VILLAGE OF SHOREWOOD HILLS
Public Health & Safety Committee Minutes - DRAFT

Tuesday, March 28, 2023 – 7:00pm or immediately following the
Parks Committee Meeting
Virtual via Zoom

1. **Call to Order:** Chair Carol Barford called the meeting to order at 7:07pm.

   a. **Roll call:** Committee members present were Carol Barford, Bill Muehl, Jeremy Tunis joined at 7:14pm, Dietmar Bassuner, and Jim Rogers. Cara Silverman and Nadeem Afghan were excused. Also present was Deputy Clerk-Treasurer Chrissy Kahl.

   b. **Note compliance with open meeting law:** Kahl confirmed that the meeting was properly posted.

2. **Public Comments, Appearances and Communications:** No one wished to speak

3. **Approve meeting minutes from January 24, 2023:** Rogers moved, Dietmar seconded to approve with corrections. The first being Rogers being more specific in his recommendation in item #8 to read as: "The creation of a Village of Shorewood Hills public video surveillance policy following the Public Video Surveillance Working Document best practices." The second correction is that Committee member Cara Silverman was marked as absent to the January 24, 2023 meeting but had joined late. Motion carried (4-0).

4. **Discussion of property maintenance ordinance with respect to vegetation:** Muehl moved, Rogers seconded to remove this item from the agenda due to Barford and the Administrator not being able to meet and talk about this item. Motion carried (4-0).

5. **Discussion of potential safety measures at the McKenna Park Boathouse:** Barford started this discussion. Bassuner feels cameras are a helpful tool for law enforcement. Tunis has noticed that there is a small group of very vocal residents in opposition to cameras. Rogers said added lighting will help with safety. He also feels the creation of a video surveillance policy is important to move forward. Muehl agrees with installing cameras still, police will know what they are arriving in to. Even updating the lighting will help. Barford discussed training staff, for backing, on security awareness through CJIS (Criminal Justice Information Service) security policy. Barford would like to pursue the idea of filling in the exact information, what is the content of the policy, to shed light on this for the board's decision-making process. Barford would like feedback on the training section of chapter 5 of the CJIS security policy manual from commissioners. Rogers asked if there is anything else we can do for safety besides additional lighting and possibly cameras? Barford asked that ideas be emailed to her.

6. **Discussion of Dane County Hazard Mitigation Plan:** Barford gave background information on this item. In the Shorewood Hills specific plan they talk about keeping trees in good shape, having an emergency shelter for weather related events, keep

good relationships with agencies, and keep community awareness. Rogers asked do we want to further improve on any of those items or are there items that are not on the list (not just weather related)? Muehl suggested perhaps meeting with DPW Head on a regular basis, every six months or annually. Muehl suggested having a PHS sponsored safety day/event such as Red Cross smoke alarm replacements or give away "Go" bags to keep handy for emergencies. We could also have the Red Cross do a presentation.

7. **Announcements, questions, and/or consideration items for future agendas (no discussion or action to be taken under this item):**
Barford won't be able to attend the May meeting. The May meeting will most likely be canceled.

8. **Next Meeting Date:** April 25, 2023 at 7:00pm

9. **Adjourn:** Muehl moved, Tunis seconded to adjourn the meeting at 8:19pm. Motion carried (5-0).

Respectfully submitted,

Chrissy Kahl
Deputy Clerk-Treasurer

Video and Audio Surveillance

Eff. Date 12/28/2021

Purpose

The Madison Police Department (MPD) recognizes the use of video and audio surveillance technology can significantly aid MPD investigative efforts and promote greater public safety in our community. Yet the use of surveillance technology must also be balanced with the need to protect the privacy rights of the public and MPD employees when and where applicable. MPD use of surveillance technology will be consistent with any applicable City of Madison Administrative Procedural Memos (APMs) and ordinances.

MPD personnel routinely utilize the City Enterprise Camera System. MPD personnel will also deploy and utilize other, stand alone, covert video or audio surveillance technology when appropriate. These deployments are generally limited in duration and are part of an on-going investigation of specific criminal activity for purposes of collecting evidence necessary for criminal or municipal prosecution.

Use of City of Madison Enterprise Camera System

All commissioned MPD employees are authorized to use the City Enterprise Camera System as outlined in this standard operating procedure (SOP). Civilian MPD employees may be authorized by the Chief of Police to access the system where there is a job-related need. No MPD employee will access or utilize the system prior to receiving training in its use.

MPD Information Management and Technology (IMAT) is responsible for administration and maintenance of appropriate user/access lists. Any complaints about use of the system will be routed through Professional Standards and Internal Affairs (PS&IA), consistent with department SOP.

Signage will be posted at appropriate MPD locations alerting the public to the use and deployment of video recording.

Authorized Use
MPD employees are only permitted to access the City Enterprise Camera System for official law enforcement business, under any of the following conditions:

- To assist with the investigation of criminal or otherwise unlawful activity.
- To assist with internal investigations as appropriate by the Chief or designee.
- To protect and secure MPD/City of Madison facilities.
- To maintain order during planned and unplanned events.
- As part of a proactive review of a tactical incident, or for internal training opportunities with prior supervisory approval.
- To remotely monitor environmental conditions or other non-investigative circumstances necessary to perform an employee's duties (i.e., weather or traffic conditions, safety hazards, management of resources, etc.).
- To preserve previously-discovered items or view/retrieve preserved evidence.

Prohibited Uses
MPD use of the City Enterprise Camera System is intended to monitor publicly available spaces. Employees will not use the system to view any area where a reasonable expectation of privacy exists (i.e., through a window into a private residence) without a warrant or other lawful justification (i.e., exigent circumstances).

Employees will not utilize the system to track or surveil any individual or vehicle without a specific and articulable law enforcement purpose. Cameras will not be accessed for any personal use.

MPD use of the City Enterprise Camera System is subject to audit, consistent with the System Audits SOP.

Retention/Evidence

City of Madison Information Technology (IT) is responsible for maintenance of the City Enterprise Camera System and for storage of video captured by the system. Video is generally retained for fourteen (14) days, unless a recording is requested under the Wisconsin Public Records law, it contains evidence, or it is determined to have other value in being preserved. Cameras on the City Enterprise Camera System deployed to sensitive areas within MPD facilities are retained for a one-year period.

Requests to preserve video on the City Enterprise Camera System server should be directed to the MPD Forensic Services Unit (FSU). The request shall be completed in a timely manner and shall include case number(s), camera name(s), date(s), and time frame(s) to be preserved for evidentiary purposes. This information shall also be documented within an official police report.

If a record is created through the preservation of video from the City Enterprise Camera System, that record will be maintained in accordance with MPD's records retention schedule. If the video contains evidence of unlawful activity, it will be maintained in accordance with MPD's digital evidence policies and procedures.

The capture and preservation of video stills ("screen shots") is permissible in instances where the full video is not necessary or required for evidentiary purposes or to supplement retention of the video. Video stills are not an equivalent substitution for proper video evidence identification and retention.

Pursuant to the State of Wisconsin's "Recording Custodial Interrogations" statutes (Wis. State Statutes 938.195 and 968.073), MPD has installed in all district stations video and audio recording equipment for purposes of recording custodial interrogations of individuals under 17 years of age and of adults involved in felonious incidents. MPD in-car audio/video systems may also be used to record custodial interrogations when necessary. All video and audio records associated with custodial interviews are maintained in accordance with applicable MPD departmental procedure.

Any requests to add or to move cameras on the City Enterprise Camera System will be forwarded to the Chief's office.

MPD Video/Audio Systems

MPD personnel deploy additional video/audio systems on a regular basis (in-car video, body worn cameras, unmanned aircraft systems, etc.). MPD personnel will only utilize or access those systems for official law enforcement purposes. Video/audio collected through those systems will be retained for 180 days unless a recording is requested under the Wisconsin Public Records law, it contains evidence, or it is determined to have other value in being preserved.

Use of Other Video/Audio Surveillance Systems

MPD personnel may deploy additional surveillance technology (i.e., covert cameras) as part of an active investigation. Such deployment will be of a limited duration and will only be done with approval as outlined below. MPD will not reveal the deployment or location of covert surveillance technology used in conjunction with criminal investigations unless the harm to the integrity and success of the investigation is outweighed by other public interests (i.e., the identification and apprehension of a fugitive). Access to covert video/audio surveillance deployed as part of an active investigation is limited to personnel authorized by the MPD commander in charge of the investigation.

MPD personnel may be provided with access to third-party video systems. MPD personnel will only utilize third-party systems for official police business.

The procedures outlined below serve to clarify and establish guidelines for further deployment of video and audio surveillance technology by MPD personnel. As noted earlier, MPD personnel use overt and covert surveillance strategies depending upon the situation. Overt surveillance for purposes of this SOP shall be defined as video or audio surveillance where the subject(s) being recorded is(are) aware of the recording.

Covert surveillance is defined as video or audio surveillance where the subject(s) is(are) not aware of the recording.

Prior to the use and deployment of video and audio surveillance technology, MPD employees shall adhere to the following:

1. All requests for the new use and deployment of video or audio surveillance will be directed to an MPD Command Officer. The Command Officer shall review the request and ensure the request is compliant with this SOP and that the anticipated installation/use of the video or audio surveillance is compliant with all applicable legal requirements.

2. The reviewing Command Officer will then review the request in light of the below matrix seeking higher level approval for the request if necessary:

Type of Surveillance	**To be Authorized by**
Covert video (only) surveillance related to criminal investigations	**Chief of Police with Commander recommendation**
Covert audio (only) surveillance related to criminal investigations (e.g., suspect telephone recording, etc.)	**Chief of Police with Commander recommendation**
Covert video or audio surveillance related to any internal, PS&IA employee investigation	**Chief of Police Only**
Access to third-party video systems	**Command approval; notice to Chief of Police**

Original SOP: 11/11/2015
(Revised: 03/04/2016, 11/15/2016, 11/30/2017, 10/09/2018, 10/09/2020, 12/28/2021)
(Reviewed Only: 01/30/2019, 01/31/2020, 01/31/2023)

UW-Madison Policy Library

Security Surveillance Camera and Video

Layout for printing

POLICY NUMBER: UW-402

RESPONSIBLE OFFICE: UW-Madison Police Department

University Policy

RATIONALE/PURPOSE: The policy is in place to:

- Ensure people viewing video surveillance are authorized to do so
- Ensure individuals requesting video surveillance and/or recording are authorized to do so
- Ensure a process of accountability for the use of video surveillance and/or recording
- Ensure that standard equipment is being installed campus-wide
- Ensure compliance with Federal, State and/or University of Wisconsin guidelines

SCOPE:

The policy is applicable to current and future UW–Madison and UW System sites and facilities including, UW Transportation Lots and parking garages, all properties leased and sub leased from and for UW–Madison, which fall under the operational jurisdiction of any or all of the following entities of the UW–Madison: Police Department (UWPD), Division of Information Technology (DoIT), and Facilities Planning and Management (FP&M).

The policy applies to all personnel, schools, colleges, departments, offices and other divisions of the University of Wisconsin–Madison that utilize video surveillance except those exempted below. The following are exempt from this policy:

- Video recording equipment used by the UWPD for evidentiary or investigative purposes
- Cameras used for academic and research purposes
- Video equipment used for the recording of public events or for broadcast, educational or operational purposes. Examples include videotaping of athletic events for post-game review; videotaping of concerts, plays and lectures; videotaped interviews of persons; Automated Teller Machines.
- Transportation Services parking gate cameras used for operational purposes (to the extent that FP&M Transportation Services personnel may view the camera images without permission, but the video will be stored in a secure location as specified below).

Monitoring of public areas for security purposes will be conducted in a manner consistent with all existing university policies, including Non-Discrimination Policy, Sexual Harassment Policy and CLERY. Monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by law. Examples include but are not limited to individual dormitory rooms, restrooms and locker rooms. When applicable, staff involved in video monitoring will be appropriately trained and supervised by a member of the UWPD in the responsible use of this technology. Video information obtained through monitoring will be used exclusively for safety, security, human Resources, risk management, training, and law enforcement purposes. Recorded data will be stored in a secure location with access limited to authorized staff

POLICY:

Policy Summary

The policy codifies the use of cameras and video equipment in the protection of lives, research, and property of the University of Wisconsin–Madison campus community. Video surveillance (CCTV and Web Cam) is used to enhance security, safety and quality of life of the community by integrating best practices with state-of-the-art technology. The policy outlines when and how fixed security cameras are to be installed, how images and data are to be stored and recorded, and the conditions under which stored images, video or data are to be used and released. The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

Policy Detail

I. Responsibilities

1. The UWPD is authorized to oversee and coordinate the use of video surveillance.
2. The Associate Vice Chancellor/Chief of Police or designee must authorize all video surveillance.
3. The Associate Vice Chancellor/Chief of Police or designee will review all requests to release video records. Any request for release of records will be made in writing.
4. The UWPD Director of Security Video Operations is appointed the administrator of the campus surveillance camera and video system.
5. The Associate Vice Chancellor/Chief of Police, Associate Vice Chancellor for FP&M and the Director, DoIT Systems Engineering & Operations at the direction of the Chief Information Officer and Vice Provost for Information Technology oversight board and will review this policy annually to recommend revisions, if needed.
6. DoIT will manage the servers associated with cameras and video surveillance.
7. FP&M or their designee will be responsible for, and have the authority over, the execution of construction activities of premise wiring in all UW–Madison buildings to ensure that all installations are both code compliant and meet University standards. FP&M Physical Plant will coordinate all installations with UWPD and DoIT.
8. Requests for repair, maintenance and replacement will be routed through the UWPD to the FP&M Physical Plant.
9. Purchasing of cameras will be handled by UWPD in consultation with DoIT and FP&M Physical regarding specifications such as camera types and megapixels.
10. UWPD IS Unit, DoIT and FP&M Physical Plant will review campus standards pertaining to cameras annually and make necessary adjustments.
11. Deans, Directors or designees of each School or College are responsible for the full implementation of this policy within their respective areas.
12. Building designee that is appointed to work with the camera administrator is responsible for keeping their list of users up to date and notifying the camera administrator of changes.

II. Security surveillance camera access and recorded data use and operation

1. UWPD will have access to all video surveillance.
2. UWPD, DoIT and FP&M will monitor developments in the law, technology and security industry practices to ensure that camera surveillance is consistent with best practices and compliant with federal and state laws.
3. UWPD will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed and report results to the oversight

board.

4. UWPD staff involved in video monitoring will be appropriately trained in responsible use of the technology.
5. UWPD's IS Unit, in conjunction with DoIT, will provide periodic administrative updates and guidance to video surveillance camera systems operators including Web-Client users.
6. Video surveillance information obtained through monitoring will be used exclusively for safety, security, human resources, risk management, training and law enforcement purposes, except where noted as "exempt" above.
7. Monitoring of individuals solely based on characteristics of race, gender, sexual orientation, disability or other protected classification is explicitly prohibited.
8. Monitoring of the non-public areas of privately owned buildings within the view of the cameras is prohibited except by court order or immediate life safety issues.
9. Authorized Web Client users or operators of video surveillance systems located in their respective buildings are individuals who have been assigned responsibility by deans, directors, or other executive authorities. The list of the authorized users will be updated annually by the UWPD IS Unit.
10. All surveillance records will be stored in a secure centralized location for a period of 120 days.
11. Any Select Agent (SA) location will be on its own video network, separate from the general campus-wide security surveillance network. The SA labs and research areas will be equipped with a notification system informing DoIT and UWPD of problems or issues with the video surveillance system.

III. Installation and issuance

1. UWPD will make assessments for new camera locations not already in existence. The assessments will be made in consultation with building occupants, DoIT and FP&M as needed and appropriate.
2. UWPD's IS Unit will maintain a current inventory of permanent camera installations.
3. UWPD's IS Unit will facilitate access to recorded images of possible crimes and incidents requiring investigation.
4. All requests for installing video surveillance on UW–Madison property must be routed to the IS Unit of the UWPD. A representative of the IS Unit trained in camera placement will then conduct a site assessment documenting proposed camera locations and document requested areas where current conditions are not feasible for placement and forward to the appropriate entities, i.e., FP&M Physical Plant Customer Service, DoIT, AIMS, to develop a cost estimate to be provided to the requestor.
5. All video surveillance equipment must comply with current University standards. See Appendix.
6. Notification of camera and network problems or issues will occur through an alarm or other notification system authorized by DoIT.
7. Video surveillance will connect to the authorized server and in circumstances identified by the UWPD IS Unit, will be encrypted.
8. All new installations of video surveillance scheduled after the effective date of this policy must be in compliance with the terms and conditions of this policy and must meet the technical specifications and campus standards listed in the Appendix.
9. Existing installations must be brought into compliance with this policy at the time that replacement or upgrades of security surveillance camera systems and components occurs.

10. All original recorded images generated by surveillance cameras must be stored in a secure location established by DoIT and UWPD.

Consequences for Non-Compliance

Violations and sanctions:

Violations of this policy by operators of surveillance camera systems will be considered misconduct on the part of the employee and will be subject to institutional or criminal sanctions

UWS 18.06 Conduct on University Lands

(6) PHYSICAL SECURITY COMPLIANCE. (a) No person may ignore, bypass, circumvent, damage, interfere with, or attempt to deceive by fraudulent means, any university authorized security measure or monitoring device, whether temporary or permanent, that is intended to prevent or limit access to, or enhance the security of, university lands, events, facilities or portions thereof. (b) No person may duplicate, falsify or fraudulently obtain a university key or access control device, or make any unauthorized attempt to accomplish the same. (c) No person who is authorized to possess a university key or access control device may transfer a university key or access control device to an unauthorized person, nor may any unauthorized person be in possession of a university key or access control device. (d) Any university key or access control device in the possession of an unauthorized person may be confiscated by any authorized University official.

UWS 18.13 Penalties

Unless otherwise specified, the penalty for violating any of the rules in ss. UWS 18.06 to 18.12 shall be a forfeiture of not more than $500, as provided in s. 36.11(1)(c), Stats.

Note: Violations of the rules in ss. UWS 18.06 to 18.12 will be processed in accordance with the citation procedure established in s. 778.25, Stats.

History: Cr. Register, March, 1976, No. 243, eff. 4-1-76; am. Register, November, 1991, No 431, eff. 121-91; CR 08-099: renum. From UWS 18.07 and am. Register August 2009 No. 644, eff. 9-1-09.

Supporting Tools

Appendix: Camera Specifications from 2014 Request for Proposal – UW–Madison Standards

Responsibilities

This policy will be maintained by the Video Surveillance Oversight Board and revisions may be made as needed.

Members: UW–Madison Associate Vice Chancellor/Chief of Police, UW–Madison Associate Vice Chancellor for Facilities Planning and Management and the Director of the UW–Madison Division of Information Technology.

Appendix – Camera Specifications from 2017 Request for Proposal

All Cameras:

- Work with the Milestone XProtext Corporate 2016 R2 Edition
- PoE
- Work within WI temperatures Indoors- -10C to 50C, Outdoors -40C to 50C

PTZ (Point to Zoom) Outdoor Cameras:

- Day/Night Functionality
- H.264 compliant
- Tour Recording Capable
- 20x optical zoom or better
- Wide Dynamic Range compatible with the ability to account for varying environmental

conditions

- 1080p compliant or better
- Image stabilization
- SD/ Card compatible with ability up to or more than 64gb
- Standard 3 year warranty or better
- Auto focus IR Illuminator

PTZ Indoor:

- Wide Dynamic Range compatible with the ability to account for varying environmental conditions
- H.264 Compliant
- Tour Recording Capable
- 20x optical zoom or better
- 1080p compliant or better

TIME SYSTEM NEWSLETTER

A Newsletter for the Crime Information Bureau Published by the Wisconsin Department of Justice

January 2023

IN THIS ISSUE

Message from our Director

Last year was a very busy year for CIB and our TIME System users. The TIME System is heavily used every day. The average transactions per day for 2022 was 159,369, this is up from 151,580 in 2021. There are over 13,500 workstations in Wisconsin that connect to the TIME System.

Over the next two years the CJIS Division at the FBI will be working to modernize the CJIS Security Policy with a goal of a final completely revised policy in the Spring of 2025. On December 7, 2022, version 5.9.2 was released. CIB is currently reviewing the changes and how it may impact our users.

I am very happy to announce the return of the CIB Conference in September of 2023. The conference is scheduled for the week of September 18th at the Radisson Hotel & Conference Center in Green Bay. The final dates will be announced in late April or early May. Please mark your calendars!

One of CIB's goals for 2023 is to return to publishing newsletters at least once per quarter. We welcome your feedback and ideas for new articles. As the Director of CIB, I also welcome your feedback on what CIB is doing well, but also what we can do to improve.

Thank You!

Brad

CJIS Security Policy Updates

Version 5.9.2 has arrived!

The newest update to the CJIS Security Policy was published December 7, 2022. The newest update of the CJIS Security Policy, marks the beginning of the modernization of the policy. The FBI will be revising and updating the policy section by section as well as adding new sections. The FBI estimates that there will be two policy updates per year while this process is ongoing, with the final update to version 6.0 anticipated for Spring 2025. Be on the lookout for more information on this in the 2023 In-Service Training.

"Kayleigh's Law"

Non-Expiring Protection Orders

A new law was passed in Wisconsin that allows for the entry of permanent or non-expiring protection orders for victims of sexual assault. Kayleigh's Law was signed into law with 2021 Wisconsin Act 256. Kayleigh's law amends statutes that govern the expiration limits of injunctions.

The victim may request that a protection order be issued permanently to ensure the victim will not have to face their abuser again. This law is applicable for domestic abuse injunctions, child abuse injunctions, individuals at risk (vulnerable adult) injunctions, and harassment injunctions.

Currently, the TIME System does not allow entry of a non-expiring protection order. In order to enter these new permanent non-expiring protection orders, agencies should enter the expiration date of December 31, 2150. Agencies may also include in the MIS Remarks that the protection order is non-expiring.

Person With Information

PWIs Can Assist in Locating Missing Persons

How is adding a Person with Information to a Missing Person entry helpful in locating a missing individual?
A potential example is, an officer pulls over a driver for speeding. When the officer approaches the vehicle, they notice an infant in the backseat. How do they determine if it is the child of the driver? What are the chances the officer will be able to obtain the necessary documents to identify the child and determine if they are missing?
A Person with Information (PWI) is a person who may have information regarding the location of a missing person. The TIME system has the capability to add two PWIs to a missing person entry. When a PWI is queried (drivers query, criminal history query, etc.) the missing person entry that includes the PWI will also be returned with the response. This can provide a valuable investigative lead to the officer and may lead to the return of a missing person.
To add a PWI to a missing person the following criteria must be met.

- The missing person was last seen under circumstances that pose a risk to the safety of that person. PWI information may only be added to missing person records in the endangered or involuntary categories. Only the agency that entered the missing person record may add PWI information to the record.
- There is a substantial likelihood that the PWI has relevant information about the missing person that could result in the recovery of the missing person.
- The identity of the PWI has been disclosed to the general public through

an Amber Alert or other formal notification.

- Entering information concerning the PWI could assist the law enforcement agency to identify and interview the PWI and the resulting information could assist in the recovery of the missing person.

- The PWI cannot be located, and time is of the essence.

- There is no prohibition under state law on the publication of information concerning the identity of a person for whom a warrant has not been obtained.

- The PWI entry must include agency contact information and guidance for the officer who encounters the PWI.

Adding DNR Information to Person Entries

One source of data that is often overlooked in person entries are the DNR files. When users query 0781 or 1781 in Portal 100, they will not receive a response back from DNR files. The user will have to do a separate query on the DNR Person files to obtain this information. This can be a great investigative tool as it can provide a phone number, an address, physical descriptors, etc. which can be especially helpful if the person does not have a driver's license or ID card. If the individual has a DNR Customer ID number, the agency can enter that Customer ID number as a Miscellaneous ID number using the prefix "PI" whenever making a person entry. This may be helpful in confirming the identity of an individual. DNR files also show citation history for the individual, which may provide information that the subject has access to weapons (bow or gun hunting). DNR files also provide information on any DNR vehicles that may be registered to that individual (boats, snowmobiles, ATVs, etc.). Be sure to keep DNR files in mind when querying for max data. Querying the information could give you a break in your case.

NICS Denial Notification

$H For NICS Denied

Beginning on September 26, 2022, agencies may have seen a new unsolicited "$" message from NCIC. This new unsolicited message, $.NDN, is a NICS Denial Notification.

These notifications are sent to agencies when an individual is denied the purchase of a firearm by NICS within an agency's jurisdiction. The unsolicited message will be sent to the agency's main terminal informing them of the denial. The message will include the name, demographic information of the individual who was denied, the reason for the denial, and where the attempted purchase was made.

It is at the agency's discretion to determine if action needs to be taken based on the message. Please reach out to the DOJ Firearms Unit with any questions.

Here is a sample message:

****
****
FIREARM DENIAL NOTICE:
A PERSON PURCHASING/RESIDING IN YOUR JURISDICTION WAS RECENTLY DENIED THE TRANSFER OF HANDGUN
****
****
THE FBI ENCOURAGES YOU TO CONTACT YOUR LOCAL BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES OFFICE PRIOR TO TAKING ACTION. CHARLESTON ATF, 304-234-5678

THENATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) SECTION CONDUCTED A NAME SEARCH USING DESCRIPTIVE DATA, NOT FINGERPRINTS, FOR A FIREARM BACKGROUND

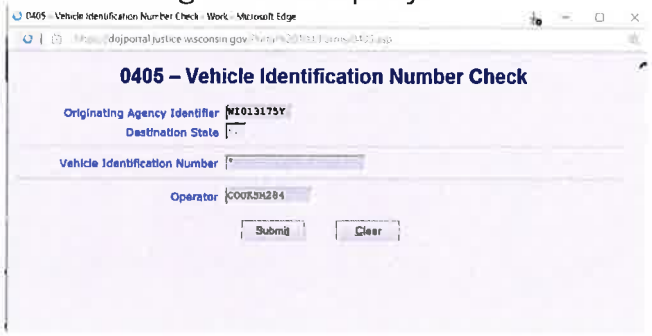
CHECK WHICH WAS DENIED ON 4/26/2022, 02:02:23PM FOR:
NAME: DOE, JOHN L. NTN: 102356748
SEX: M RACE: W DATE OF BIRTH: 10-11-1990 PLACE OF BIRTH: WV
HEIGHT: 6'1" WEIGHT: 185 SOCIAL SECURITY NUMBER: 123-45-6789
RESIDENCE ADDRESS: 456 AMERICAN WAY, APPLE PIE, APPLE PIE COUNTY, WV 22445
INFORMATION RECEIVED INDICATES THE ATTEMPTED PURCHASER IS PROHIBITED FROM RECEIVING OR POSSESSING FIREARMS IN THE STATE OF PURCHASE AND/OR STATE OR RESIDENCE, BASED ON:
SUBJECT OF QUALIFYING PROTECTION ORDER
THE ATTEMPTED PURCHASE OCCURRED AT:
FIREARM DEALER: USA ARMS
ADDRESS: 123 MAIN STREET, HOMETOWN, HOMETOWN COUNTY WV, 23456
PHONE: 304-625-1002
SHOULD YOU HAVE QUESTIONS REGARDING THIS NOTIFICATION, PLEASE VISIT: (Web address will be inserted when established WWW.FBI.GOV)
THIS NOTIFICATION WAS ALSO PROVIDED TO THE FOLLOWING ORI(S):
WV0470150 SO APPLE PIE COUNTY 304-478-0000
WV0625630 PD HOMETOWN 304-457-0000

Portal Form 0405

Vehicle Identification Number Check

When entering a vehicle into the TIME system, some agencies think that they only have the report/vehicle title information to use as supporting documentation; however, there is another source in which users can obtain information on the vehicle. The Vehicle Identification Number Check form in Portal (0405 query) allows a user to query the VIN attached to a vehicle and obtain information such as: vehicle type, make, model, model year, manufacturer location, body type, physical descriptors, etc. Even if a vehicle is not registered with the Department of Transportation, the VIN may have information tied to it that can be used for entry. Some examples of types of vehicles that may not be registered through DOT, but are searchable are trailers, snowmobiles, ATVs, etc.

So, prior to entering stolen/missing vehicles into the TIME system, please remember to use the 0405 query to find additional data. The user may need to check the NCIC Code Manual to find the correct make/model codes that were located using the 0405 query.



/0405 1692 3CC5E2B4 WI013175Y
NLET 299923 13 10/19/22 13:48 01 OF 02
GVR NL0000000
11:48 10/19/2022 57215
11:48 10/19/2022 27066 WI013175Y
*00299923XX
TXT
VEHICLE DATA
VIN: 112233MKLS908756
Vehicle Type: TRAILER
Make: EAGER BEAVER
Model Year: 1995
Transmission Type: Not Applicable
Adaptive Cruise Control: Not Applicable
Adaptive Driving Beam: Not Applicable
Additional Information: 0= standard length , 2= 2ft 0" longer than standard etc and letters will represent shorter deck length i.e A= 1 ft 0" shorter, B = 2 ft shorter etc
Air Bag Location Curtain: Not Applicable
Air Bag Location Front: Not Applicable
Air Bag Location Knee: Not Applicable
Air Bag Location Seat Cushion: Not Applicable
Air Bag Location Side: Not Applicable
Anti Lock Brakes: Not Applicable
Automatic Pedestrian Alerting Sound: Not Applicable
Automatic Reverse System: Not Applicable
Battery Type: Not Applicable
Bed Type: Not Applicable
Blind Spot Monitoring: Not Applicable
Body Cab Type: Not Applicable
Bus Type: Not Applicable
Bus Floor Configuration: Not Applicable
CAN_AACN: Not Applicable

DOT Update

End of Month Registrations

Wisconsin DMV has recently implemented changes to the expiration date when issuing new registration for several types of vehicles. Included in this new change are autocycles, automobiles, dual-purpose farm vehicles or dual-purpose vehicles (8,000 pounds or less),

and light trucks. Other registration types are not affected by this change.

DMV's new policy went into effect on September 11, 2022. New registration and renewal dates for the previously mentioned vehicle types will consist of the month in which the vehicle was first registered. The registration will then expire the last day of that same month, the following year. For example, a light truck first registered October 5, 2022, will have a registration expiration of October 31, 2023.

Current registrations will not have their expiration date advanced until the registration is renewed. Due to individual registration's renewal habits, it could take until January 2024 or possibly later for all current automobile registrations that expire on a day other than the last day of the month to advance to the last day of the expiration month.

Auto-Cycle Expiration & Plate Design Updates

DOT has announced a new expiration date system for autocycle registrations. Prior to September 2022, autocycles were registered on an annual basis with all autocycle registrations expiring April 30. Autocycle (ACY) plate designs have "APR" printed on the plate.

Beginning on September 11, 2022, DMV announced the change to autocycle registrations expiring on a monthly basis. Plates now expire on the last date of the month of registration. A new plate design was also announced where the "APR" will no longer be printed on the plate.

New autocycle plates will be issued starting in September 2022. The new plates will have a white background with black numbers and letters. "Autocycle" is printed at the top of the plates; "WIS" is printed at the bottom center of the plates.

The autocycle plates printed with APR continue to be valid for use on vehicles, provided they have valid registration. DMV will reissue plates where the registration expiration is not April of each year.

New Plate Type Code: Fleet Plates!

Beginning on December 1, 2022, a new plate type is available from DOT. This new plate type, fleet plates, are issued to eMV fleet customers only. There are no special parking privileges associated with fleet plates.

The new fleet license plates will have a white background with green and blue details with blue numbers and letters. "Wisconsin" is printed at the top and "Fleet" is printed at the bottom of the plates.

To query a fleet plate, use license plate type code "FL". To enter a fleet plate as lost or stolen, use license plate type code "CO" (commercial).

Record Retention

What Do I Need to Keep on File?

Do I really need to keep everything I query for an entry? How long must I keep it?

CIB requires that you keep certain documentation in your case file to support any active entry into the TIME System. You must keep any responses that support entry of certain information into your entry. If you query a subject's CHRI and find aliases, social security numbers, and scars, marks, and tattoos that you enter, you must keep a copy of the CHRI in your case file for documentation or document the State ID number/FBI number of the record so it can be queried to find the information again.

One response you should always keep is a DOT return. If you are entering a stolen license plate and the expiration year of the plate is listed as 2022, you will need to retain this documentation. If the owner goes to DOT and gets a new plate number, DOT will cancel the stolen registration and associate the new plate information with the vehicle. But querying the stolen registration will return a new expiration date from the new registration. Keeping the original query response for DOT will show that you entered the stolen license plate with the correct year of expiration during an audit.

CIB does not require that you keep all documentation for entries forever. Once an

entry is removed from the TIME System, CIB no longer has retention requirements for the documentation. You can use your agency's retention schedule to determine when to destroy documentation. It might be beneficial to keep documentation for an old entry if a new entry of the same item or warrant is being made to show that it was entered previously.

CIB Contacts

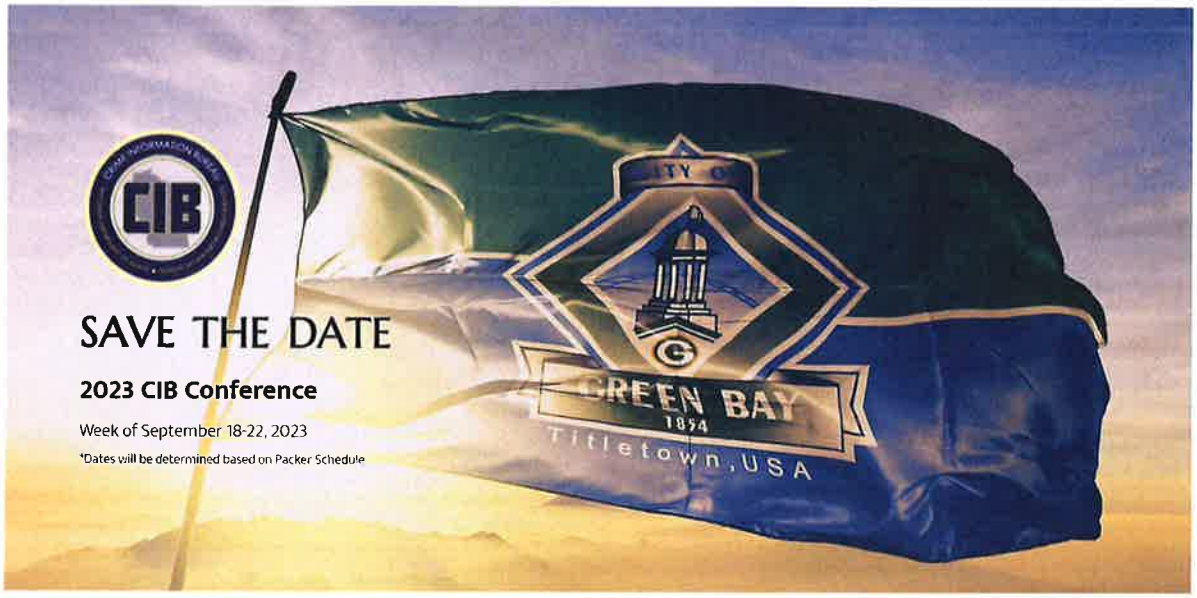
	Name	Telephone	Fax Number	Email
Director	Bradley Rollo	608-264-8134	608-267-1338	rollobr@doj.state.wi.us
Deputy Director-TIME System/Criminal History	Katie Schuh	608-266-0335	608-267-1338	schuhkr@doj.state.wi.us
Deputy Director-Firearms	Andrew Nowlan	608-267-2776	608-267-1338	nowlanam@doj.state.wi.us
TIME & Technical Services Manager	Vacant		608-267-1338	
Training Officer - Senior	Emily Freshcorn	608-261-5800	608-267-1338	freshcornek@doj.state.wi.us
Training Officer	Sarah Cook	608-261-7667	608-267-1338	cooksm@doj.state.wi.us
Training Officer	Ben Brandner	608-266-9341	608-267-1338	brandnerb@doj.state.wi.us
TIME Systems Operations Manager	Brian Kalinoski	608-266-7394	608-267-1338	kalinoskibt@doj.state.wi.us
TIME Analyst	Sarah Steindorf	608-261-8135	608-267-1338	steindorfsr@doj.state.wi.us
TIME Analyst	Vacant	608-266-7792	608-267-1338	
TIME Analyst	Zach Polachek	608-264-9470	608-267-1338	polachekzd@doj.state.wi.us
TIME Analyst	Jeanette Devereaux-Weber	608-266-2426	608-267-1338	devereauxweberjd@doj.state.wi.us
TIME System Audits				cibaudit@doj.state.wi.us
TIME Billing			608-267-1338	timebilling@doj.state.wi.us
AFIS Operations Manager	Adrianna Bast	414-382-7500	414-382-7507	bastar@doj.state.wi.us
Criminal History Section Record Check & Criminal Records	Craig Thering	608-261-6267	608-267-1338	theringcd@doj.state.wi.us
	Brandon Smith	608-266-0872	608-267-1338	smithbp@doj.state.wi.us
Firearms Unit	Jen Garske	608-264-6373	608-267-1338	garskejt@doj.state.wi.us
	Mike Worth	608-261-8104	608-267-1338	worthmj@doj.state.wi.us
TRAIN		608-266-7792	608-267-1338	CIBTrain@doj.state.wi.us
TSCC		608-266-7633	608-266-6924	
WORCS		608-266-7314		cibrecordcheck@doj.state.wi.us
WILEnet		608-266-8800		wilenet@doj.state.wi.us

Check the WILEnet website for additional data at https://wilenet.widoj.gov/

Resources

Name	Telephone/Website	Terminal Identifier	Email/Fax
National Crime Information Center (NCIC)			
Recalls	304-625-3000		ioau@leo.gov
Hits to Wants	304-625-9245		304-625-9899
WI Division of Criminal Investigation (DCI)			
General	608-266-1671		
AMBER/Silver Alerts	844-WSP-HELP		info@wisconsincrimealert.gov
International Justice and Public Safety Information Sharing Network (Nlets)			
Control Center	800-528-4020		helpdesk@nlets.org
WI Crime Information Bureau (CIB)			
TIME System Control Center	608-266-7633	TSCC	
Training, Policies & Manuals	www.wilenet.widoj.gov		
Fingerprint card requests	See link below		
WI Recalls			cibtrain@doj.state.wi.us
WI Dept of Corrections (DOC)			
Community Corrections	608-240-5300		
Central Records	608-240-3750		
Monitoring Center	888-222-4362		
WI Dept of Natural Resources (DNR)			
Enforcement	608-266-2141	WDNR	
Registration	608-266-2621	RDNR	
WI Dept of Transportation			
Vehicle Records	608-264-7447	WREG	
Driver's Records	608-264-7049	WOLN	driverrecords.dmv@dot.state.wi.us
National Center for Missing or Exploited Children (NCMEC)	800-THE-LOST www.missingkids.com	VA007019W	
National Insurance Crime Bureau (NICB)	847-544-7000	ILNICB000	investigativeassistance@NICB.org
WI Clearinghouse for Missing & Exploited Children & Adults	800-THE-HOPE		wimissingpersons@doj.state.wi.us
WI Consolidated Court Access (CCAP)	https://wcca.wicourts.gov/		
US I.C.E. Bulk Cash Smuggling Center (BCSC)	866-981-5332	VTICE1600	

Fingerprint card requests https://forms.fbi.gov/cjis-fingerprinting-supply-requisition-form



2023 CIB Conference
Radisson Hotel & Conference Center
Green Bay, WI

We are pleased to announce the return of the CIB Conference in 2023 during the week of September 18, 2023. Actual dates will be set once the Green Bay Packer schedule is released for the 2023 year. Our preferred dates will be September 20 – 22, 2023 if there is not a Thursday night game during this week.

Look for the return of some great plenary speakers and breakout sessions to include such topics as:

- NLETS
- School Safety
- CJIS
- Officer and Dispatcher Wellness programs
- Chaplains in your Agency
- Cybersecurity
- UCR and Use of Force Data
- And of course, updates from TIME & Tech, Firearms, and the Criminal History units

Questions for Video Surveillance Policy Development

1. What are the significant threats to life safety in VoSH? Who determines this?

2. What are the significant threats to property in VoSH? Who determines this?

3. Who should submit a request for permanent video surveillance? To whom?

4. Who should decide whether to purchase and implement video surveillance? Who decides to end video surveillance after it has been implemented?

5. If / How should the use of the video system be reviewed, other than according to the state and federal rules?

6. How should the public be made aware of video systems and rules around their use (e.g., CJIS, TIME, etc.)?

7. Are there other ways to mitigate a given threat besides video surveillance?