

• Comparing available biometric information during a rapidly evolving criminal investigation involving an imminent threat of harm.

In exigent circumstances, authorized personnel may access available biometric identification resources consistent with applicable law, Department policy, and system-specific requirements.

Exigent circumstances do not eliminate the requirement to comply with legal restrictions, documentation requirements, court orders, user agreements, or Department policies. Information obtained through biometric identification systems remains subject to the same protections governing access, retention, dissemination, and disclosure that apply during routine operations.

9. Compliance With State and Federal Law

The use of Biometric Identification Systems will comply with all applicable federal, state, and local laws governing biometric information, criminal justice records, forensic evidence, privacy protections, and information security.

Personnel authorized to access these systems are required to comply with all restrictions governing access, use, retention, dissemination, and disclosure of biometric information.

10. Summary

Biometric Identification Systems provide authorized personnel with tools to identify individuals, support criminal investigations, assist forensic examinations, and enhance public safety. Access to these systems is restricted and governed by legal requirements, Department policies, training standards, and oversight measures intended to protect privacy, civil rights, and civil liberties while supporting legitimate law enforcement objectives.

Covert Video & Thermal Surveillance Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Covert Video and Thermal Surveillance Systems.

The purpose of this policy is to:

Define authorized and prohibited uses.

- Protect privacy, civil liberties, and constitutional rights.
- Ensure accountability and oversight.
- Establish standards governing the deployment, use, retention, and dissemination of covert video and thermal surveillance recordings and data.
- Promote lawful and responsible use of covert video and thermal surveillance technologies in support of criminal investigations and public safety operations.

2. Authorized Uses

Covert Video and Thermal Surveillance Systems may be used only for legitimate law enforcement, investigative, and public safety purposes consistent with applicable law and Department policy.

Authorized uses include:

- Supporting criminal investigations.
- Documenting criminal activity.
- Gathering evidence relevant to criminal prosecutions.
- Identifying suspects involved in criminal activity.
- Identifying vehicles associated with criminal activity.
- Monitoring locations associated with authorized criminal investigations.
- Supporting undercover investigations.
- Verifying investigative information.
- Supporting officer safety.
- Supporting public safety operations.
- Assisting other law enforcement agencies in legitimate investigations.
- Locating missing, endangered, injured, or vulnerable persons.
- Supporting search-and-rescue operations.
- Locating suspects in low-light or nighttime conditions.
- Supporting officer safety through the lawful use of thermal imaging technology.

- Identifying heat signatures associated with persons or vehicles during authorized investigations.

Thermal imaging may be used to detect heat signatures associated with persons, vehicles, or other objects relevant to authorized criminal investigations, public safety incidents, search-and-rescue operations, and officer safety functions.

All use must be connected to a legitimate law enforcement, investigative, or public safety objective.

3. Prohibited Uses

Covert Video and Thermal Surveillance Systems shall not be used for:

- Monitoring individuals without a legitimate law enforcement purpose.
- Conducting surveillance based upon personal curiosity.
- Monitoring individuals solely because of race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.
- Monitoring lawful First Amendment activity absent a legitimate law enforcement purpose.
- Deploying systems in violation of applicable law, court order, Department policy, or constitutional requirements.
- Disseminating recordings or thermal imaging data to unauthorized persons or organizations.
- Using recordings for personal, political, commercial, or non-governmental purposes.
- Retaining or disseminating recordings beyond what is authorized by law or policy.
- Recording audio unless separately authorized by law, court order, judicial authorization, or other lawful legal process.
- Using thermal imaging technology to conduct warrantless searches of private residences or other constitutionally protected areas except as authorized by law.
- Using thermal imaging technology for non-law-enforcement or non-public-safety purposes.

4. Approval and Oversight

Access to Covert Video and Thermal Surveillance Systems is restricted to authorized personnel whose official duties require such access.

Supervisors are responsible for ensuring that:

- Deployments are supported by legitimate investigative objectives.
- Personnel use the systems only for authorized purposes.
- Access permissions remain appropriate to assigned duties.
- Potential misuse is investigated and addressed.
- Personnel comply with applicable laws, court orders, and Department policies.

Any deployment of thermal imaging technology complies with applicable constitutional requirements, Department policy, and legal standards.

System deployments and recordings may be monitored, reviewed, and audited to ensure compliance.

5. Exigent Circumstances

Exigent circumstances involving Covert Video and Thermal Surveillance Systems may arise when immediate deployment is necessary to protect life, prevent serious bodily injury, locate endangered persons, identify dangerous offenders, or respond to active public safety threats.

Examples may include:

- Locating a violent offender.
- Identifying individuals involved in a violent crime.
- Supporting emergency investigative operations.
- Protecting potential victims.
- Investigating imminent threats to public safety.
- Supporting active criminal investigations involving immediate risk of serious harm.
- Locating a missing, lost, abducted, suicidal, or endangered person during nighttime or low-visibility conditions.
- Locating a violent offender believed to present an immediate threat to the public.
- Supporting rescue operations in large outdoor areas where visibility is limited.

In exigent circumstances, authorized personnel may deploy or access available Covert Video and Thermal Surveillance Systems consistent with applicable law and Department policy.

Exigent circumstances do not eliminate constitutional protections, documentation requirements, legal standards, or Department policies.

6. Data Retention, Access, and Dissemination

Video recordings and thermal imaging data obtained through Covert Video and Thermal Surveillance Systems may be retained when incorporated into official police reports, investigative files, evidentiary records, intelligence products, or other authorized Department records.

Access is restricted to authorized personnel.

Video recordings and thermal imaging data may be disseminated only as permitted by applicable law, court order, Department policy, evidentiary requirements, or legitimate law enforcement purpose.

Retention schedules shall be governed by records retention requirements, evidentiary obligations, court orders, and Department policy.

7. Third-Party Data Handling

Some Covert Video and Thermal Surveillance Systems may utilize third-party hardware, software, storage platforms, or technical support services.

The Department will comply with applicable contracts, legal requirements, operational restrictions, and security standards governing such services.

The Department does not permit unauthorized third-party access to investigative recordings or thermal imaging data.

Where third-party support is necessary, access shall be limited to authorized functions and governed by applicable agreements and legal requirements.

8. Training and Authorized Users

Only authorized personnel may access or deploy Covert Video and Thermal Surveillance Systems.

Personnel granted access shall complete any required training and maintain any required certifications or credentials.

Training may include:

- Authorized and prohibited uses.
- Constitutional and legal requirements.
- Privacy and civil liberties protections.
- Department deployment procedures.
- Information security requirements.
- Documentation requirements.
- Audit and accountability standards.
- System-specific operating requirements.
- Constitutional limitations applicable to thermal imaging technology.
- Legal restrictions governing surveillance technologies.
- Proper deployment of thermal imaging systems.
- Search-and-rescue applications of thermal imaging systems.

9. Auditing, Accountability, and Discipline

Use of Covert Video and Thermal Surveillance Systems is subject to:

- Supervisory review.
- Audit logging where available.
- Internal compliance reviews.
- Investigation of suspected misuse.
- Audits conducted by authorized oversight entities.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Covert Video and Thermal Surveillance Systems.

Information regarding system usage, compliance efforts, and operational impacts may be included in annual surveillance technology reporting, subject to legal, evidentiary, security, and investigative limitations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, evolving technology, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Covert Video & Thermal Surveillance Systems Use Report

1. Description of the Surveillance Technology and How It Works

The Urbana Police Department utilizes Covert Video and Thermal Surveillance Systems to support lawful criminal investigations and public safety operations.

Systems within this category include:

- Temporarily Deployed Covert Surveillance Cameras
- Thermal Imaging Device

These systems capture video images or thermal signatures of locations, activities, vehicles, property, and individuals relevant to authorized criminal investigations, public safety operations, and search-and-rescue activities.

Video surveillance systems record visible imagery, while thermal imaging systems detect heat signatures emitted by persons, vehicles, animals, and other objects. Thermal imaging systems may be used to assist officers in locating individuals in low-light or nighttime conditions, identifying suspects during criminal investigations, locating missing or endangered persons, enhancing officer safety, and supporting emergency response operations.

The systems may be deployed temporarily or for extended periods depending upon investigative need, legal requirements, and operational objectives.

These systems record video only and do not record audio unless separately authorized by law, court order, judicial authorization, or other applicable legal process.

Thermal imaging technology shall not be used to conduct searches of private residences or other constitutionally protected areas except as authorized by law.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to support criminal investigations and public safety operations.

Authorized uses include:

- Documenting criminal activity.
- Gathering evidence relevant to criminal investigations.
- Identifying suspects involved in criminal offenses.
- Identifying vehicles associated with criminal activity.
- Supporting undercover investigations.
- Supporting surveillance operations authorized by law.
- Verifying investigative information.
- Locating wanted offenders.
- Locating missing, endangered, or vulnerable persons.
- Conducting search-and-rescue operations.
- Supporting nighttime public safety operations.
- Enhancing officer safety.
- Supporting criminal prosecutions.

These systems may only be deployed for legitimate law enforcement and investigative purposes consistent with applicable law and Department policy.

3. Deployment Authorization and Operational Oversight

Access to Covert Video and Thermal Surveillance Systems is restricted to authorized personnel.

Deployment shall be based upon documented investigative need and supervisory approval.

Personnel utilizing these systems shall comply with applicable constitutional requirements, Department policy, court orders, judicial authorizations, and legal restrictions.

System activity may be monitored, audited, and reviewed to ensure compliance.

Unauthorized deployment, access, use, disclosure, or dissemination of information may result in disciplinary action, criminal penalties, civil liability, or revocation of access privileges.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

- Equipment costs: Unknown exact – These are existing systems that were purchased years ago. Estimated cost is $1,000
- Replacement costs: TBD
- Storage costs: TBD
- Maintenance costs: TBD
- Training costs: TBD
- Funding source(s): Special Funds - Forfeiture

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Covert Video and Thermal Surveillance Systems could result in a disparate impact on protected classes.

Safeguards include:

- Supervisor approval requirements
- Purpose-based deployment restrictions
- Documentation requirements
- Audit and accountability measures
- User training
- Compliance with applicable law and policy
- Deployment based on documented investigative or public safety needs and not on protected characteristics
- Thermal imaging used to detect heat signatures and locate persons or objects, not to profile individuals or groups

The Department does not deploy these systems based solely upon race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that covert video and thermal surveillance may raise privacy concerns.

Safeguards Include:

Restricted Access

Access is limited to authorized personnel with a legitimate investigative purpose.

Investigative Justification Requirements

Deployments must be supported by a legitimate law enforcement objective.

Audit and Accountability Measures

System use may be documented, reviewed, and audited.

Information Sharing Restrictions

Recorded information may only be shared consistent with applicable law, court order, Department policy, or legitimate investigative purpose.

Protection of Constitutional Rights

Covert Video and Thermal Surveillance Systems shall not be used to monitor, record, or investigate individuals solely because they engage in activities protected by the United States Constitution or Illinois Constitution.

Thermal imaging systems shall not be used to conduct warrantless searches of private residences or to detect suspected criminal activity occurring within a home, except as authorized by law.

7. Data Storage, Retention, and Third-Party Access

Video recordings and thermal imaging data obtained through these systems may be retained when incorporated into official reports, investigative files, evidentiary records, intelligence products, or other authorized Department records.

Retention schedules shall be governed by applicable law, court orders, evidentiary requirements, records retention schedules, and Department policy.

Third-party support services shall comply with applicable contracts, legal requirements, and information security standards.

8. Exigent Circumstances Use

Exigent circumstances involving Covert Video and Thermal Surveillance Systems may arise when immediate deployment is necessary to protect life, prevent serious bodily injury, identify dangerous offenders, locate endangered persons, or respond to rapidly evolving public safety threats.

Examples may include:

- Locating a violent offender.
- Identifying individuals involved in a violent crime.
- Supporting emergency investigative operations.
- Protecting potential victims.
- Investigating imminent threats to public safety.
- Supporting active criminal investigations involving immediate risk of harm.
- Locating a missing, lost, injured, abducted, or endangered person during nighttime or low-visibility conditions.
- Locating a suspect believed to pose an immediate threat to public safety.
- Assisting officers searching large outdoor areas where visibility is limited.
- Supporting emergency response operations following natural disasters, severe weather events, or other public safety emergencies.

Exigent circumstances do not eliminate compliance with applicable laws, documentation requirements, constitutional protections, or Department policy.

9. Compliance With State and Federal Law

The use of Covert Video and Thermal Surveillance Systems shall comply with all applicable federal, state, and local laws governing surveillance, criminal investigations, privacy protections, evidence collection, and constitutional rights.

Audio recording shall not occur unless separately authorized by law, court order, judicial authorization, or other applicable legal process.

10. Summary

Covert Video and Thermal Surveillance Systems provide authorized personnel with the ability to document criminal activity, gather evidence, identify suspects, locate missing persons, support

search-and-rescue operations, and assist criminal investigations. Access to these systems is restricted and governed by legal requirements, supervisory oversight, audit measures, training standards, and privacy safeguards designed to protect civil rights and civil liberties while supporting legitimate public safety objectives.

Digital Forensics & Mobile Device Investigation Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Digital Forensics and Mobile Device Investigation Systems.

The purpose of this policy is to:

Define authorized and prohibited uses.

- Protect privacy, civil liberties, and constitutional rights.
- Ensure accountability and oversight.
- Establish standards for the collection, analysis, retention, dissemination, and management of digital evidence.
- Promote lawful and responsible use of digital forensic tools supporting criminal investigations and public safety operations.

2. Authorized Uses

Digital Forensics and Mobile Device Investigation Systems may be used only for legitimate law enforcement, investigative, and public safety purposes consistent with applicable law and Department policy.

Authorized uses include:

- Extracting digital evidence from mobile devices, computers, digital storage media, and associated accounts when authorized by law.
- Preserving electronic evidence for criminal investigations and prosecutions.
- Identifying suspects, victims, witnesses, and associates.
- Verifying information obtained during investigations.
- Recovering deleted, hidden, encrypted, or otherwise inaccessible information when authorized by law.
- Analyzing communications, application data, photographs, videos, internet activity, and other digital evidence relevant to criminal investigations.
- Identifying device ownership, user associations, or account relationships.
- Reviewing subscriber information, call detail records, and other telecommunications records obtained through lawful legal process.
- Analyzing location information obtained through search warrants, court orders, or other authorized legal process.
- Supporting criminal prosecutions.

- Assisting other law enforcement agencies in legitimate investigations.
- Supporting officer safety and public safety operations.

All use must be connected to a legitimate law enforcement, investigative, or public safety objective.

3. Prohibited Uses

Digital Forensics and Mobile Device Investigation Systems shall not be used for:

- Accessing digital information without lawful authority or a legitimate law enforcement purpose.
- Conducting examinations based upon personal curiosity.
- Researching individuals for personal, political, commercial, or non-governmental purposes.
- Accessing information in violation of applicable law, court orders, warrant limitations, user agreements, or Department policy.
- Exceeding the scope of authorized legal process.
- Disseminating digital evidence or investigative information to unauthorized persons or organizations.
- Conducting examinations unrelated to an authorized criminal investigation or public safety activity.
- Monitoring, collecting, or retaining information about individuals based solely upon race, ethnicity, religion, disability, sexual orientation, political beliefs, or other protected characteristics.
- Monitoring lawful First Amendment activity absent a legitimate law enforcement purpose.
- Retaining or disseminating information beyond what is authorized by law, court order, or Department policy.

4. Approval and Oversight

Access to Digital Forensics and Mobile Device Investigation Systems is restricted to authorized personnel whose official duties require such access.

Supervisors are responsible for ensuring that:

Personnel use these systems only for authorized purposes.

- Appropriate legal authority exists before examinations are conducted.
- Examinations remain within the scope authorized by law.
- Digital evidence is properly collected, documented, preserved, and secured.
- Chain-of-custody requirements are maintained.
- Potential misuse is investigated and addressed.
- Personnel comply with applicable laws, court orders, user agreements, and Department policies.

System use may be monitored, reviewed, and audited by the Department and authorized oversight entities.

Unauthorized access, misuse, dissemination, or disclosure of information may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

5. Exigent Circumstances

Exigent circumstances involving Digital Forensics and Mobile Device Investigation Systems may arise when immediate access to digital evidence is necessary to protect life, prevent serious bodily injury, locate endangered persons, apprehend dangerous offenders, or respond to active public safety threats.

Examples may include:

- Locating a missing, abducted, suicidal, or endangered person.
- Identifying a suspect involved in a violent crime who presents an imminent threat to public safety.
- Supporting emergency response operations during active threats.
- Identifying communications associated with an immediate threat of violence.
- Locating a dangerous offender who poses an imminent risk to the public.
- Obtaining time-sensitive information is necessary to prevent imminent harm.

In exigent circumstances, authorized personnel may utilize Digital Forensics and Mobile Device Investigation Systems consistent with applicable law and Department policy.

Exigent circumstances do not eliminate constitutional protections, documentation requirements, legal standards, warrant requirements when applicable, or Department policies.

Information obtained during exigent circumstances remains subject to the same protections governing retention, dissemination, disclosure, and use that apply during routine operations.

6. Data Retention, Access, and Dissemination

Information obtained through Digital Forensics and Mobile Device Investigation Systems may be retained when incorporated into official police reports, investigative files, evidentiary records, intelligence products, or other authorized Department records.

Access is restricted to authorized personnel.

Information obtained through these systems may be disseminated only as permitted by applicable law, court order, Department policy, evidentiary requirements, or legitimate law enforcement purpose.

Retention schedules shall be governed by applicable records retention requirements, evidentiary obligations, court orders, and Department policy.

Digital evidence shall be maintained in a manner designed to preserve evidentiary integrity, security, and chain of custody.

7. Third-Party Data Handling

Some Digital Forensics and Mobile Device Investigation Systems may be provided, maintained, or supported by third-party vendors.

The Department will comply with applicable licensing agreements, legal requirements, security requirements, and operational restrictions governing the use of such systems.

The Department does not permit unauthorized vendor access to investigative information or evidence.

Where vendor support is necessary, access shall be limited to authorized functions and governed by applicable contracts, agreements, legal requirements, and Department policy.

Any cloud-based storage or processing services utilized by vendors shall be subject to applicable security standards, contractual safeguards, and legal requirements.

8. Training and Authorized Users

Only authorized personnel may access Digital Forensics and Mobile Device Investigation Systems.

Personnel granted access shall complete any required training and maintain any required certifications or credentials.

Training may include:

- Authorized and prohibited uses.
- Applicable search and seizure laws.
- Digital evidence handling procedures.
- Privacy and civil liberties protections.
- Warrant and legal process requirements.
- Documentation requirements.
- Information security requirements.
- Chain-of-custody procedures.
- Audit and accountability standards.
- System-specific operating requirements.

9. Auditing, Accountability, and Discipline

Use of Digital Forensics and Mobile Device Investigation Systems is subject to:

Supervisory review.

- Audit logging.
- Internal compliance reviews.
- Investigation of suspected misuse.
- Audits conducted by authorized oversight entities.
- Documentation review and case audits where appropriate.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Digital Forensics and Mobile Device Investigation Systems.

Information regarding system usage, compliance efforts, and operational impacts may be included in annual surveillance technology reporting, subject to legal, evidentiary, security, and investigative limitations.

Sensitive investigative techniques, evidentiary information, and information that would compromise investigations, officer safety, or public safety, shall not be publicly disclosed except as required by law.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, evolving technology, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Digital Forensics & Mobile Device Investigation Systems Use Report

1. Description of the Surveillance Technology and How It Works

The Urbana Police Department utilizes Digital Forensics and Mobile Device Investigation Systems to lawfully extract, analyze, preserve, and manage digital evidence obtained from mobile devices, computers, digital storage media, and telecommunications providers.

Systems within this category include:

- Cellebrite – $9,990
- Magnet AXIOM – $10,704.53
- Cellular Provider Records (tower) - Varies depending on use. Last year $600 total for 2 uses.
- Cell Site Location Information (CSLI)

These systems allow authorized personnel to collect, preserve, and analyze digital evidence relevant to criminal investigations. Information may be obtained through search warrants, consent searches, court orders, subpoenas, exigent circumstances, or other lawful legal authority.

Information obtained through these systems may include call records, text messages, photographs, videos, application data, internet activity, subscriber information, device identifiers, and historical location information. Digital evidence may be analyzed independently or in conjunction with other investigative information.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to assist investigators in conducting lawful criminal investigations and preserving digital evidence.

Authorized uses include:

- Extracting and preserving digital evidence from mobile devices and electronic storage media.
- Recovering deleted or hidden information.
- Identifying suspects, victims, witnesses, and associates.
- Verifying investigative information.
- Analyzing communications relevant to criminal investigations.
- Identifying relationships between individuals involved in criminal activity.
- Determining device ownership or use.

- Analyzing location information obtained through lawful legal process.
- Supporting criminal prosecutions.
- Enhancing officer and public safety.

These systems may only be used for legitimate law enforcement, investigative, and public safety purposes consistent with applicable law and Department policy.

3. Deployment Authorization and Operational Oversight

Access to Digital Forensics and Mobile Device Investigation Systems is restricted to authorized personnel whose job responsibilities require such access.

Personnel utilizing these systems must receive appropriate training and comply with applicable legal requirements, Department policy, court orders, search warrants, consent agreements, and established evidence-handling procedures.

Supervisors are responsible for ensuring that:

- System use is connected to a legitimate criminal investigation.
- Appropriate legal authorization has been obtained when required.
- Digital evidence is properly handled and documented.
- Audit and accountability measures are maintained.
- Potential misuse is investigated and addressed.

System activity may be logged, monitored, audited, and reviewed to ensure compliance with legal requirements and Department policy.

Unauthorized access, improper use, dissemination, or disclosure of information may result in disciplinary action, revocation of access, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

- Annual costs: $21,294.53
- Software maintenance costs: TBD
- Hardware replacement costs: TBD
- Training costs: TBD
- Administrative support costs: TBD
- Funding source(s): PD Budget

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Digital Forensics and Mobile Device Investigation Systems could result in a disparate impact on protected classes.

Safeguards include:

- Legal process requirements
- Judicial oversight where required
- Supervisor approval
- User training
- Audit logging
- Documentation requirements
- Compliance with applicable laws and policies

The Department does not utilize these systems to target individuals based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Investigations must be based upon legitimate law enforcement objectives, articulable facts, probable cause, or other legally authorized investigative standards.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that digital devices may contain substantial amounts of personal information.

Safeguards include:

Restricted Access

Access is limited to authorized personnel with a legitimate investigative or public safety purpose.

Legal Process Requirements

Information shall be obtained only through lawful authority, including search warrants, consent, court orders, subpoenas, or other legally recognized methods.

Audit and Accountability Measures

System activity may be reviewed and audited to detect unauthorized access or misuse.

Information Sharing Restrictions

Information obtained through these systems may only be shared as permitted by law, court order, Department policy, or legitimate law enforcement purpose.

Protection of Constitutional Rights

The Department does not utilize Digital Forensics and Mobile Device Investigation Systems to investigate, monitor, or collect information regarding individuals solely because they engage in lawful activity protected by the United States Constitution or the Illinois Constitution.

7. Data Storage, Retention, and Third-Party Access

Information obtained through these systems may be retained when incorporated into official police reports, investigative files, evidentiary records, intelligence products, or other authorized Department records.

Digital evidence storage, retention, access, dissemination, and destruction shall be governed by applicable laws, court orders, records retention schedules, evidentiary requirements, and Department policy.

Third-party vendors may provide technical support, software maintenance, cloud storage, or evidence management services. Access to such information shall be governed by applicable contracts, legal requirements, security standards, and Department policy.

8. Exigent Circumstances Use

Exigent circumstances involving Digital Forensics and Mobile Device Investigation Systems may arise when immediate access to digital evidence is necessary to protect life, prevent serious bodily injury, locate endangered persons, apprehend dangerous offenders, or address rapidly evolving public safety emergencies.

Examples may include:

- Locating a missing, abducted, suicidal, or endangered person.
- Identifying a suspect involved in a violent crime who presents an imminent threat to public safety.
- Supporting emergency response operations during an active threat.
- Identifying communications associated with an ongoing threat of violence.
- Locating a wanted offender presenting an immediate danger.
- Obtaining time-sensitive information necessary to prevent imminent harm.

Exigent circumstances do not eliminate applicable constitutional protections, documentation requirements, legal standards, or Department policies.

9. Compliance With State and Federal Law

The use of Digital Forensics and Mobile Device Investigation Systems shall comply with all applicable federal, state, and local laws governing digital evidence, telecommunications records,

privacy protections, criminal investigations, search and seizure requirements, and evidentiary procedures.

Personnel shall comply with all applicable laws, court orders, user agreements, and Department policies governing access, retention, dissemination, disclosure, and use of digital evidence.

10. Summary

Digital Forensics and Mobile Device Investigation Systems provide authorized personnel with tools to lawfully collect, preserve, analyze, and manage digital evidence relevant to criminal investigations and public safety operations. Access to these systems is restricted and governed by legal requirements, Department policy, supervisory oversight, audit measures, and privacy safeguards designed to protect civil rights and civil liberties while supporting legitimate law enforcement objectives.

Specialized Investigative Systems Policy Report

1. Purpose of the Policy

This Policy Report establishes the governance framework, restrictions, and safeguards governing the Urbana Police Department's use of Specialized Investigative Systems.

The purpose of this policy is to:

- Define authorized and prohibited uses.
- Protect privacy, civil liberties, and constitutional rights.
- Ensure accountability and oversight.
- Establish standards for the use of specialized investigative databases and systems.
- Promote lawful and responsible use of investigative resources supporting firearms-related investigations and travel document verification.

2. Authorized Uses

Specialized Investigative Systems may be used only for legitimate law enforcement, investigative, and public safety purposes consistent with applicable law and Department policy.

Authorized uses include:

- Tracing firearms recovered during criminal investigations.
- Identifying potential firearm purchasers, dealers, manufacturers, or transfer histories where authorized by law.
- Verifying whether a passport has been reported lost or stolen.
- Supporting violent crime investigations.
- Supporting fugitive investigations.
- Assisting other law enforcement agencies in legitimate investigations.
- Supporting officer safety and public safety operations.

All use must be connected to a legitimate law enforcement, investigative, or public safety objective.

3. Prohibited Uses

Specialized Investigative Systems shall not be used for:

- Accessing information without a legitimate law enforcement or investigative purpose.

- Conducting inquiries based on personal curiosity.
- Researching individuals for personal, political, commercial, or non-governmental purposes.
- Accessing information in violation of applicable law, user agreements, or Department policy.
- Disseminating information to unauthorized persons or organizations.
- Conducting queries unrelated to an active investigation, intelligence function, or authorized public safety activity.
- Using information obtained through these systems to monitor individuals based solely upon protected characteristics or lawful First Amendment activity.
- Retaining or disseminating information beyond what is authorized by law or policy.

4. Approval and Oversight

Access to Specialized Investigative Systems is restricted to authorized personnel whose official duties require such access.

Supervisors are responsible for ensuring that:

- Personnel use these systems only for authorized purposes.
- Access privileges remain appropriate to assigned duties.
- Investigative activity is tied to a legitimate law enforcement objective.
- Potential misuse is investigated and addressed.
- Personnel comply with applicable laws, user agreements, and Department policies.

System use may be monitored, reviewed, and audited by the Department or the agencies responsible for administering the systems.

5. Exigent Circumstances

Exigent circumstances involving Specialized Investigative Systems may arise when immediate access to firearms-related information or travel document information is necessary to protect life, prevent serious bodily injury, apprehend dangerous offenders, or respond to active public safety threats.

Examples may include:

- Tracing a firearm recovered during an active violent crime investigation.

- Assisting in the identification or apprehension of a suspect involved in a recent violent offense.
- Verifying travel document information during an investigation involving a dangerous fugitive or other serious criminal activity.
- Obtaining time-sensitive information necessary to support emergency law enforcement operations.

In exigent circumstances, authorized personnel may access available Specialized Investigative Systems consistent with Department policy, applicable law, and system-specific requirements.

Exigent circumstances do not eliminate legal restrictions, documentation requirements, audit requirements, user agreement obligations, or Department policies. Information obtained during exigent circumstances remains subject to the same restrictions governing retention, dissemination, and use that apply during routine operations.

6. Data Retention, Access, and Dissemination

Information obtained through Specialized Investigative Systems may be retained when incorporated into official police reports, investigative files, evidentiary records, or other authorized Department records.

Access is restricted to authorized personnel.

Information obtained through these systems may be disseminated only as permitted by applicable law, governing agency requirements, user agreements, court order, or legitimate law enforcement purpose.

Information retained by external systems remains subject to the retention schedules, security requirements, and legal authorities established by the agencies responsible for maintaining those systems.

7. Third-Party Data Handling

Most Specialized Investigative Systems are owned and maintained by federal agencies or other governmental entities.

The Department will comply with applicable user agreements, operational requirements, and security standards established by the agencies responsible for administering those systems.

The Department does not control the internal storage, retention schedules, auditing mechanisms, or system architecture of systems maintained by external entities.

8. Training and Authorized Users

Only authorized personnel may access Specialized Investigative Systems.

Personnel granted access shall complete any required training and maintain any required certifications or credentials.

Training may include:

- Authorized and prohibited uses.
- Applicable legal requirements.
- Information security obligations.
- Privacy and civil liberties protections.
- Information dissemination restrictions.
- Audit and accountability standards.
- System-specific operating requirements.

9. Auditing, Accountability, and Discipline

Use of Specialized Investigative Systems is subject to:

- Supervisory review.
- Audit logging.
- Internal compliance reviews.
- Audits conducted by governing agencies.
- Investigation of suspected misuse.

Violations of this policy may result in disciplinary action, suspension or revocation of access privileges, criminal prosecution, civil liability, or other corrective action as appropriate.

10. Transparency and Reporting

The Department will comply with applicable ordinance reporting requirements concerning the use of Specialized Investigative Systems.

Information regarding system usage, compliance efforts, and operational impacts may be included in annual surveillance technology reporting, subject to legal, security, and investigative limitations.

11. Policy Review and Updates

This policy shall be reviewed periodically to ensure continued compliance with applicable law, evolving technology, operational needs, and community expectations.

Revisions shall be made as necessary and submitted for approval in accordance with applicable ordinance requirements and Department policy.

Specialized Investigative Systems Use Report

1. Description of the Surveillance Technology and How It Works

Specialized Investigative Systems

The Urbana Police Department utilizes Specialized Investigative Systems that support specific law enforcement functions involving firearms tracing and travel document verification.

Systems within this category include:

- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) E-Trace
- Lost and Stolen Passport Database

These systems provide authorized personnel with access to information that may assist with firearms-related investigations and the verification of travel documents reported as lost or stolen.

Information available through these systems is generally maintained by state, federal, or international governmental agencies. The Urbana Police Department accesses information maintained within these systems but generally does not own, manage, or control the underlying databases.

2. Proposed Purpose(s) of the Surveillance Technology

The purpose of these systems is to support specialized investigative functions and improve public safety.

Authorized uses include:

• Tracing firearms recovered during criminal investigations

• Identifying firearm purchase and transfer information when authorized by law

• Verifying whether travel documents have been reported lost or stolen

• Supporting fugitive investigations

• Assisting with interstate and multi-jurisdictional investigations

• Supporting firearms-related criminal investigations

• Enhancing officer and public safety

These systems may only be used for legitimate law enforcement purposes consistent with applicable law, Department policy, and system-specific requirements.

3. Deployment Authorization and Operational Oversight

Access to Specialized Investigative Systems is restricted to authorized personnel whose duties require such access.

User permissions are assigned based upon job responsibilities, operational necessity, and any requirements established by the agency operating the system. Personnel granted access must comply with all applicable Department policies, user agreements, security requirements, and governing agency rules.

System activity may be monitored or audited by the Department, the system owner, or other authorized oversight entities.

Unauthorized access, misuse, dissemination, or disclosure of information may result in disciplinary action, loss of access privileges, criminal penalties, or civil liability.

4. Fiscal Impact

OPEN ITEMS TO BE FINALIZED:

• Annual access costs: No known cost at this time.

• Subscription or licensing fees: NA

• Equipment costs: NA

• Training costs: TBD

• Administrative support costs: NA

• Funding source(s): PD Budget

5. Assessment of Potential Disparate Impact

The Department has assessed whether the use of Specialized Investigative Systems could result in a disparate impact on protected classes.

Safeguards include:

• Purpose-based access controls

• Supervisor oversight

• Required user training

• Audit and accountability measures

• Documentation requirements

• Compliance with applicable laws and policies

The Department does not utilize Specialized Investigative Systems to target individuals based solely upon race, ethnicity, religion, disability, sexual orientation, or other protected characteristics.

Information obtained through these systems is used only for legitimate investigative, public safety, and criminal justice purposes.

6. Civil Liberties and Civil Rights Impact Assessment

The Department recognizes that Specialized Investigative Systems may contain sensitive information related to criminal investigations, firearms transactions, ballistic evidence, travel documents, and other law enforcement records.

Safeguards include:

Restricted Access

Access is limited to authorized personnel with a legitimate law enforcement or investigative purpose.

Purpose-Based Use Requirements

System queries and information retrieval must be related to an authorized investigation, public safety objective, intelligence function, or other official law enforcement activity.

Audit and Accountability Measures

System activity may be reviewed, monitored, and audited to identify unauthorized access or misuse.

Information Sharing Restrictions

Information obtained through these systems may only be shared as authorized by law, court order, interagency agreement, or official law enforcement purpose.

Protection of Constitutional Rights

The Department does not utilize Specialized Investigative Systems to monitor, track, or investigate individuals solely because they engage in lawful activity protected by the United States Constitution or the Illinois Constitution.

Investigative activity must be based upon legitimate law enforcement objectives and not upon protected beliefs, viewpoints, associations, or activities alone.

7. Data Storage, Retention, and Third-Party Access

Most Specialized Investigative Systems utilized by the Department are owned and maintained by federal agencies or other governmental entities.

The retention, storage, dissemination, and security requirements governing information within these systems are established by the agency operating the database.

Information obtained from these systems may be incorporated into official police reports, investigative files, evidentiary records, intelligence products, or other Department records when authorized and necessary for law enforcement purposes.

Third-party access is governed by applicable law, system-specific requirements, and policies established by the owning agency.

8. Exigent Circumstances Use

Exigent circumstances involving Specialized Investigative Systems may arise when immediate access to firearms-related information or travel document information is necessary to protect life, prevent serious bodily injury, apprehend dangerous offenders, or respond to active public safety threats.

Examples may include:

• Tracing a firearm recovered during an active violent crime investigation.

• Assisting in the identification or apprehension of a suspect involved in a recent violent offense.

• Verifying travel document information during an investigation involving a dangerous fugitive or other serious criminal activity.

• Obtaining time-sensitive information necessary to support emergency law enforcement operations.

In exigent circumstances, authorized personnel may access available Specialized Investigative Systems consistent with Department policy, applicable law, and system-specific requirements.

Exigent circumstances do not eliminate legal restrictions, documentation requirements, audit requirements, user agreement obligations, or Department policies. Information obtained during exigent circumstances remains subject to the same restrictions governing retention, dissemination, and use that apply during routine operations.

9. Compliance With State and Federal Law

The use of Specialized Investigative Systems will comply with all applicable federal, state, and local laws, user agreements, security requirements, and governing agency policies.

Personnel authorized to access these systems are required to comply with all restrictions governing access, use, retention, dissemination, and disclosure of information obtained through such systems.

10. Summary

Specialized Investigative Systems provide authorized personnel with access to resources that support firearms tracing, travel document verification, and other specialized investigative functions. Access to these systems is restricted and governed by legal requirements, policy

controls, training standards, and oversight measures intended to protect privacy, civil rights, and civil liberties while supporting legitimate public safety and investigative objectives.