

---

**REPORT OF:** President’s Work Group to Develop City-Wide Surveillance  
Equipment and Data Management Policies

**TITLE:** Recommendations on Surveillance Technology Use and  
Acquisition

**DATE:** 1/16/2020

---

**WORK GROUP MEMBERS:** Alder Rebecca Kemble (Chair), Alder Paul Skidmore, Alder Samba Baldeh, Alder Sheri Carter, and Ledell Zellers as Alder through April, 2019 and as resident member from August, 2019.

## **BACKGROUND**

In 2003, the Common Council established the Ad Hoc Committee on Security Cameras, which was tasked with developing a city-wide policy on use and installation of security cameras. The Committee collected survey information on City agencies’ security camera usage. As a result of that survey, the Committee recommended developing “guidelines for agencies to use in writing their own policies” through the creation of an Administrative Procedure Memorandum (APM). APM 3-17, Use of Surveillance Cameras (<https://www.cityofmadison.com/mayor/apm/3-17.pdf>), and APM 3-9, Appropriate Use of Computer Resources (<https://www.cityofmadison.com/mayor/apm/3-9.pdf>), are currently in effect.

In 2017, the President’s Work Group on Police and Community Relations recommended the creation of a “policy governing the purchase and use of all surveillance equipment employed by all City agencies including MPD” (p. 11).<sup>1</sup> The Work Group expressed concern over the growing ubiquity of surveillance technologies and the lack of a comprehensive surveillance policy for the City.

Additionally, concerns were raised by alders and residents that many of the cameras owned and operated by the City had the capability of rotating, zooming and recording video of private spaces and residences. Council members thought it important to develop policy prohibiting the viewing and recording of private spaces in the interest of protection from unreasonable searches and protection of civil liberties, including freedom of speech or association.

In order to carry out the development of the recommended policy, on December 5<sup>th</sup>, 2017, the Common Council approved a resolution establishing the President’s Work

---

<sup>1</sup> Report of the President’s Work Group on Police and Community Relations, submitted 5/12/2017.

Group to Develop City-Wide Surveillance Equipment and Data Management Policies (RES-17-00937).

## **CHARGE OF THE WORK GROUP**

The charge of the President's Work Group to Develop City-Wide Surveillance Equipment and Data Management Policies is to:

- Develop a policy governing the purchase and use of all surveillance equipment employed by all City agencies, also addressing data management and storage, which will be developed in consultation with City of Madison staff and officials, including staff from Information Technology, the City Attorney, and all departments and divisions that currently use or plan to utilize surveillance equipment;
- Seek expert opinions from a variety of departments;
- Use a racial equity and social justice lens throughout its work; and
- Create an inventory of all City of Madison surveillance equipment

## **SUMMARY OF RECOMMENDATIONS**

The President's Work Group to Develop City-Wide Surveillance Equipment and Data Management Policies (Surveillance Work Group) collaborated with City staff to develop a citywide policy on the acquisition of surveillance technology in the form of a proposed ordinance. The Work Group makes the following recommendations:

- That the Common Council approve the proposed ordinance on surveillance technology;
- That the Common Council Executive Committee (CCEC), in consultation with the Mayor, further develop the approval processes referred to in the proposed ordinance;
- That the CCEC and the Mayor review the Madison Police Department resident camera registration program with a view towards increasing transparency for the general public;
- That city staff to continue working with the Mayor to develop a corresponding APM so that City agencies have clear direction on how to comply with the ordinance; and
- That the Common Council seek a more precise definition of "active investigation" as used by MPD under section 2(15) of the proposed ordinance.

## **OVERVIEW OF ACTIVITIES**

The Work Group met 22 times of the course of approximately 24 months from January 2018 through January 2020. Over the course of their meetings, they reviewed other cities' surveillance policies, surveyed and compiled an inventory of City agencies' surveillance technology and policies, heard presentations from several City agencies, and created a proposed surveillance technology acquisition and use ordinance.

The Work Group created a survey to collect information about City agencies' surveillance technology and distributed it to all of the City departments and divisions for completion. The 27-question survey (attached) covered a broad list of topics, including the types, amount, locations, and policies regulating City agencies' use of surveillance technology.

### ***Review of Peer Cities' Surveillance Policies***

The Work Group conducted a review of surveillance policies from four local governments: Seattle, WA, Santa Clara County, CA, Sommerville, MA, and Nashville, TN. These policies were analyzed focusing primarily on the following elements:

- Purchase approval processes
- Use policies and approval of those policies
- Policies related to data management
- Level of transparency, and public engagement
- Oversight processes
- Exemptions (law enforcement and other)
- Policy enforcement processes

### ***Findings of Work Group after Inventory and Department Presentations***

The Work Group found a lack of uniformity of practices and policies across departments regarding the purchase and use of surveillance technology. Currently, there is spotty oversight of what was purchased or how it is being used. There are currently no generally utilized training protocols for safeguarding the privacy of the general public against misuse of surveillance technology, and there are unclear and uneven accountability measures in the event of such misuse by a city employee. These findings reinforced the need to develop a comprehensive policy that applies to all city agencies in a uniform manner.

In the interest of transparency, the Work Group recommends that, with a few exceptions, surveillance technology purchased by City of Madison agencies be approved by the Common Council through public processes. Some of the details of those processes still need to be worked out, so the Work Group recommends that the CCEC work in consultation with the Mayor to finalize them as soon as possible.

The Work Group also recommends that the CCEC and the Mayor review the Madison Police Department's resident camera registration program. As the Work Group discussed the issue of posting notice to the general public about the presence of surveillance cameras, the topic of this program arose. The issue of whether information about the location of residents' cameras that have been registered with MPD to support its surveillance and crime investigation activities should be made public was not settled by the Work Group, but the Work Group agrees this is an issue of concern that should be taken up by the CCEC.

### ***Creation of Proposed Surveillance Technology Ordinance***

In drafting this ordinance, the Work Group initially included the terms “civil rights and civil liberties” and reference to Constitutional protections, such as protection from unreasonable search, freedom of association and freedom of speech, in multiple sections. After advice from the City Attorney’s Office, the Work Group struck that language and replaced it with the term “privacy interests” where the references to Constitutional rights had been.

The draft ordinance covers the acquisition of new surveillance technology, via city money, grant funds, or accepting donations of said technology. It also addresses entering into agreements with other entities to share surveillance technology or data. Additionally, the ordinance requires all City agencies to submit an annual report to the Common Council with specifically-designated information. The proposed ordinance contains sections on definitions, an approval process, a reporting process, and exemptions to the established processes.

#### *Definitions*

The proposed ordinance provides the following definitions (see attached draft ordinance for additional detail):

- **Surveillance:** Observation of a place, person, group, or ongoing activity in order to gather information;
- **Surveillance Data:** Any electronic data collected, captured, recorded, retained, processed, intercepted, analyze, or shared by surveillance technology;
- **Surveillance Technology:** Any hardware, software, electronic device, or system utilizing an electronic device, owned by the City or under contract with the City, designed, or primarily intended, to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory, or other personally identifiable information of members of the public for the purpose of surveillance;
- **Sensitive Surveillance Technology Information:** Any information about Surveillance Technology that public disclosure of would unreasonably expose or endanger City infrastructure; would adversely impact operations of City agencies; or may not be legally disclosed.

#### *Approval Process*

The proposed ordinance delineates an approval process for the acquisition of new, or substantive changes in the use of, surveillance technology. The Department’s request for Surveillance Technology will be approved only upon the determination that the benefits to the residents of the City outweigh the potential negative impact upon privacy interests and that, in the judgment of the Common Council, there is not an effective alternative with a lesser impact upon privacy interests nor is there an alternative with equivalent impact on privacy interests but with a lesser economic cost. The approval process for acquisition or contracting of new surveillance technology that will be part of

the citywide network enterprise system consists of referral to the Common Council either as part of the annual budget approval process or through a resolution. If the technology will not be connected to the citywide system, departments must notify the Mayor, Common Council leadership, and the information technology director, and post a notice to its website.

### *Exemptions*

The proposed ordinance lists the following four categories of exemption from the approval process outlined above:

- The surveillance technology is deemed to produce “sensitive surveillance technology information” as defined in the proposed ordinance;
- The technology is acquired through a federal property disposition program, and it is necessary to acquire it quickly. However, before installation or use, the agency must obtain approval;
- Acquisition of the surveillance technology is deemed to be needed to address an emergency “that poses an imminent and serious risk of death or substantial bodily harm”; and
- The acquisition is needed to implement a technical patch or upgrade. Prior to acquisition the acquiring department must consult with the IT department and include a description of the upgrade in the agency’s annual technology report.

### *Reporting Process*

The proposed ordinance also establishes an annual review process for all departmental surveillance technology. All City agencies “will complete an Annual Surveillance Technology Report which will be submitted to the Common Council.” The Annual Surveillance Technology Report will include an inventory of the agency’s surveillance technology, along with a narrative describing how the agency uses its surveillance technology, how it is being shared, how it is being protected, and how it is resolving any complaints it has received regarding its technology.

### ***Working with City Staff and Mayor’s Office on Corresponding Administrative Procedures Memorandum***

City staff, in particular IT Director Sarah Edgerton, Assistant City Attorney Marci Paulsen, and Assistant Chief of Police Vic Wahl, discussed with the Work Group the creation of an Administrative Procedures Memorandum intended to provide more detail about how City staff would comply with the proposed ordinance. The drafting of that APM is still underway. The same city staff provided ongoing recommendations and insights into preparation of the draft ordinance.

## **ATTACHMENTS**

Proposed Ordinance to Establish Surveillance Technology Guidelines for Departments

Resolution Establishing a President's Work Group to Develop City-Wide Surveillance Equipment and Data Management Policies (File # 49217)

Survey Questions with Answers

Spreadsheet of Departmental Surveillance Policies

City of Madison Camera System Inventory

Chart of Municipal Surveillance Policy Comparison

Ordinance (file #49284): Operating Security Cameras at Convenience Stores

APM 3-9: Appropriate Use of Computer Network Resources

APM 3-17: Use of Surveillance Cameras

ACLU Model Legislation

Final Report of the President's Work Group on Police and Community Relations

CITY OF MADISON, WISCONSIN

AN ORDINANCE \_\_\_\_\_

Creating Section 23.63 of the Madison General Ordinances to establish Surveillance Technology guidelines for Departments.

PRESENTED  
REFERRED

February 4, 2020  
CCEC, PSRC, EOC,  
Digital Tech. Committee

DRAFT

Drafted by: Marci Paulsen

Date: January 22, 2020

SPONSORS: Aids. Kemble, Baldeh, Carter

DRAFTER'S ANALYSIS: This ordinance requires all Departments to provide notification to the Mayor and Common Council before obtaining or using new surveillance technology. The ordinance requires all Departments to provide an annual report on its use of surveillance technology to the Common Council and public. The ordinance creates several exceptions for the approval process outlined within the ordinance, including when there is an emergency or when the surveillance technology involves information that must remain confidential. This ordinance establishes several definitions including surveillance data and surveillance technology.

\*\*\*\*\*

The Common Council of the City of Madison do hereby ordain as follows:

1. Section 23.63 entitled "Use of Surveillance Technology" of the Madison General Ordinances is created to read as follows:

**"23.63 USE OF SURVEILLANCE TECHNOLOGY.**

- (1) Intent and Purpose. City of Madison Departments have identified a wide variety of legitimate business reasons to use surveillance technology. The Common Council recognizes the need to carefully balance the need for surveillance for gathering data, public safety and the prosecution of crimes with the public's right to privacy. The Common Council desires to adopt a City-wide surveillance technology and surveillance data management policy that is consistent for all City Departments and covers all types of surveillance equipment usage and surveillance data management.

- (2) Definitions.
  - "City-wide Network" means the City's IT infrastructure which is connected using high speed fiber optic connections which allows City employees to share communications, software, hardware devices, and data and information.
  - "Information Technology Director" means the head of the City Information Technology Department.
  - "Department" means any agency, department, or division of the City.
  - "Sensitive Surveillance Technology Information" means any information about Surveillance Technology of which public disclosure would unreasonably expose or endanger City infrastructure; would adversely impact operations of City agencies; or may not be legally disclosed.
  - "Surveillance" means observation of a place, person, group, or ongoing activity in order to gather information.

Approved as to form:

“Surveillance Data” means any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by Surveillance Technology.

“Surveillance Technology” means any hardware, software, electronic device, or system utilizing an electronic device, owned by the City or under contract with the City, designed, or primarily intended, to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or other personally identifiable information of members of the public for the purpose of surveillance. Surveillance Technology includes but is not limited to the following: cell site simulators; automatic license plate readers; gunshot detection systems; facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed; and unmanned aircraft systems equipped with remote video capabilities. Surveillance Technology does not include the following devices:

1. Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers;
2. Audio/video teleconference systems;
3. City databases and enterprise systems that contain information, including, but not limited to, human resource, permit, license and business records;
4. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases;
5. Information technology security systems, including firewalls and other cybersecurity systems;
6. Systems or databases that capture information where an individual knowingly and voluntarily consented to provide the information, such as applying for a permit, license or reporting an issue;
7. Physical access control systems, employee identification management systems, and other physical control systems;
8. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, or water or sewer functions;
9. Manually-operated technological devices used primarily for internal City and Department communications and are not designed to surreptitiously collect surveillance data, such as radios, cell phones, personal communication devices and email systems;
10. Manually-operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designed to be used surreptitiously and whose function is limited to manually capturing and manually downloading video and/or audio recordings;
11. Devices that cannot record or transmit audio or video or electronic data or be remotely accessed, such as vision-stabilizing binoculars or night vision goggles;
12. Computers, software, hardware or devices used in monitoring the work and work-related activities involving City buildings, employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
13. Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the course of providing City services;
14. Parking Ticket Devices;
15. Equipment used on a temporary basis during active investigations and in accordance with City policies;
16. Cameras intended to record activities at City facilities in nonpublic areas;
17. Police Department interview rooms, holding cells, and Police Department internal security audio/video recording systems;
18. Police Department records/case management systems, digital fingerprinting systems, Computer Aided Dispatch (CAD); and
19. Fire Department equipment and technology used for Emergency Medical Services, Hazardous Material, Lake Rescue and Heavy Urban Rescue, such as tunneling cameras, sonar, and thermal imaging.

- (3) Applicability. This ordinance applies to all Departments that do any of the following:
- (a) Currently uses or has access to any Surveillance Technology
  - (b) Seeks funds for new Surveillance Technology including applying for or accepting grants, state or federal funds or other donations;
  - (c) Acquires new Surveillance Technology, with or without a cost;
  - (d) Enters into a contract or agreement with any other entity to share Surveillance Technology or Surveillance Data; and
  - (e) Changes the use of existing surveillance technology for a purpose substantially different than originally approved.
- (4) Approval Process. Within ninety (90) days of adoption of this ordinance, all Departments must comply with this section prior to any use of new Surveillance Technology or any substantial change of use of existing Surveillance Technology.
- (a) All Department requests to purchase, acquire or contract for the use of new Surveillance Technology or substantially change the use of existing Surveillance Technology that will connect to the City-wide Network will be referred to the Common Council via the budget process or through a resolution. The resolution or budget request will include at least the following information:
    - 1. The circumstances which necessitate the use of the Surveillance Technology;
    - 2. The training protocols on Surveillance Technology use, including access to data and images, the Department will utilize;
    - 3. The staff position responsible for the account management and administration of the Surveillance Technology;
    - 4. The staff position responsible for receiving complaints regarding the Department's use of Surveillance Technology;
    - 5. The process for determining staff roles and access to Surveillance Technology;
    - 6. The process to ensure access to Surveillance Technology is revoked when the employee no longer has a job related need to said access;
    - 7. The personnel responsible for training staff and reviewing staff access and use of the Surveillance Technology;
    - 8. The process for providing the Madison Police Department with immediate access to all data recordings that may constitute evidence of a crime, unless otherwise prohibited by law;
    - 9. The time period that recorded audio and video will be retained, in accordance with the Department's record retention policy;
    - 10. The prohibition of using Surveillance Technology to visually or audibly monitor the interior of private dwellings where a reasonable expectation of privacy exists, absent a court order or other lawful justification; and
    - 11. Procedures for ensuring that records are not destroyed during the pendency of any public records request, investigation or civil or criminal litigation.
  - (b) The Department's request for Surveillance Technology will be approved only upon the determination that the benefits to the community members and residents of the City outweigh the potential privacy interests and that, in the judgment of the Common Council, there is not an effective alternative with a lesser impact upon privacy interests nor is there an alternative with equivalent impact on privacy interests but with a lesser economic cost.
  - (c) As part of the annual budget request, all Departments will notify the Information Technology Director, the Mayor and Common Council leadership of any request to purchase, acquire or contract for the use of new Surveillance Technology that is not connected to the City-wide Network. The Department will post on the Department's website notice to the public of its intent to obtain or use new Surveillance Technology. If the Mayor or Common Council leadership request that a Department notify residents, the Department will work with IT to create a process for residents to

submit feedback and comments. The Department will hold a public meeting if requested by the Mayor or Common Council Leadership.

- (d) If a Department needs to move a camera location on the City-wide enterprise camera system, or activates new functions not previously approved, or adds a new camera of a previously-approved type, the Department will notify the Mayor and Common Council Leadership and the Alder(s) of the affected district(s). The Mayor, Common Council Leadership, or Alder(s) of the affected district(s) will coordinate with the Department to notify the residents, including creating a variety of notification and outreach mechanisms for residents to submit feedback and comments. The Department will hold a public meeting if requested by the Mayor, Common Council Leadership, or the Alder of the district where the camera is located.

(5) Reporting Process.

- (a) Each Department will conduct an annual review of its Surveillance Technology and ensure compliance with this ordinance.
- (b) Each Department will complete an Annual Surveillance Technology Report which will be submitted to the Common Council through a resolution. The Annual Surveillance Technology Report will include:
  1. An inventory of current Surveillance Technology and the applicable policies;
  2. How the Department has used the data collected by its Surveillance Technology;
  3. How any Surveillance Data is being shared with other entities;
  4. How well Surveillance Data management protocols are safeguarding individual information; and
  5. Whether the Department has received any complaints or concerns about its Surveillance Technology use and the resolution of said complaints.
- (c) The Common Council shall review and take action on the resolution accompanying the Annual Surveillance Technology Report.

(6) Exceptions. This ordinance does not apply to the following:

- (a) Federal Property Disposition Programs. If the Surveillance Technology is available through federal property disposition programs and/or the purchase or acquisition decision must be executed quickly, such acquisition may be made. However, if the Surveillance Technology is obtained under this subdivision, the Department must apply for approval as described in subsection (4) within thirty (30) days and before installation or use of said equipment.
- (b) Emergency Situations. In the event of an emergency, that poses an imminent and serious risk of death or substantial bodily harm, a Department may acquire Surveillance Technology without prior Common Council approval, for the sole purpose of preventing or mitigating such risk, if the Department reasonably believes the acquisition of such Surveillance Technology will result in reduction of said risk. The Department's use of the Surveillance Technology must cease when such risk no longer exists or the use of the Surveillance Technology can no longer reasonably reduce the risk. The Department shall apply for approval of the Surveillance Technology per subsection (4) of this ordinance within thirty (30) days of cessation of the risk that prompted purchase of said Technology. The use of the Surveillance Technology must be documented in the Department's Annual Surveillance Technology Report.
- (c) Technical Patch or Upgrade. A Department, in consultation with the City Information Technology Department, may apply a technical patch or upgrade that is necessary to mitigate threats to the City's infrastructure, even if the patch or upgrade materially alters the surveillance capabilities of the technology. However, if such patch or upgrade does materially alter the surveillance capability of the technology, it must be highlighted in the Annual Surveillance Technology Report.
- (d) Sensitive Surveillance Technology Information. Sensitive Surveillance Technology Information is exempt from the requirements in the ordinance. Departments will provide the basis for exemption to the Information Technology Director. The Information Technology Director will notify the Mayor and Common Council Leadership of the exemption for mayoral approval."



Legislation Details (With Text)

**File #:** 49217      **Version:** 1      **Name:** Establishing a President's Work Group to Develop City-Wide Surveillance Equipment and Data Management Policies.

**Type:** Resolution      **Status:** Passed

**File created:** 10/13/2017      **In control:** COMMON COUNCIL EXECUTIVE COMMITTEE

**On agenda:** 12/5/2017      **Final action:** 12/5/2017

**Enactment date:** 12/11/2017      **Enactment #:** RES-17-00937

**Title:** Establishing a President's Work Group to Develop City-Wide Surveillance Equipment and Data Management Policies.

**Sponsors:** Marsha A. Rummel, Rebecca Kemble

**Indexes:**

**Code sections:**

**Attachments:**

Date	Ver.	Action By	Action	Result
12/5/2017	1	COMMON COUNCIL	Adopt	Pass
11/21/2017	1	COMMON COUNCIL EXECUTIVE COMMITTEE	RECOMMEND TO COUNCIL TO ADOPT - REPORT OF OFFICER	Pass
10/17/2017	1	COMMON COUNCIL	Refer	Pass
10/13/2017	1	Council Office	Referred for Introduction	

No appropriations required.

Establishing a President's Work Group to Develop City-Wide Surveillance Equipment and Data Management Policies.

WHEREAS, the City of Madison has an interest in ensuring that all official surveillance activities carefully safeguard privacy and confidentiality for residents and visitors, while ensuring safety and security for the public; and,

WHEREAS, the City of Madison video surveillance is governed by APM 3-17 regarding Use of Surveillance Cameras; and,

WHEREAS, APM 3-17 requires all department heads to develop their policies in partnership with Information Technology and to file those policies with the City Clerk's Office; and,

WHEREAS, the Madison Police Department has various Standard Operating Procedure policies which address surveillance; and,

WHEREAS, there are surveillance technologies which are not governed by existing policies; and,

WHEREAS, the City of Madison has an interest in a city-wide surveillance and data management policy that is consistent for all City agencies and covers all type of surveillance equipment usage and data management; and,

WHEREAS, The President's Work Group on Police and Community Relations Recommendations and Report, adopted in May 2017 called for the Common Council to develop a city-wide policy for the purchase, use and

management of data related to surveillance equipment,

NOW THEREFORE IT BE RESOLVED, that the Common Council of the City of Madison establish a President's Work Group to develop a policy governing the purchase and use of all surveillance equipment employed by all City agencies and the surveillance policy will address data management and storage; and,

BE IT FURTHER RESOLVED, the Work Group will be staffed by Common Council staff and will seek expert opinions from a variety of departments; and,

BE IT FURTHER RESOLVED, that the Work Group will use a racial equity and social justice lens throughout its work and may access training to apply the City of Madison Racial Equity and Social Justice Impact Tool; and,

BE IT FURTHER RESOLVED, that the Work Group will begin work upon adoption of this resolution with a goal of completing the surveillance policy by June 2018; and,

BE IT FURTHER RESOLVED, that the Common Council will develop this policy in consultation with City of Madison staff and officials, including but not limited to Information Technology, the City Attorney and all Departments or Divisions that currently use or plan to utilize any kind of surveillance equipment; and,

BE IT FINALLY RESOLVED, that the policy will include an inventory of all City of Madison surveillance equipment as of December 2017 and the surveillance equipment inventory will be updated annually thereafter.

#1

COMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 11:34:46 AM  
**Last Modified:** Wednesday, May 02, 2018 11:39:23 AM  
**Time Spent:** 00:04:36  
**IP Address:** 204.147.0.15

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Harper Donahue

---

**Q2** Please enter the name of your City agency.

Human Resources

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

I did not indicate this...

---

**Q4** What is the purpose of the surveillance technology?

No surveillance technology

---

**Q5** How is the technology utilized?

No surveillance technology

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No surveillance technology

---

**Q9** How many pieces of this type of technology does your agency own?

No surveillance technology

---

**Q10** Please indicate whether the technology is mobile or stationary. Other (please specify):  
No surveillance technology

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

No surveillance technology

---

**Q12** What factors determine where the surveillance technology is used?

No surveillance technology

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

No surveillance technology

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

No surveillance technology

---

### Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

No surveillance technology

---

**Q18** Which positions in your agency are authorized to access the data?

No surveillance technology

---

**Q19** For what reason do the authorized positions have access to the data?

No surveillance technology

---

**Q20** Other than the positions authorized to access the data, who has access?

No surveillance technology

---

**Q21** How long is the data stored?

No surveillance technology

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

No surveillance technology

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

No surveillance technology

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

No surveillance technology

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #2

**INCOMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 11:49:20 AM  
**Last Modified:** Wednesday, May 02, 2018 11:50:28 AM  
**Time Spent:** 00:01:08  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Mark Hanson

---

**Q2** Please enter the name of your City agency.

Assessor

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology. **Respondent skipped this question**

---

**Q4** What is the purpose of the surveillance technology? **Respondent skipped this question**

---

**Q5** How is the technology utilized? **Respondent skipped this question**

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Respondent skipped this question**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized. **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q9** How many pieces of this type of technology does your agency own? **Respondent skipped this question**

---

**Q10** Please indicate whether the technology is mobile or stationary. **Respondent skipped this question**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.) **Respondent skipped this question**

---

**Q12** What factors determine where the surveillance technology is used? **Respondent skipped this question**

---

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Respondent skipped this question**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment? **Respondent skipped this question**

---

**Q16** How does your agency control unauthorized use of the surveillance equipment? **Respondent skipped this question**

---

---

### Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored? **Respondent skipped this question**

---

**Q18** Which positions in your agency are authorized to access the data? **Respondent skipped this question**

---

**Q19** For what reason do the authorized positions have access to the data? **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q20** Other than the positions authorized to access the data, who has access? Respondent skipped this question

---

**Q21** How long is the data stored? Respondent skipped this question

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic. Respondent skipped this question

---

---

### Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? Respondent skipped this question

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. Respondent skipped this question

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. Respondent skipped this question

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. Respondent skipped this question

---

**Q27** Were you unable to completely answer any of the questions in the survey? Respondent skipped this question

---

# #3

**INCOMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 1:14:04 PM  
**Last Modified:** Wednesday, May 02, 2018 1:14:38 PM  
**Time Spent:** 00:00:33  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Maribeth Witzel-Behl

---

**Q2** Please enter the name of your City agency.

City Clerk's Office

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology. **Respondent skipped this question**

---

**Q4** What is the purpose of the surveillance technology? **Respondent skipped this question**

---

**Q5** How is the technology utilized? **Respondent skipped this question**

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Respondent skipped this question**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized. **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q9** How many pieces of this type of technology does your agency own? **Respondent skipped this question**

---

**Q10** Please indicate whether the technology is mobile or stationary. **Respondent skipped this question**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.) **Respondent skipped this question**

---

**Q12** What factors determine where the surveillance technology is used? **Respondent skipped this question**

---

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Respondent skipped this question**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment? **Respondent skipped this question**

---

**Q16** How does your agency control unauthorized use of the surveillance equipment? **Respondent skipped this question**

---

---

### Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored? **Respondent skipped this question**

---

**Q18** Which positions in your agency are authorized to access the data? **Respondent skipped this question**

---

**Q19** For what reason do the authorized positions have access to the data? **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q20** Other than the positions authorized to access the data, who has access?

Respondent skipped this question

---

**Q21** How long is the data stored?

Respondent skipped this question

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Respondent skipped this question

---

---

### Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency?

Respondent skipped this question

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Respondent skipped this question

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

Respondent skipped this question

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

Respondent skipped this question

---

**Q27** Were you unable to completely answer any of the questions in the survey?

Respondent skipped this question

---

# #4

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 2:33:14 PM  
**Last Modified:** Wednesday, May 02, 2018 2:47:35 PM  
**Time Spent:** 00:14:21  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

David Gawenda

---

**Q2** Please enter the name of your City agency.

City Treasurer

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Cameras placed in our ceiling focused on the inside and lobby area of the office.

---

**Q4** What is the purpose of the surveillance technology?

To capture interactions with citizens in case of robbery. Also, the video can be used to review staff/citizen interactions on the occasion of complaints.

---

**Q5** How is the technology utilized?

It is only accessed in case of need. Access is via PC.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

I do not believe our cameras are capable of audio (although they may be, and I am unaware of it.)

---

**Q9** How many pieces of this type of technology does your agency own?

Eight cameras.

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

NA

---

**Q12** What factors determine where the surveillance technology is used?

NA

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

City IT. I believe City IT is considered the owner.

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

City Treasurer.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

The city treasurer is the only individual who can access the video.

---

Page 5: Surveillance Technology Survey Part 2 Continued

Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

city servers.

---

**Q18** Which positions in your agency are authorized to access the data?

City Treasurer.

---

**Q19** For what reason do the authorized positions have access to the data?

As above. (In the event of robbery or citizen complaints.)

---

**Q20** Other than the positions authorized to access the data, who has access?

no one

---

**Q21** How long is the data stored?

I do know; IT controls that.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

See answer #21.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Sign posted on our bulletin board.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

NA

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey?

**Respondent skipped this question**

---

# #5

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 3:58:29 PM  
**Last Modified:** Wednesday, May 02, 2018 4:20:58 PM  
**Time Spent:** 00:22:29  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Chuck Kamp

---

**Q2** Please enter the name of your City agency.

Metro Transit

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Cameras on buses, at our bus facilities, at our transfer points, automated vehicle locator systems that track where a bus is at a certain point, which can be helpful for safety or security reasons, and a farebox system with features a tracking system that has been used to address safety and security issues.

---

**Q4** What is the purpose of the surveillance technology?

To try to achieve the highest levels of safety and security, consistent with guidance we get from other transit systems, our transit insurance company, the police department, and the national TSA.

---

**Q5** How is the technology utilized?

Address customer complaints more accurately, evaluate accidents more thoroughly, help the police with criminal activities at any of our facilities, assist the school district with security issues on our buses that serve MMSD, assist with non-Metro related issues such as criminal cases where a person used the bus on or about the time of the crime, and we can assist sometimes in those cases.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

3-17.pdf (27.2KB)

---

Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

I believe we use audio if we have deemed it appropriate, but not all cameras have audio. The AVL and fareboxes, of course, do not have audio.

---

**Q9** How many pieces of this type of technology does your agency own?

Several hundred.

---

**Q10** Please indicate whether the technology is mobile or stationary.

Other (please specify):

Both - cameras on buses move around, and cameras at facilities are stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

On buses that serve throughout the city (see route map).

---

**Q12** What factors determine where the surveillance technology is used?

A security incident that requires an investigation.

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology?

Yes

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

The police and the school district can access a file sharing system to allow quick access to address security or safety issues.

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Specific supervisors and managers, but not all. They need to have a job-specific reason, such as the supervisor who responds to security incidents that require follow-up, or the Metro IT manager who is often needed to assist with that.

---

## Surveillance Technology Survey - Part 2

**Q16** How does your agency control unauthorized use of the surveillance equipment?

We monitor it by responding to incidents where an unauthorized person used or shared surveillance equipment, and where necessary, discipline may apply.

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

On servers at Metro and at the City IT Dept.

---

**Q18** Which positions in your agency are authorized to access the data?

Specific supervisor and manager positions who have job specific reasons, such as the safety supervisor or our IT manager.

---

**Q19** For what reason do the authorized positions have access to the data?

To address safety and security incidents.

---

**Q20** Other than the positions authorized to access the data, who has access?

No one.

---

**Q21** How long is the data stored?

Each security system has a different level of data storage capability.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

With cameras, the data is overwritten if not accessed, and with downloaded data, we follow the city policy.

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

We let bus customers and employees know by posting information on the buses and at facilities.

---

## Surveillance Technology Survey - Part 2

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. **Respondent skipped this question**

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #6

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 3:57:14 PM  
**Last Modified:** Wednesday, May 02, 2018 4:22:11 PM  
**Time Spent:** 00:24:56  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Charlie Romines

---

**Q2** Please enter the name of your City agency.

Streets

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Cameras that oversee the three public drop off locations as well as oversee the Streets Division work locations, Badger, Sycamore, Transfer Station and South Point

---

**Q4** What is the purpose of the surveillance technology?

Monitor public use of the drop off locations\ discourage illegal dumping. Further serves as a deterrent to breakins of our outside equipment as well as facilities. Cameras in shop areas are primarily used to monitor equipment location but also employee actions.

---

**Q5** How is the technology utilized?

I hope I answered this above.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No, video only

---

**Q9** How many pieces of this type of technology does your agency own?

31 cameras

---

**Q10** Please indicate whether the technology is mobile or stationary.

**Mobile,**  
Other (please  
specify):  
Most cameras will rotate but are not otherwise  
mobile

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

**Respondent skipped this question**

---

**Q12** What factors determine where the surveillance technology is used?

**Respondent skipped this question**

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology?

**No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

**Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Comp Group 18 (Supervisory) employees have varying degrees of access to cameras.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Access is limited by individual log on. So unless someone comes to know a managers log on they can not access the surveillance cameras

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

Cameras can only store the last 15 minutes of video that anyone with access can reach

---

**Q18** Which positions in your agency are authorized to access the data?

Supervisors only for the 15 min option. Supt and Asst Supt have access to go back several months thru the system.

---

**Q19** For what reason do the authorized positions have access to the data?

Investigations of an internal and external nature, identify vandalism, illegal dumping, break ins. Also quickly verify where a specific piece of equipment is located. During snow events helps to identify where employees and equipment are located, activity occurring. Access to traffic cameras very helpful in auto accident reviews as well as monitoring winter road conditions.

---

**Q20** Other than the positions authorized to access the data, who has access?

No one.

---

**Q21** How long is the data stored?

Camera info can be accessed for several months retroactively by Supt and Asst Supt.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Process is automatic and is outside Streets pervue.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Signs are placed in any areas where the public may be on our cameras, ie Drop off sites.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

---

**Respondent skipped this question**

**Q27** Were you unable to completely answer any of the questions in the survey?

---

**No**

#7

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Wednesday, May 02, 2018 1:17:30 PM  
**Last Modified:** Wednesday, May 02, 2018 4:35:11 PM  
**Time Spent:** 03:17:40  
**IP Address:** 204.147.0.15

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Finance Department

---

**Q2** Please enter the name of your City agency.

David Schmiedicke

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Cameras and audio at two access doors to the department work areas.

---

**Q4** What is the purpose of the surveillance technology?

To identify and communicate with individuals other than department employees needing to gain access to the department work spaces.

---

**Q5** How is the technology utilized?

Staff can view the doorways on their screens and allow access through the doorways.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**Finance Dept Video Surveillance Policy 20171031.docx (20.9KB)**

---

Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

Please contact IT for that information.

---

**Q9** How many pieces of this type of technology does your agency own?

Two cameras and audio.

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

At the doorways that access work areas of the department.

---

**Q12** What factors determine where the surveillance technology is used?

Identification of individuals and ability to communicate with them.

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

Information Technology

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Payroll, Document Services, Reception

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

The cameras are fixed at the entrances and used for facial recognition only.

---

### Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

IT maintains the storage.

---

**Q18** Which positions in your agency are authorized to access the data?

Explained earlier

---

**Q19** For what reason do the authorized positions have access to the data?

Explained earlier.

---

**Q20** Other than the positions authorized to access the data, who has access?

City Risk Manager

---

**Q21** How long is the data stored?

IT maintains the storage.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

IT maintains the storage.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Signage at the entrances.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. **Respondent skipped this question**

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #8

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, May 15, 2018 11:42:23 AM  
**Last Modified:** Tuesday, May 15, 2018 4:24:58 PM  
**Time Spent:** 04:42:34  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Connie Thompson

---

**Q2** Please enter the name of your City agency.

Monona Terrace

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

We have cameras and monitors.

---

**Q4** What is the purpose of the surveillance technology?

To protect the building, employees and event attendees from active shooting incidents and other unsafe behavior or potential criminal activity.

---

**Q5** How is the technology utilized?

We have a Command Center Operator who monitors the docks, main entrances and hallways. They can use the camera's to check on disturbances, or other incidents that occur throughout the day.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**CCTV building Policy Final (2).pdf (45KB)**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No.

---

**Q9** How many pieces of this type of technology does your agency own?

Not sure.

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

In general the cameras cover all inside and outside areas except offices, restrooms, locker rooms, break rooms, mechanical rooms, and stairwells.

---

**Q12** What factors determine where the surveillance technology is used?

Advice of Homeland Security.

---

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

MPD can request and be granted access.

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Command Center Operators, Operations Managers, Associate Director of Operations, Executive Director

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

The system is password protected

---

---

Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

In an IT server.

---

**Q18** Which positions in your agency are authorized to access the data?

Executive Director, Associate Director, Operations Managers, IT Specialist, Command Center Operators.

---

**Q19** For what reason do the authorized positions have access to the data?

To view real time camera images, to review recorded images. Also for use in criminal cases and customer/event issues.

---

**Q20** Other than the positions authorized to access the data, who has access?

IT administrators.

---

**Q21** How long is the data stored?

It varies on storage room and activity. 2 weeks to 1 month.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

It is recorded over. This is automatic.

---

---

### Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. **Respondent skipped this question**

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

We do not inform visitors and guests of surveillance technology. Cameras are only used for monitoring the safety of individuals, property and facility. For monitoring of any activity or behavior that seems out of the ordinary. And to investigate criminal activity. Images are recorded over within 2 - 4 weeks.

---

## Surveillance Technology Survey - Part 2

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

---

**Respondent skipped this question**

**Q27** Were you unable to completely answer any of the questions in the survey?

---

**No**

#9

COMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Friday, May 18, 2018 11:18:08 AM  
**Last Modified:** Friday, May 18, 2018 11:40:35 AM  
**Time Spent:** 00:22:27  
**IP Address:** 204.147.2.12

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Krissy Wick

---

**Q2** Please enter the name of your City agency.

Library

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

We have IP cameras that are connected to the City of Madison IT department's server at some (3 currently) of our libraries. As locations are renovated/updated/built new, we anticipate adding surveillance technology.

---

**Q4** What is the purpose of the surveillance technology?

The Library uses surveillance technology to assist in identifying individuals who participate in negative behavior, threaten staff or public safety, or otherwise engage in dangerous or criminal activity.

---

**Q5** How is the technology utilized?

The cameras run 24/7 with City IT storing the images. If an incident occurs, we then go back and take any relevant information from the cameras.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

Yes. We think that all of our cameras are able to record sound, but City IT is not utilizing this.

---

**Q9** How many pieces of this type of technology does your agency own?

21

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Central Library, Goodman South Madison Library, Meadowridge Library

---

**Q12** What factors determine where the surveillance technology is used?

We put them in high traffic public areas, such as entry and exit points, and in locations that are not easily seen by staff.

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Branch Supervisors (at branches that have cameras), Library Security Staff at Central Library, Library and City IT

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

We are not aware of any unauthorized use.

---

### Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

City IT server

---

**Q18** Which positions in your agency are authorized to access the data?

Branch Supervisors (at branches with cameras), Library Security at Central Library, Library and City IT

---

**Q19** For what reason do the authorized positions have access to the data?

After an incident, authorized staff captures the information and releases it to any approved requestor (City Attorney and Police).

---

**Q20** Other than the positions authorized to access the data, who has access?

No one that we are aware of.

---

**Q21** How long is the data stored?

We don't know. It is controlled by City IT.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Again, we are not sure. We believe it is deleted after it's no longer needed.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. **Respondent skipped this question**

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

We are not aware of any legal obligation to inform residents about the use of surveillance technology.

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #10

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Friday, May 18, 2018 2:53:21 PM  
**Last Modified:** Friday, May 18, 2018 2:53:36 PM  
**Time Spent:** 00:00:15  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Norman Davis

---

**Q2** Please enter the name of your City agency.

Civil Rights

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology. **Respondent skipped this question**

---

**Q4** What is the purpose of the surveillance technology? **Respondent skipped this question**

---

**Q5** How is the technology utilized? **Respondent skipped this question**

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Respondent skipped this question**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized. **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q9** How many pieces of this type of technology does your agency own? **Respondent skipped this question**

---

**Q10** Please indicate whether the technology is mobile or stationary. **Respondent skipped this question**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.) **Respondent skipped this question**

---

**Q12** What factors determine where the surveillance technology is used? **Respondent skipped this question**

---

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Respondent skipped this question**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment? **Respondent skipped this question**

---

**Q16** How does your agency control unauthorized use of the surveillance equipment? **Respondent skipped this question**

---

---

### Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored? **Respondent skipped this question**

---

**Q18** Which positions in your agency are authorized to access the data? **Respondent skipped this question**

---

**Q19** For what reason do the authorized positions have access to the data? **Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q20** Other than the positions authorized to access the data, who has access? **Respondent skipped this question**

---

**Q21** How long is the data stored? **Respondent skipped this question**

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic. **Respondent skipped this question**

---

---

### Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Respondent skipped this question**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. **Respondent skipped this question**

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. **Respondent skipped this question**

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **Respondent skipped this question**

---

#11

COMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 10:11:55 AM  
**Last Modified:** Tuesday, June 19, 2018 10:26:09 AM  
**Time Spent:** 00:14:14  
**IP Address:** 204.147.0.15

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

In-car video systems in marked squads and certain unmarked squads.

---

**Q4** What is the purpose of the surveillance technology?

In-car video has been utilized by MPD for 15+ years. It is intended to serve a variety of purposes; the most significant is to capture evidence for use in a prosecution (this can include driving behavior, field sobriety tests, etc.). In-car video is also used to help investigate citizen complaints about officer behavior, to audit officer driving habits, etc.

---

**Q5** How is the technology utilized?

The system consists of one camera that faces forward and one internal camera facing the back seat of the vehicle. Officers also wear a portable microphone that is connected to the system and transmits audio.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**InCarVideo.pdf (96.5KB)**

---

Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

146

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

The cameras go wherever the vehicles go; and the microphone goes where the officer goes.

---

**Q12** What factors determine where the surveillance technology is used?

Wherever MPD officers are requested/deployed.

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

Another agency can request a particular video, but no other agency (with the exception of the City Attorney's Office) has immediate access to the data server. All data is subject to request and potential release under the public records law. The City Attorney's Office can review video that has been specifically designated for them to review.

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

All sworn personnel who operate vehicles equipped with in-car video.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

The system has an audit log to document any video review.

---

Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

All data from the video is stored on a dedicated MPD server. Video designated as evidence is stored on a separate server. A working copy may also be stored in the MPD evidence/property system (on a DVD or other type of storage).

---

**Q18** Which positions in your agency are authorized to access the data?

All sworn personnel are authorized to review their own videos. Sworn personnel at the rank of detective or higher are authorized to review video that has not been designated as restricted. Restricted video is only viewable by select MPD technology personnel, FSU personnel and executive personnel.

---

**Q19** For what reason do the authorized positions have access to the data?

To assist with investigations, for report writing, to review personnel complaints, for audit purposes, etc.

---

**Q20** Other than the positions authorized to access the data, who has access?

No one

---

**Q21** How long is the data stored?

General video is kept for 180 days, consistent with the City's records retention schedule. Video designated as evidence is retained as long as is needed for the case.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Video on the server is automatically removed after the retention period has passed. Video that has been designated as evidence goes through a review process to ensure that all relevant court proceedings have been completed.

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

MPD was very public when in-car video was first deployed 15+ years ago. Subsequent purchases of updated systems have been part of the City budget process. In-car video is regularly released and used publicly (by media and others); it seems well-known that MPD squads may be equipped with in-car video.

---

## Surveillance Technology Survey - Part 2

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

n/a

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey?

**No**

---

# #12

COMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 10:26:10 AM  
**Last Modified:** Tuesday, June 19, 2018 10:31:27 AM  
**Time Spent:** 00:05:17  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Auto-chalk system

---

**Q4** What is the purpose of the surveillance technology?

Auto-chalk is used by MPD parking enforcement officers to more efficiently enforce non-metered, time restricted parking violations.

---

**Q5** How is the technology utilized?

The vehicles with the auto-chalk system drive through areas with time-restricted parking regulations (1 or 2 hour). The system captures photos of each vehicle (to include wheel position, shape of the vehicle, and the license plate). After the applicable time period has passed, the vehicle will drive through the area again, and the system will take a second sequence of photos, and compare them with the first pass. If there is a match – indicating that the vehicle has been present for the designated period – an alert notifies the PEO. At that time the PEO will issue the appropriate citation. The system will store the photo/data for violations; however, photos/data captured during the first pass are not retained. For violations, the system stores the photos that were taken along with some additional data (time, location). The license plate is also stored, but the system does not integrate with DOT/CIB (so the vehicle registration info is not imported into the system).

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

## Surveillance Technology Survey - Part 2

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

### Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

The system has limited functionality as a license plate reader system. Specific license plates can be entered into the system will alert if one of the plates is detected. If this is activated, then the auto-chalk enforcement capability described above is not functional. The system does not store plates that are detected if used in this manner, and it does not integrate with DOT/CIB. Only manually entered plates can be searched for. This has been used occasionally to look for specific vehicles (like "scofflaw" parking violator vehicles), but it is not used routinely.

---

**Q9** How many pieces of this type of technology does your agency own?

2

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Throughout the City (where time-limited parking restrictions are in effect).

---

**Q12** What factors determine where the surveillance technology is used?

Areas that have 1 or 2 hour parking restrictions.

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Parking enforcement officers

---

## Surveillance Technology Survey - Part 2

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Only limited personnel have access

---

### Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

A dedicated server

---

**Q18** Which positions in your agency are authorized to access the data?

The parking enforcement supervisor and parking/traffic administrative assistant.

---

**Q19** For what reason do the authorized positions have access to the data?

To obtain photo evidence for parking citations that are contested and/or taken to court.

---

**Q20** Other than the positions authorized to access the data, who has access?

MPD Technology personnel

---

**Q21** How long is the data stored?

Data for violations/citations have been retained since the technology was first deployed. Photos/data that do not alert or result in citations are not retained. We are in the process of setting up the software to purge data after 7 years.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Will be automatically purged

---

### Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

The auto-chalk system was fairly well-publicized when first deployed, and the vehicles with these devices are very obvious.

---

## Surveillance Technology Survey - Part 2

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

n/a

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey?

**No**

---

# #13

COMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 10:31:27 AM  
**Last Modified:** Tuesday, June 19, 2018 10:46:37 AM  
**Time Spent:** 00:15:09  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

SWAT Body Cameras

---

**Q4** What is the purpose of the surveillance technology?

These are small cameras used by SWAT team members during tactical operations. They can be used to resolve citizen complaints, provide documentation for use-of-force encounters, assist with prosecution, etc. Video is also used as a training aid.

---

**Q5** How is the technology utilized?

During pre-planned tactical operations (like the execution of search warrants), specific officers are assigned to wear cameras. There are not enough cameras to assign one to each officer, so they are assigned with the goal of providing as much coverage of the operation as possible. After the incident, supervisors download the video. The cameras are also deployed when possible for spontaneous tactical incidents, but there will be a delay in their arrival at a scene (and sometimes it is not practical to deploy them).

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

SWATBodyWornCameras.pdf (94.1KB)

---

Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

We currently have about 15 older, consumer-grade cameras that are being used in this capacity. We are in the process of transitioning to body worn cameras that are designed for police use and integrated into the same infrastructure as our in-car video systems. We have 10 of those newer cameras that will be utilized for this purpose. The older cameras may be retained for back-up purposes.

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

On SWAT officers for tactical operations.

---

**Q12** What factors determine where the surveillance technology is used?

Wherever the SWAT operation takes place

---

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

SWAT officers

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

The cameras are not accessible to non-SWAT personnel.

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

All data from the video is stored on a dedicated MPD server (the same server used for in-car video). Video designated as evidence is stored on a separate server; a working copy may also be stored in the MPD evidence/property system (on a DVD or other storage).

---

**Q18** Which positions in your agency are authorized to access the data?

All sworn personnel are authorized to review their own videos. Sworn personnel at the rank of detective or higher are authorized to review video that has not been designated as restricted. Restricted video is only reviewable by select MPD Technology personnel, FSU personnel and executive personnel.

---

**Q19** For what reason do the authorized positions have access to the data?

To review an incident, to assist in report writing, to prepare for court, for training, etc.

---

**Q20** Other than the positions authorized to access the data, who has access?

n/a

---

**Q21** How long is the data stored?

General video is kept for 180 days; consistent with the City's records retention schedule. Video designated as evidence is retained as long as is needed for the case.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Video on the server is automatically removed after the retention period has passed. Video that has been designated as evidence will go through a review process to ensure that the relevant court proceedings have completed.

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Body cameras have been deployed with SWAT personnel for at least 7 years. We have been very public in discussing this, and the SOP is available on MPD's website.

---

## Surveillance Technology Survey - Part 2

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

n/a

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey?

**No**

---

# #14

COMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 10:46:37 AM  
**Last Modified:** Tuesday, June 19, 2018 10:55:30 AM  
**Time Spent:** 00:08:53  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Small Unmanned Aircraft Systems (sUAS or UAS)

---

**Q4** What is the purpose of the surveillance technology?

The UAS provides assistance to officers in a variety of contexts: search and rescue, crime scene processing, major events, etc.

---

**Q5** How is the technology utilized?

Officers investigating an incident where a UAS would be beneficial can request that the UAS team respond. The UAS provides real-time video which enables officers to check large open areas much more quickly than they could on foot.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**UnmannedAircraftSystems.pdf (102.5KB)**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

2

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Wherever the incident/event is located.

---

**Q12** What factors determine where the surveillance technology is used?

Wherever the incident/event is located.

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

There is a small UAS team who are the only ones authorized to access/utilize the devices.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

UAS team members are the only ones who are permitted to utilize the aircraft.

---

### Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

Same as in-car video.

---

**Q18** Which positions in your agency are authorized to access the data?

Same as in-car video

---

**Q19** For what reason do the authorized positions have access to the data?

Same as in-car video

---

**Q20** Other than the positions authorized to access the data, who has access?

n/a

---

**Q21** How long is the data stored?

Same as in-car video

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Same as in-car video

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

We informed the public when the program was initiated. Chief's blog, appearance at Public Safety Review Committee, etc.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

n/a

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #15

**COMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 10:55:31 AM  
**Last Modified:** Tuesday, June 19, 2018 10:58:52 AM  
**Time Spent:** 00:03:21  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

SWAT Robotics

---

**Q4** What is the purpose of the surveillance technology?

SWAT has several robotics platforms that are equipped with audio and/or visual monitoring. The robotics are used to enter and observe areas during high-risk tactical operations. They are intended to aid officers in searching for high-risk individuals in a safe manner.

---

**Q5** How is the technology utilized?

During high-risk, tactical operations.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

\*\*\*

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Wherever the high-risk incident occurs.

---

**Q12** What factors determine where the surveillance technology is used?

Wherever the high-risk incident occurs.

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

SWAT personnel only

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Only SWAT personnel have access to the equipment

---

### Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

Some of the devices to allow for recording. That data is stored consistently with the in-car video system.

---

**Q18** Which positions in your agency are authorized to access the data?

Same as in-car video.

---

**Q19** For what reason do the authorized positions have access to the data?

Same as in-car video.

---

**Q20** Other than the positions authorized to access the data, who has access?

Same as in-car video.

---

**Q21** How long is the data stored?

Same as in-car video.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Same as in-car video.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

These devices are not covert and are only used in limited circumstances.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

n/a

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

---

**Respondent skipped this question**

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #16

**COMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 10:58:52 AM  
**Last Modified:** Tuesday, June 19, 2018 11:03:55 AM  
**Time Spent:** 00:05:02  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Covert tracking devices

---

**Q4** What is the purpose of the surveillance technology?

Criminal investigations

---

**Q5** How is the technology utilized?

To track the location of an individual suspect (pursuant to a court order)

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

\*\*\*

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Pursuant to specific criminal investigations

---

**Q12** What factors determine where the surveillance technology is used?

Pursuant to specific criminal investigations

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Only limited personnel have access to this technology.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Only limited personnel have access to this technology.

---

Page 5: Surveillance Technology Survey Part 2 Continued

Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

\*\*\*

---

**Q18** Which positions in your agency are authorized to access the data?

\*\*\*

---

**Q19** For what reason do the authorized positions have access to the data?

\*\*\*

---

**Q20** Other than the positions authorized to access the data, who has access?

\*\*\*

---

**Q21** How long is the data stored?

\*\*\*

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

\*\*\*

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

n/a

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

To maintain integrity of criminal investigations

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

---

**Respondent skipped this question**

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #17

**COMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 11:03:55 AM  
**Last Modified:** Tuesday, June 19, 2018 11:10:51 AM  
**Time Spent:** 00:06:56  
**IP Address:** 204.147.0.15

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Telephone recording devices

---

**Q4** What is the purpose of the surveillance technology?

Devices that attach to a telephone and record the conversation. Most common use would be by members of the Crisis Negotiation Team (CNT) to record negotiations during a tactical situation.

---

**Q5** How is the technology utilized?

Personnel involved in a phone conversation would attach the device to their phone and record it.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**MPD SWAT SOP 2017.pdf (61.6KB)**

---

Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

\*\*\*

---

**Q10** Please indicate whether the technology is mobile or stationary. **Mobile**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

n/a

---

**Q12** What factors determine where the surveillance technology is used?

n/a

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Generally issued to CNT members and some detectives.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Only limited personnel have access to these devices.

---

Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

Same as in-car video.

---

**Q18** Which positions in your agency are authorized to access the data?

Same as in-car video.

---

**Q19** For what reason do the authorized positions have access to the data?

Same as in-car video.

---

**Q20** Other than the positions authorized to access the data, who has access?

Same as in-car video.

---

**Q21** How long is the data stored?

Same as in-car video.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Same as in-car video.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

n/a

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

To maintain integrity of investigations

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #18

**COMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 11:10:52 AM  
**Last Modified:** Tuesday, June 19, 2018 11:13:57 AM  
**Time Spent:** 00:03:05  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Covert recording devices

---

**Q4** What is the purpose of the surveillance technology?

Used on a temporary basis for criminal investigations

---

**Q5** How is the technology utilized?

Varies

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**VideoAudioSurveillance.pdf (216.4KB)**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

\*\*\*

---

**Q10** Please indicate whether the technology is mobile or stationary. Other (please specify):  
Both

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Pursuant to specific criminal investigations

---

**Q12** What factors determine where the surveillance technology is used?

Based on investigative needs

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Only limited personnel have access to these devices

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Only limited personnel have access to these devices

---

Page 5: Surveillance Technology Survey Part 2 Continued

Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

\*\*\*

---

**Q18** Which positions in your agency are authorized to access the data?

\*\*\*

---

**Q19** For what reason do the authorized positions have access to the data?

\*\*\*

---

**Q20** Other than the positions authorized to access the data, who has access?

\*\*\*

---

**Q21** How long is the data stored?

\*\*\*

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

**Respondent skipped this question**

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency?

**No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

n/a

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

To maintain integrity of criminal investigations

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #19

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 19, 2018 11:13:57 AM  
**Last Modified:** Tuesday, June 19, 2018 11:18:38 AM  
**Time Spent:** 00:04:41  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Asst. Chief Vic Wahl

---

**Q2** Please enter the name of your City agency.

Police

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Computer, cellphone and mobile device extraction tools

---

**Q4** What is the purpose of the surveillance technology?

Tools used by MPD's forensic services unit to analyze data stored on an electronic device as part of a criminal investigation.

---

**Q5** How is the technology utilized?

Pursuant to a court order or with the consent of the owner.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

DigitalForensics.pdf (101.1KB)

---

## Page 3: Surveillance Technology Survey Part 2 Continued

Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

\*\*\*

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

n/a

---

**Q12** What factors determine where the surveillance technology is used?

n/a

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology. **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Limited FSU personnel

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Only select FSU personnel have access to this equipment

---

Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

Dedicated server

---

**Q18** Which positions in your agency are authorized to access the data?

Limited FSU personnel

---

**Q19** For what reason do the authorized positions have access to the data?

Criminal investigations

---

**Q20** Other than the positions authorized to access the data, who has access?

n/a

---

**Q21** How long is the data stored?

Varies

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

Varies

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

n/a

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

Individuals will generally know that we have seized their device and that it will be subject to analysis.

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #20

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Friday, June 22, 2018 2:49:13 PM  
**Last Modified:** Friday, June 22, 2018 2:54:45 PM  
**Time Spent:** 00:05:32  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Enis Ragland

---

**Q2** Please enter the name of your City agency.

Mayor's Office

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Security camera at main entrance to office

---

**Q4** What is the purpose of the surveillance technology?

Security

---

**Q5** How is the technology utilized?

For security

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**The use of surveillance cameras policy.doc(31KB)**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

1

---

**Q10** Please indicate whether the technology is mobile or stationary. **Stationary**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

---

**Respondent skipped this question**

**Q12** What factors determine where the surveillance technology is used?

---

**Respondent skipped this question**

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology?

---

**Respondent skipped this question**

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

---

**Respondent skipped this question**

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

---

**Respondent skipped this question**

**Q16** How does your agency control unauthorized use of the surveillance equipment?

---

**Respondent skipped this question**

### Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

---

**Respondent skipped this question**

## Surveillance Technology Survey - Part 2

**Q18** Which positions in your agency are authorized to access the data? Respondent skipped this question

---

**Q19** For what reason do the authorized positions have access to the data? Respondent skipped this question

---

**Q20** Other than the positions authorized to access the data, who has access? Respondent skipped this question

---

**Q21** How long is the data stored? Respondent skipped this question

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic. Respondent skipped this question

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? Respondent skipped this question

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. Respondent skipped this question

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. Respondent skipped this question

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. Respondent skipped this question

---

**Q27** Were you unable to completely answer any of the questions in the survey? Respondent skipped this question

---

# #21

**COMPLETE**

**Collector:** Web Link 1 (Web Link)  
**Started:** Friday, June 22, 2018 2:57:05 PM  
**Last Modified:** Friday, June 22, 2018 3:02:44 PM  
**Time Spent:** 00:05:39  
**IP Address:** 204.147.0.15

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Enis Ragland

---

**Q2** Please enter the name of your City agency.

Mayor's Office

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Security Camera

---

**Q4** What is the purpose of the surveillance technology?

Security

---

**Q5** How is the technology utilized?

For Security

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**The use of surveillance cameras policy.doc(31KB)**

---

Page 3: Surveillance Technology Survey Part 2 Continued

Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

1

---

**Q10** Please indicate whether the technology is mobile or stationary.      **Stationary**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)      **Respondent skipped this question**

---

**Q12** What factors determine where the surveillance technology is used?      **Respondent skipped this question**

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology?      **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.      **Respondent skipped this question**

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

All Mayor's Staff

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

N/A

---

Page 5: Surveillance Technology Survey Part 2 Continued

Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

IT

---

**Q18** Which positions in your agency are authorized to access the data?

Deputy Mayor's, Administrative & support staff

---

**Q19** For what reason do the authorized positions have access to the data?

Security purposes

---

**Q20** Other than the positions authorized to access the data, who has access?

IT

---

**Q21** How long is the data stored?

?

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

The data is written over after a specific period of time.

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Signage

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. **Respondent skipped this question**

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #22

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Friday, June 22, 2018 2:38:17 PM  
**Last Modified:** Friday, June 22, 2018 3:07:23 PM  
**Time Spent:** 00:29:05  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Sabrina Tolley

---

**Q2** Please enter the name of your City agency.

Parking Utility

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

The Parking Utility places cameras at all entrances/exits and at Pay-On-Foot revenue collection machines in parking facilities. Additionally, it is our goal to install additional cameras to cover rooftop levels, all elevator and stairwell lobbies, and ground floor access points in parking garages.

The monthly parking permit card access system may fall under the definition of surveillance. It relies on entry and exit data to control user access, track facility occupancy data, update parking space availability counts, and calculate additional hourly fees owed when a permit holder parks for durations outside of their permit hours for billing purposes. Every access card is issued to a specific individual or business group, and entry and exit movements by card number are tracked. However, permit holders may allow others to use their parking permit or share a permit with a carpool group for example, so the entry/exit data alone does not necessarily provide personally identifiable information.

---

**Q4** What is the purpose of the surveillance technology?

The cameras are used to protect the Parking Utility's assets and prevent theft of money from machines and/or damage to equipment, improve safety of parking facility users, and deter crime. While they are not monitored 24/7, cameras are used to aid in customer service when responding to helpline calls, as well as suicide prevention to respond to any unusual activity occurring on rooftops, such as a vehicle parked on the roof when there is significant availability on lower levels, or a person wandering/lingering on the rooftop.

---

## Surveillance Technology Survey - Part 2

### Q5 How is the technology utilized?

Video footage is reviewed when there is an incident, such as damage to gates to identify the vehicle that drove through them and invoice the owner for repair costs, and as evidence to issue a citation for a violation of City Ordinance 8.14(2)(c)4, "Causing Damage at a Municipal Parking Facility While Exiting". Additionally, it is reviewed when there are customer service dispute/resolution issues to verify a vehicle entry time for example. It is also used to monitor/review operations for customer service improvements, for example, reviewing footage to look at timeframes of vehicle queuing, exit wait times, and identify causes of backups to make operational improvements. The Police Department archives and uses video when there is a critical incident or significant crime in/near a parking garage.

Live video is used by staff responding to helpline calls to assist them with the problem; for example, if a customer cannot pay at the exit and has lost their ticket, the vehicle plate number can be verified via camera so that a failure-to-pay notice can be mailed to the customer (allowing them to pay the parking fee within 10 days), and the gate can be raised remotely. Video also allows staff to view the exit lane and adjacent surroundings to verify that there is a vehicle in the lane and the gate can be raised safely before raising remotely.

Monthly parking entry/exit data is used to control access, generate accurate data and fee calculations for customer billing, troubleshoot problems reported by customers about a particular card and determine whether it is malfunctioning and needs to be replaced, controlling space availability, and occupancy reporting.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**Video Policy PU June 2010.pdf (67.3KB)**

---

Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

None that we are aware of

---

**Q9** How many pieces of this type of technology does your agency own?

57 cameras

---

**Q10** Please indicate whether the technology is mobile or stationary. **Stationary**

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

**Respondent skipped this question**

---

## Surveillance Technology Survey - Part 2

**Q12** What factors determine where the surveillance technology is used?

Respondent skipped this question

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology?

Yes

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

Access to cameras is controlled by City IT. Police Department and others, as authorized by IT may have access.

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

All Field Supervisors, Parking Revenue Leadworkers, all field office personnel, Parking Equipment Electrical Technician, Parking Equipment Mechanic I, Parking Engineer, Assistant Parking Utility Manager, and Parking Technical Aide.

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Access control via user login credentials are controlled by City IT.

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

City IT controls storage of video.

**Q18** Which positions in your agency are authorized to access the data?

All Field Supervisors, Parking Revenue Leadworkers, all field office personnel, Parking Equipment Electrical Technician, Parking Equipment Mechanic I, Parking Engineer, Assistant Parking Utility Manager, and Parking Technical Aide.

**Q19** For what reason do the authorized positions have access to the data?

Assisting customers who are having problems using our parking access and revenue control equipment, reviewing incidents where our equipment is damaged by patrons who drive through the exit gates to avoid paying their parking fees, to resolve customer service issues or disputed entrance or exit times, operational review and decision making.

**Q20** Other than the positions authorized to access the data, who has access?

Unauthorized people do not have access.

## Surveillance Technology Survey - Part 2

**Q21** How long is the data stored?

Two weeks - retention is determined by City IT.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

This is performed by City IT.

---

---

### Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Signage is conspicuously posted at various locations within parking facilities to notify the public that surveillance cameras are in use.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

NA - the public is informed through posted signage.

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #23

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, June 26, 2018 8:15:39 AM  
**Last Modified:** Tuesday, June 26, 2018 9:06:47 AM  
**Time Spent:** 00:51:08  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Chris Wilkins

---

**Q2** Please enter the name of your City agency.

Water Utility

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

The water utility has Axis Cameras located at each of its 36 locations. The camera models include bullet style cameras (P1405-LE, P1425-LE, P1427-LE) and dome style cameras (P3364, P3215-VE, P3225-LVE MkII, Q1615). These cameras all have live view and record video based on motion that is detected.

---

**Q4** What is the purpose of the surveillance technology?

The cameras at our remote sites monitor the entrance (interior and exterior) of our building and the reservoir hatches. These reservoir hatches allow access into the water supply. The cameras at the Paterson and Olin Offices monitor the entrances (interior and exterior) into the building, the parking lot, and the vehicle storage area for city vehicles.

---

**Q5** How is the technology utilized?

The live camera footage is used by the 24 hour operator to monitor the water utility sites. The record video footage is used by the water utility to review incidents (for example vandalism). The police also review our video footage for help with their investigations near our facilities.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

## Surveillance Technology Survey - Part 2

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**MWU UseOfVideoSurvCameras.pdf (132.5KB)**

---

### Page 3: Surveillance Technology Survey Part 2 Continued

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

The water utility is not utilizing the audio recording features of the cameras.

---

**Q9** How many pieces of this type of technology does your agency own?

The water utility currently has 168 cameras. A new site will be going online this fall that will have 3 cameras. This will give the water utility a total of 171 cameras.

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

The water utility only has surveillance cameras.

---

**Q12** What factors determine where the surveillance technology is used?

The water utility is monitoring the areas that are viewed as critical to maintaining a safe water supply for the city and keeping the employees at the water utility safe. Any location that would allow access to controlling the water system or give access to the water supply itself.

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

The Madison Police Department, specifically the Forensics Department has access to our cameras and stored footage. They will typically ask the water utility's permission prior to viewing it. IT also has access to our technology. They maintain the camera servers.

---

## Surveillance Technology Survey - Part 2

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Managers, the 24 hour pump operator (live view only), Electronics Maintenance Technician, and the Control Systems Programmer. The Electronics Maintenance Technician and Control Systems Programmer are responsible for the installation/replacement of cameras.

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

The water utility works with IT to set policies for the authorized personnel. The water utility has not had an incident of unauthorized use of the surveillance equipment. In the event of an incident, the individual would be required to meet with HR and the Water Utility GM for possible disciplinary action.

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

It is stored on IT's Exacq Servers located at the City County Building.

---

**Q18** Which positions in your agency are authorized to access the data?

Managers, Electronics Maintenance Technician, and Control Systems Programmer.

---

**Q19** For what reason do the authorized positions have access to the data?

The access is for reviewing footage of incidents that take place at the water utility. These incidents would include vandalism and vehicle accidents that may occur.

---

**Q20** Other than the positions authorized to access the data, who has access?

IT and the Police Forensics Department.

---

**Q21** How long is the data stored?

The video footage is stored for 2 weeks.

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

IT deletes the footage after it has been stored for 2 weeks. I believe this is an automatic process. IT would need to be contacted for more specifics.

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **Yes**

---

## Surveillance Technology Survey - Part 2

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

There are signs posted at our facilities letting people know that it is under video surveillance.

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use. **Respondent skipped this question**

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #24

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Friday, June 29, 2018 7:02:36 PM  
**Last Modified:** Friday, June 29, 2018 7:32:13 PM  
**Time Spent:** 00:29:37  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Brian Smith

---

**Q2** Please enter the name of your City agency.

Traffic Engineering

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Cameras

---

**Q4** What is the purpose of the surveillance technology?

Monitoring traffic conditions at to enable traffic engineering staff to make real time changes to traffic signal timing to improve traffic flow during unexpected traffic events and incidents.

---

**Q5** How is the technology utilized?

Traffic Engineering monitors the cameras during working hours and during planned nighttime and weekend events to determine if changes in signal timing are required to improve traffic operations.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

Not that I am aware of

---

**Q9** How many pieces of this type of technology does your agency own?

Several

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

On traffic Signal and Street Light poles

---

**Q12** What factors determine where the surveillance technology is used?

Locations where information collected from the cameras can be useful to making better traffic control decisions to improve traffic operations.

---

---

### Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

City Engineering and Madison Police

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Traffic Signal and Traffic Operations Engineers as well as the Traffic Engineer and Assistant Traffic Engineer

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

All Staff with access to traffic cameras have received verbal instructions as to not use these cameras for any other purpose than observations of traffic operations.

---

---

### Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

City IT controls the storage

---

**Q18** Which positions in your agency are authorized to access the data?

Traffic Signal and Operations Engineering staff as well at the City Traffic Engineer and Assistant Traffic Engineer

---

**Q19** For what reason do the authorized positions have access to the data?

For monitoring traffic conditions in order to better improve traffic operations

---

**Q20** Other than the positions authorized to access the data, who has access?

Individuals in other departments such as Police and Engineering as authorized by City IT

---

**Q21** How long is the data stored?

City IT controls this. I believe it is typically stored about 2 weeks

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

City IT controls this

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. **Respondent skipped this question**

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

Traffic Engineering staff surveillance is limited to traffic operations only

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here. **Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **No**

---

# #25

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, July 03, 2018 12:57:16 PM  
**Last Modified:** Tuesday, July 03, 2018 1:17:41 PM  
**Time Spent:** 00:20:24  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Herbert King Jr.

---

**Q2** Please enter the name of your City agency.

Information Technology

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

IP Cameras

---

**Q4** What is the purpose of the surveillance technology?

Monitor ingress/egress of city critical IS infrastructure

---

**Q5** How is the technology utilized?

Monitor access

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **Yes**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here.

**IT Camera Policy.pdf (559.7KB)**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

No

---

**Q9** How many pieces of this type of technology does your agency own?

4

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

NA

---

**Q12** What factors determine where the surveillance technology is used?

Secure access

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **No**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

NA

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Management

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Security group membership

---

Page 5: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q17** Where is the data collected from this technology stored?

Enterprise camera application

---

**Q18** Which positions in your agency are authorized to access the data?

Management

---

**Q19** For what reason do the authorized positions have access to the data?

Review access to/from data centers

---

**Q20** Other than the positions authorized to access the data, who has access?

None

---

**Q21** How long is the data stored?

14 days

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

written over - automatically

---

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

NA

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

residents don't have access to room

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

**Respondent skipped this question**

---

**Q27** Were you unable to completely answer any of the questions in the survey? **Yes**

---

# #26

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, July 03, 2018 1:17:45 PM  
**Last Modified:** Tuesday, July 03, 2018 1:26:33 PM  
**Time Spent:** 00:08:48  
**IP Address:** 204.147.0.15

---

## Page 1: Instructions for Survey

**Q1** Please enter your name.

Tom Conrad

---

**Q2** Please enter the name of your City agency.

CDA Housing Operations Division

---

## Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

Security cameras

---

**Q4** What is the purpose of the surveillance technology?

to make visual recordings of criminal acts

---

**Q5** How is the technology utilized?

Housing staff review video after incidents and provide access to the recordings for law enforcement.

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

## Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

no

---

**Q9** How many pieces of this type of technology does your agency own?

I'm not sure how many cameras CDA has.

---

**Q10** Please indicate whether the technology is mobile or **Stationary** stationary.

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

Public housing sites.

---

**Q12** What factors determine where the surveillance technology is used?

Crime rates

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology? **Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

3rd party security company, Wisconsin Security Services.

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

Housing site managers

---

**Q16** How does your agency control unauthorized use of the surveillance equipment? **Respondent skipped this question**

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

On site

---

## Surveillance Technology Survey - Part 2

**Q18** Which positions in your agency are authorized to access the data?

Housing site managers

---

**Q19** For what reason do the authorized positions have access to the data?

Security

---

**Q20** Other than the positions authorized to access the data, who has access?

Respondent skipped this question

---

**Q21** How long is the data stored?

Respondent skipped this question

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

---

Respondent skipped this question

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency?

Yes

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use.

Respondent skipped this question

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

Respondent skipped this question

---

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

Respondent skipped this question

---

**Q27** Were you unable to completely answer any of the questions in the survey?

Yes

---

#27

INCOMPLETE

**Collector:** Web Link 1 (Web Link)  
**Started:** Tuesday, July 03, 2018 2:55:36 PM  
**Last Modified:** Tuesday, July 03, 2018 3:17:05 PM  
**Time Spent:** 00:21:28  
**IP Address:** 204.147.0.15

---

Page 1: Instructions for Survey

**Q1** Please enter your name.

Assistant Chief Mike Popovich

---

**Q2** Please enter the name of your City agency.

City of Madison Fire Department

---

Page 2: Surveillance Technology Survey Part 2 Continued

**Q3** You previously indicated that your agency has surveillance technology. Please describe the surveillance technology.

We have installed, under the guidance of city IT about 25 PTZ cameras at Fire Administration and outside all 13 fire stations. All of our cameras are within the execVision software and viewable by MFD command staff and IT manager.

---

**Q4** What is the purpose of the surveillance technology?

Safety of employees welfare and security of POV's. Cameras may also be reviewed during an accident investigation.

---

**Q5** How is the technology utilized?

A manager may look at recorded video

---

**Q6** Does your agency have a policy governing the use of the surveillance technology? **No**

---

**Q7** If your agency has a policy governing the use of the surveillance technology, please upload it here. **Respondent skipped this question**

---

Page 3: Surveillance Technology Survey Part 2 Continued

## Surveillance Technology Survey - Part 2

**Q8** Does the technology have capabilities that are not utilized? For example, an agency may have security cameras capable of recording audio, though the audio recording is not utilized.

Not to my knowledge

The dash camera on our command vehicle is none audio

---

**Q9** How many pieces of this type of technology does your agency own?

About 30, mounted to front and rear of fire stations and inside fire administration. 1 vehicle dash camera on the MFD command suburban

---

**Q10** Please indicate whether the technology is mobile or stationary.

**Stationary,**  
Other (please  
specify):  
both

---

**Q11** This question does NOT pertain to surveillance cameras. Please answer this question for all other surveillance equipment. Where is the technology deployed throughout the City of Madison? Please be specific. (Note: If providing this information would jeopardize security, please indicate why you cannot disclose the locations.)

fire administration and the 13 stations

command vehicle

---

**Q12** What factors determine where the surveillance technology is used?

funding was used over the last several years to provide the safety and security at all stations and fire administration

---

Page 4: Surveillance Technology Survey Part 2 Continued

**Q13** Does another City agency or other external organization share access to the technology?

**Yes**

---

**Q14** If you answered "yes," above please note which City agency or other external organizations share access to the technology and which agency is considered the owner of the surveillance technology.

IT and MPD, I believe

---

**Q15** Which positions in your agency are authorized to use the surveillance equipment?

11 command staff and MFD IT

---

**Q16** How does your agency control unauthorized use of the surveillance equipment?

Not possible as far as I know

---

Page 5: Surveillance Technology Survey Part 2 Continued

**Q17** Where is the data collected from this technology stored?

IT and city network

---

**Q18** Which positions in your agency are authorized to access the data?

command staff

---

**Q19** For what reason do the authorized positions have access to the data?

na

---

**Q20** Other than the positions authorized to access the data, who has access?

na

---

**Q21** How long is the data stored?

several months  
Dash Camera is longer

---

**Q22** How is the data destroyed once the data storage has been completed? Please be specific and describe the process including whether the process is automatic.

unsure

---

Page 6: Surveillance Technology Survey Part 2 Continued

**Q23** Do you inform residents that this surveillance technology is in use by your agency? **No**

---

**Q24** If you inform residents about the surveillance technology please indicate how your agency informs residents that this surveillance technology is in use. **Respondent skipped this question**

---

**Q25** If you do not inform residents about the surveillance technology, please explain why residents are not informed that the surveillance technology is in use.

this was never discussed

---

## Surveillance Technology Survey - Part 2

**Q26** If you needed more space to respond to any questions, you are welcome to provide additional information by attaching files. You can upload doc, docx, and pdf files here.

---

**Respondent skipped this question**

**Q27** Were you unable to completely answer any of the questions in the survey?

---

**No**

Department/Area	Purpose	Statement of Need	Enterprise System?	Personnel w/Access	Circumstances of Access	Type of Data Recorded	Location of Equipment	Location of Public Notice	Data Retention Period	Data Retention Procedures
<b>MPD General</b>	To aid investigative nefforts and promote greater public safety	To assist in investigations, protect and secure MPD facilities, maintain order during planned and unplanned events.	Yes. Occasionally uses stand alone covert video limited in duration.	All commissioned members of MPD	Only in comjnction with official duties as an MPD Officer.	Video	Public areas in MPD facilities	Entrances, customer service areas, internal secure holding areas.	Purged after 14 days	In complaine with MPD departmental procedures.
<b>MPD UAS</b>	Support department operations by providing aerial observasion of law enformcement and public safety incidents.	To assist in special events, aerial visual support of MPD operations, search and rescue, aerial documentation of crime scenes, aerial images of hazardous areas, tactical operations, training testing and evaluation, deomonstration or maintenance, other activites as designated by the Chief.	Unknown	UAS Program coordinator	Determined by Chief, program coordinator or designee.	Video	Aerial/mobile	NA	In accordance with MPD records retention schedules. 180 days	Unknown
<b>MPD Body Cameras</b>	To document activities of SWAT officers during tactical operations	Identify performance improvements and colpliance with MPD's code of conduct and SOPs	Yes	SWAT officers and supervisors	SWAT team leaders	Video and audio	Worn by officers	NA	Reference made to MPD record retention schedules purged after 180 days	Downloaded onto evidentiary server of MPD.
<b>MPD Digital Forensics</b>	Enhance capabilities of officers to conduct investigations and prosecute crimes that involve the use of computers, tablets, cell phones or other stage data devices.	Needed to investigate and prosecute crimes committed with devices which store digital data.	Yes	MPD officers. No specificity of rank.	Officers conducting an investigation of crimes committed with digital devices	Digital data	Wherever crimes with digital devices are committed.	NA	Unknown. Policy references preservation of evidence procedures.	Computer forensic examiners will ensuer chain of custody and ensure that evidence is properly secured.
<b>MPD In-Car Video</b>	To accurately document events, actions, conditions and statements during LE contacts.	Document events, actions, conditions and statements during LE contacts.	Yes	All officers operating MPD cars with cameras	All officers operating MPD cars with cameras	Video	In MPD vehicles	NA	Retrieved after every shift and stored on server	Downloaded onto evidentiary server of MPD.
<b>IT</b>	To monitor activities in the department's 2 data centers.	Monitoring is needed because critical network infrastructure and sensitive information is located at both locations	Yes	IT managment staff and Network Operations Staff	The 2 system adminitrators are authorized to extract footage as needed for investigations. Access given to MPD upon request.	Video	At data centers	At entrances and exits	7 years as according to open records statutes	City's retention and open records policies

Department/Area	Purpose	Statement of Need	Enterprise System?	Personnel w/Access	Circumstances of Access	Type of Data Recorded	Location of Equipment	Location of Public Notice	Data Retention Period	Data Retention Procedures
<b>Mayor's Office</b>	Safety and security	Equipment may be activated by any member of the mayor's office to facilitate quality improvement of customer service, providing trainings to staff, complying with public records laws or to document an incident for investigative purposes.	Yes	Mayoral office clerks and MPD	Equipment may be activated by any member of the Mayor's office to facilitate quality improvements of customer service or to document an incident for investigative purposes. Access given to MPD upon request.	Video	Mounted in the reception area	Mounted in the reception area	City's retention policy 90 days minimum	City's retention and open records policies
<b>Monona Terrace</b>	To enhance the security and safety of guests as well as detect and deter criminal activity in and around the facility	Needed to monitor safety of individuals, property and facility, investigation of criminal activity, monitor any behavior outside the ordinary	No	Identified trained and supervised personnel and MPD when requested.	Stored video access is limited to the Monona Terrace Director, Director of Operations, Operations Manager, and Assistant Operations Manager. Access granted for investigations and assess performance etc. Access given to MPD upon request.	Video	In and around Monona Terrace	Unknown	unknown	Stored in a secure locatiopn in the command center
<b>Parking Utility</b>	ensure safety and security of customers and employees; safeguard revenue stream	Ensure safety and security of customers and employees; safeguard revenue stream	Yes	Approved Parking Utility staff, not specific, A witness to confirm identification, MPD	Specific Parking Utility management and line staff, not detailed in the document have access as well as MPD for investigations.	Video	Payment machines, entrances and exits. Some portable cameras to identify problem behavior.	Entrances and exits of facilities	Unknown, policy only states video will be stored on an ongoing basis. Copied videos retained in accordance to open records laws.	Any copied videos will be stored in a separate area from the video storage system and retained in accordance to open records laws.

Department/Area	Purpose	Statement of Need	Enterprise System?	Personnel w/Access	Circumstances of Access	Type of Data Recorded	Location of Equipment	Location of Public Notice	Data Retention Period	Data Retention Procedures
<b>Water Utility</b>	Security of City assets, infrastructure and chemical supplies.	To provide security, ensure safety of wells etc and to have documentation when there are accidents , particulalry to Water Utility personnel.	Yes	Water Supply Manager has oversight, MWU managers and pump operators will be allowed to view continuous loops	Electronic Maintenance Techs will have access for maintenance of software and hardware, otherwise it is used to monitor operations and possible illegal activity. Access given to MPD upon request.	Video	35 remote facilities, Administration building , maintenance and storage facilities.	Entrances of facilities and around infrastructure like wells etc.		
<b>Finance</b>	Safety and securitysecurity	It is needed for staff to identify who is coming into the department and grant access.	Yes	Any staff working the front desk	Staff use it to allow access into the department and MPD can access data upon request	Video	Outside Rooms 406 and 416 at the City-County Building	NA	City's retention policy 90 days minimum	City's retention and open records policies
<b>Treasurer's Office</b>	Security reasons, in case of a robbery	Security reasons, in case of a robbery	yes	City Treasurer	IT and MPD have access as needed.	Video, no audio	8 cameras inside and lobby area	sign posted on bulletin board.	determined by IT, unknown.	data stored on city servers
<b>Metro Transit</b>	Cameras on buses, at our bus facilities, at our transfer points, automated vehicle locator systems that track where a bus is at a certain point, which can be helpful for safety or security reasons, and a farebox system with features a tracking system that has been used to address safety and security issues.	To try to achieve the highest levels of safety and security, consistent with guidance we get from other transit systems, our transit insurance company, the police department, and the national TSA.	yes	Specific supervisors and managers, but not all. They need to have a job-specific reason, such as the supervisor who responds to security incidents that require follow-up, or the Metro IT manager who is often needed to assist with that	MPD has access as needed as well as school district	Video, some cameras also have audio capabilities.	Busses, facilities and transit points	on buses and at facilities.	varies depending on the security system	data kept on City and Metro servers with IT

Department/Area	Purpose	Statement of Need	Enterprise System?	Personnel w/Access	Circumstances of Access	Type of Data Recorded	Location of Equipment	Location of Public Notice	Data Retention Period	Data Retention Procedures
<b>Streets</b>	Cameras that oversee the three public drop off locations as well as oversee the Streets Division work locations, Badger, Sycamore, Transfer Station and South Point	Monitor public use of the drop off locations\ discourage illegal dumping. Further serves as a deterrent to breakins of our outside equipment as well as facilities. Cameras in shop areas are primarily used to monitor equipment location but also employee actions.	yes	Comp Group 18 (Supervisory) employees have varying degrees of access to cameras.	MPD as needed. Access limited by individual log on. Supervisors only for the 15 min option. Supt and Asst Supt have access to go back several months thru the system.	video only	facilities	signs placed in public areas like drop off sites	Cameras can only store the last 15 minutes of video that anyone with access can reach	Supervisors only for the 15 min option. Supt and Asst Supt have access to go back several months thru the system.
<b>Library</b>	The Library uses surveillance technology to assist in identifying individuals who participate in negative behavior, threaten staff or public safety, or otherwise engage in dangerous or criminal activity.	safety and security	yes	Branch Supervisors (at branches that have cameras), Library Security Staff at Central Library, Library and City IT	Only MPD as needed.	Video only but cameras have sound capability	Central Library, Goodman South Madison Library, Meadowridge Library	None	Unknown, managed by IT	Unknown, managed by IT
<b>Traffic Engineering</b>	Monitoring traffic conditions at to enable traffic engineering staff to make real time changes to traffic signal timing to improve traffic flow during unexpected traffic events and incidents.	Traffic Engineering monitors the cameras during working hours and during planned nighttime and weekend events to determine if changes in signal timing are required to improve traffic operations.	yes	Traffic Signal and Traffic Operations Engineers as well as the Traffic Engineer and Assistant Traffic Engin	City Engineering and Madison Police	video	On traffic Signal and Street Light poles	None, limited to traffic operations	Determined by City IT	City IT is responsible for storage
<b>CDA</b>	to make visual recordings of criminal acts	Housing staff review video after incidents and provide access to the recordings for law enforcement.	Unknown. Don't think so.	Housing site managers	3rd party security company, Wisconsin Security Services and MPD as needed.	video	Public housing sites	unknown	Unknown, managed by IT	Data stored on site
<b>MFD</b>	Safety of employees welfare and security of POV's. Cameras may also be reviewed during an accident investigation.	Safety and security	yes	11 command staff and MFD IT	IT and MPD have access as needed.	video	13 fire stations, 1 dash camera in commad vehicle.	NA	several months Dash Camera is longer	IT City network

	<b>Nashville</b>	<b>Santa Clara</b>	<b>Seattle</b>	<b>Sommerville</b>
<b>Approval (General)</b>	Required for: installing, accepting funds or donations, entering into agreements to share tech or data	Required for: acquiring new technology, seeking funds or donations, using tech in a manner not previously approved, or entering into agreements to share tech or data	Council reviews and votes on acquisition and deployment of all new and existing surveillance tech	Mayoral approval prior to acquisition, subject to appropriation by Board of Aldermen
<b>Approval for Use Policies</b>		Required for: seeking funds or donations, using tech in a manner not previously approved, or entering into agreements to share tech or data	Departments must obtain a Surveillance Impact Report (SIR) for the technology prior to approval which includes a usage policy (see Seattle chart for details)	Mayoral approval of operational protocols required prior to deployment or installation
<b>Approval for Data Management Policies</b>		Data collection, access, protection, retention and public access are all included in the surveillance use policy	Departments must obtain a Surveillance Impact report for the technology prior to approval which includes a data management policy	City departments shall submit written protocols for managing data collected by surveillance equipment to the Mayor.

**Nashville****Santa Clara****Seattle****Sommerville**

<b>Transparency</b>		The County department seeking approval for surveillance tech must submit to the Board an Anticipated Surveillance Impact Report and a proposed Surveillance Use Policy before the public meeting; printed copies of both shall be released before the meetings	The CTO shall post the latest version of all proposed and all approved SIRs to the City's website with an indication of its current approval status and if available the planned Council date for action. The Annual Surveillance Usage Review is also posted to the City's website	Requests for approval and supporting documentation shall be posted on the City's website upon submission to the Mayor
<b>Public Engagement</b>		1) All approvals take place at public regular Board meetings. 2) The annual review takes place in a public Board meeting and includes the Department's Annual Surveillance Reports and all approvals/rejections of surveillance use policies in the past year	One or more meetings with opportunity for public comment and written response are required for each surveillance tech approval	Requests for approval shall include a public notification plan for each community in which the department intends to use the surveillance equipment

**Nashville****Santa Clara****Seattle****Sommerville**

<b>Review</b>		<p>Annual Surveillance Report required from each County department</p> <p>The Board will utilize the Annual Surveillance Report to determine whether the benefits to the County departments outweigh the costs and concerns</p>	<p>1) The Chief Technology Officer produces an annual "Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report" 2) The Inspector General and the City Auditor shall conduct an annual review of use of surveillance tech and the compliance with the requirements of the ordinance</p>	<p>One year after the effective date of this policy, the Mayor will review implementation as it applies to City department use of surveillance equipment</p>
<b>Law Enforcement Exemptions</b>	<p>Law enforcement and governmental exemption from ordinance if the surveillance technology is used: 1) On a temporary basis for the purpose of a criminal investigation supported by reasonable suspicion, 2) Pursuant to a lawfully issued search warrant, 3) Under exigent circumstances as defined in case law</p>	<p>1) Sheriff and DA exempt from approval requirements including surveillance use policies for surveillance tech use in investigations and prosecutions 2) The Sheriff's Office and the DA's Office may temporarily acquire or temporarily use surveillance tech in exigent circumstances. The Board shall not obstruct the investigative function of the Sheriff nor the investigative or prosecutorial functions of the DA</p>	<p>1) Body-worn cameras, police car cameras, traffic cameras, security cameras, technology to monitor City employee performance 2) Emergency situations that pose a serious threat of death or bodily harm</p>	<p>1) Somerville Police may use surveillance equip on a temporary basis for the purpose of a criminal investigation under the following conditions 2) Supported by reasonable suspicion with supervisory authority, pursuant to a lawfully issued search warrant 3) Under exigent circumstances as defined in case law 4) Or when the Chief of Police finds, subject to approval of the Mayor, that compelling circumstances in the public interest warrant temporary use</p>

**Nashville****Santa Clara****Seattle****Sommerville**

<b>Other Exemptions</b>	Building security /unlawful access	DA and Sheriff otherwise need to obtain approval for acquiring, using, and entering into agreements with other entities on surveillance tech	1) Information knowingly volunteered or where the individual could opt out 2) Technical patch or upgrade necessary to mitigate threats to the City's environment	
<b>Other Exemptions</b>	The ordinance does not apply to the Nashville Electric Service, the Airport Authority, the Housing Agency or Transit Authority		The ordinance does not apply to the Seattle Municipal Court, Seattle Public Library	
<b>Enforcement</b>		1) Violations resulting from arbitrary or capricious action or conduct by the County or an officer thereof in his or her official capacity, the prevailing complainant in an action for injunctive relief may collect from the County reasonable attorney's fees 2) Intentional misuse of County-owned surveillance technology is a misdemeanor	1) A person who is surveilled and injured by a violation of the ordinance may institute proceedings against the City 2) The Chief Tech Officer shall direct any City department out of compliance with the ordinance to cease use of surveillance tech	



# City of Madison

City of Madison  
Madison, WI 53703  
www.cityofmadison.com

## Master

**File Number: 49284**

**File ID:** 49284

**File Type:** Ordinance

**Status:** Passed

**Version:** 3

**Reference:**

**Controlling Body:** PUBLIC SAFETY  
REVIEW  
COMMITTEE

**File Created Date :** 10/23/2017

**File Name:** Operating security cameras at convenience stores

**Final Action:** 04/10/2018

**Title:** 2nd SUBSTITUTE Creating Section 23.52 of the Madison General Ordinances to establish guidelines for the operation of security cameras at convenience stores and amending Section 1.08 to establish a bail deposit schedule for violation of this ordinance.

**Notes:** 6026cameras2ndSUB  
Mayoral Approval Date: 04/18/2018

**Sponsors:** Paul E. Skidmore and Paul R. Soglin

**Effective Date:** 04/24/2018

**Attachments:** 2nd Substitute Body, Substitute Body, Version 1,  
Pixels per Foot

**Enactment Number:** ORD-18-00042

**Author:** Marci Paulsen

**Hearing Date:**

**Entered by:** dalthaus@cityofmadison.com

**Published Date:** 04/23/2018

### Approval History

Version	Date	Approver	Action
1	10/23/2017	Michael May	Approved as to Form
1	10/25/2017	Elizabeth York	Approve
2	03/09/2018	Michael May	Approved as to Form
2	03/09/2018	Elizabeth York	Approve
3	04/03/2018	Michael May	Approved as to Form
3	04/03/2018	Elizabeth York	Approve

### History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

- 1 Attorney's Office/Approval 10/23/2017 Referred for  
Group Introduction  
**Action Text:** This Ordinance was Referred for Introduction  
**Notes:** Public Safety Review Committee
- 1 COMMON COUNCIL 10/31/2017 Refer PUBLIC SAFETY REVIEW COMMITTEE 03/14/2018 Pass  
**Action Text:** A motion was made by Rummel, seconded by Baldeh, to Refer to the PUBLIC SAFETY REVIEW COMMITTEE. The motion passed by voice vote/other.  
**Notes:**
- 1 PUBLIC SAFETY REVIEW COMMITTEE 11/08/2017 Referred PUBLIC SAFETY REVIEW COMMITTEE 03/14/2018  
**Action Text:** Alder Skidmore shared an email from Dave Ring of Kwik Trip in favor of the guidelines. Andrew Bowman from Stop N Go shared his questions and concerns about the guidelines. Alder McKinney suggested taking more time to make the ordinance stronger and clearer. Alder Skidmore was in favor of getting more industry input. Alder McKinney motioned to postpone until January. Alder Skidmore seconded. The proposed motion was unanimously approved by the committee.
- 2 PUBLIC SAFETY REVIEW COMMITTEE 03/14/2018 RECOMMEND TO COUNCIL TO ADOPT - REPORT OF OFFICER 03/14/2018 Pass  
**Action Text:** Catherine Van Hove, Forensic Video Analyst from the Madison Police Department presented information on the quality of cameras and shared images of different resolutions and frames per second from the quality and the distance of a camera. Marci Paulsen, Assistant City Attorney shared information on the substitute ordinance at convenience stores which are required to have security cameras. The substitute ordinance changes the number of days from 30 to 15 days that pictures must be stored and maintained after capturing an image. Information was discussed on the cost of cameras for convenience stores and the number of storage days and whether 15 days was long enough to hold videos in storage.  
  
Alder Skidmore made a motion to go with the substitute ordinance as written. Alder Zellers seconded the motion. The motion passed by the following:  
Absent: 4 Syed (John) Mustajab Abbas; Mary T. Anglim; Barbara Harrington-McKinney and Charles Myadze  
Ayes: 5 Paul E. Skidmore; Ledell Zellers; Debra F. Julian; Margaret Anderson and Gideon W. Amoah  
Noes: 1 Sara J. Petzold
- 3 COMMON COUNCIL 04/10/2018 Adopt Pass  
**Action Text:** A motion was made by Baldeh, seconded by Verveer, to Adopt. The motion passed by voice vote/other.  
**Notes:**
- 

## Text of Legislative File 49284

### Fiscal Note

The proposed ordinance establishes guidelines for the operation of security cameras at convenience stores and establishes a bail deposit schedule for violation of this ordinance. There are no direct costs for the City associated with the creation of the ordinance. It is not anticipated that there will be many citations. MPD may incur additional expenses to take in video as evidence (i.e., preservation, redaction, open records) in those instances where the cameras help to identify suspects engaged in crimes. However, efficiencies gained in getting the evidence should offset any additional processing costs. No appropriation is required.

### Title

2nd SUBSTITUTE Creating Section 23.52 of the Madison General Ordinances to establish guidelines for the operation of security cameras at convenience stores and amending Section 1.08 to establish a bail deposit schedule for violation of this ordinance.

**Body**

DRAFTER'S ANALYSIS: This ordinance requires all convenience stores to have security cameras. The ordinance further requires minimum lighting for the use of security cameras. Under this ordinance, convenience stores are required to have security cameras that provide an overview of transaction counter and register area, a camera that captures an individual's face as they enter or exit the store and cameras at all fuel areas. The cameras must have an image quality of at least fifty pixels per foot and a recorded resolution of 1280 x 720. Convenience stores are required to record images at a rate of at least fifteen frames per second and store the images captured on the cameras and be capable of duplication. The ordinance further requires a notice be posted at all entrances and exits informing individuals that they are being recorded. The ordinance also establishes a penalty and bail deposits for violations. This ordinance shall be effective six months after adoption. This second substitute corrects a typographical error, clarifies that all other ordinances regarding exterior lighting must be followed and provides clarification regarding the position of the security cameras.

\*\*\*\*\*

The Common Council of the City of Madison do hereby ordain as follows:  
Please see "2nd Substitute Body" in Attachments.

**LEGISTAR 49284 – 2<sup>nd</sup> Substitute Body**

DRAFTER'S ANALYSIS: This ordinance requires all convenience stores to have security cameras. The ordinance further requires minimum lighting for the use of security cameras. Under this ordinance, convenience stores are required to have security cameras that provide an overview of transaction counter and register area, a camera that captures an individual's face as they enter or exit the store and cameras at all fuel areas. The cameras must have an image quality of at least fifty pixels per foot and a recorded resolution of 1280 x 720. Convenience stores are required to record images at a rate of at least fifteen frames per second and store the images captured on the cameras and be capable of duplication. The ordinance further requires a notice be posted at all entrances and exits informing individuals that they are being recorded. The ordinance also establishes a penalty and bail deposits for violations. This ordinance shall be effective six months after adoption. This second substitute corrects a typographical error, clarifies that all other ordinances regarding exterior lighting must be followed and provides clarification regarding the position of the security cameras.

\*\*\*\*\*

The Common Council of the City of Madison do hereby ordain as follows:

1. Section 23.52 entitled "Security Cameras at Convenience Stores" of the Madison General Ordinances is created to read as follows:

**"23.52 SECURITY CAMERAS AT CONVENIENCE STORES.**

(1) Definitions.

"Convenience Store" shall mean an establishment where motor fuel products or other minor accessories are retailed directly to the public on the premises, in combination with the sale of items typically found in a convenience market or supermarket.

"Lighting" shall mean sufficient lighting to ensure that the security camera is able to produce discernable images, including imagery sufficient to identify persons.

"Security camera" shall mean a high resolution camera that can produce reproducible digital color images and shall display a date and time stamp on each image and that has an image quality of at least fifty (50) pixels per foot and a recorded resolution of 1280 x 720.

(2) All owners of convenience stores shall maintain and operate security cameras during all hours the convenience store is open to customers. Subject to all other ordinances regulating lighting, owners of convenience stores must maintain adequate lighting to ensure that the security camera captures a clear, identifiable image. Security cameras shall be located at all of the following locations:

- (a) At least one security camera shall be positioned to capture an overview of each transaction counter and register area;
- (b) At least one security camera shall be positioned to capture a clear, identifiable full-frame image of an individual's face as they enter or exit the convenience store; and
- (c) At least one security camera shall be positioned to capture the general area surrounding any fuel area to capture an image which identifies the operator and the vehicle.

(3) Storage and Preservation of Records. All digital video records from security cameras must be recorded at a rate of at least fifteen (15) frames per second and stored and maintained in good viewing order for fifteen (15) days after capturing an image. The digital video recorder must be capable of exporting exact duplicates of their recordings to a standard removable media format (e.g. CD, DVD, Flash Drive). When requested by the Madison Police Department, the convenience store owner shall insure that requested record is stored and maintained adequately until retrieved by the Madison Police Department. The convenience store owner shall insure that they are adequate staff trained in the retrieval of digital video records to appropriately respond to a request for said record.

- (4) Notice. All convenience store owners shall conspicuously post a sign at all entrances and exits (excluding emergency exits and employee-only entrances). The sign must contain at least the following language, in lettering that shall be bold and a minimum of two (2) inches in height:

VIDEO RECORDING EQUIPMENT IN USE. YOU MAY BE RECORDED

- (5) Penalty. Whoever violates any provision of this ordinance shall be subject to a penalty of not less than one hundred dollars (\$100) and not more than one thousand dollars (\$1000). Each and every day that a violation exists shall constitute a separate offense.”

2. Subdivision (a) of Subsection (3) entitled “Schedule of Deposits” of Section 1.08 entitled “Issuance of Citations for Violations of Certain Ordinances and Providing a Schedule of Cash Deposits” of the Madison General Ordinances is amended by creating and amending therein the following:

<u>“Offense</u>	<u>Ord. No./Adopted Statute No.</u>	<u>Deposit</u>
Security cameras in convenience stores.	23.52	\$200, 1st \$500, 2nd \$750, 3rd & sub.”

3. This ordinance shall be effective six months after adoption.

EDITOR’S NOTE: New bail deposits must be approved by the Municipal Judge prior to adoption. This deposit has been so approved.



# City of Madison

City of Madison  
Madison, WI 53703  
www.cityofmadison.com

## Master

**File Number: 49284**

**File ID:** 49284

**File Type:** Ordinance

**Status:** Passed

**Version:** 3

**Reference:**

**Controlling Body:** PUBLIC SAFETY  
REVIEW  
COMMITTEE

**File Created Date :** 10/23/2017

**File Name:** Operating security cameras at convenience stores

**Final Action:** 04/10/2018

**Title:** 2nd SUBSTITUTE Creating Section 23.52 of the Madison General Ordinances to establish guidelines for the operation of security cameras at convenience stores and amending Section 1.08 to establish a bail deposit schedule for violation of this ordinance.

**Notes:** 6026cameras2ndSUB  
Mayoral Approval Date: 04/18/2018

**Sponsors:** Paul E. Skidmore and Paul R. Soglin

**Effective Date:** 04/24/2018

**Attachments:** 2nd Substitute Body, Substitute Body, Version 1,  
Pixels per Foot

**Enactment Number:** ORD-18-00042

**Author:** Marci Paulsen

**Hearing Date:**

**Entered by:** dalthaus@cityofmadison.com

**Published Date:** 04/23/2018

### Approval History

Version	Date	Approver	Action
1	10/23/2017	Michael May	Approved as to Form
1	10/25/2017	Elizabeth York	Approve
2	03/09/2018	Michael May	Approved as to Form
2	03/09/2018	Elizabeth York	Approve
3	04/03/2018	Michael May	Approved as to Form
3	04/03/2018	Elizabeth York	Approve

### History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

- 1 Attorney's Office/Approval 10/23/2017 Referred for  
Group Introduction  
**Action Text:** This Ordinance was Referred for Introduction  
**Notes:** Public Safety Review Committee
- 1 COMMON COUNCIL 10/31/2017 Refer PUBLIC SAFETY REVIEW COMMITTEE 03/14/2018 Pass  
**Action Text:** A motion was made by Rummel, seconded by Baldeh, to Refer to the PUBLIC SAFETY REVIEW COMMITTEE. The motion passed by voice vote/other.  
**Notes:**
- 1 PUBLIC SAFETY REVIEW COMMITTEE 11/08/2017 Referred PUBLIC SAFETY REVIEW COMMITTEE 03/14/2018  
**Action Text:** Alder Skidmore shared an email from Dave Ring of Kwik Trip in favor of the guidelines. Andrew Bowman from Stop N Go shared his questions and concerns about the guidelines. Alder McKinney suggested taking more time to make the ordinance stronger and clearer. Alder Skidmore was in favor of getting more industry input. Alder McKinney motioned to postpone until January. Alder Skidmore seconded. The proposed motion was unanimously approved by the committee.
- 2 PUBLIC SAFETY REVIEW COMMITTEE 03/14/2018 RECOMMEND TO COUNCIL TO ADOPT - REPORT OF OFFICER 03/14/2018 Pass  
**Action Text:** Catherine Van Hove, Forensic Video Analyst from the Madison Police Department presented information on the quality of cameras and shared images of different resolutions and frames per second from the quality and the distance of a camera. Marci Paulsen, Assistant City Attorney shared information on the substitute ordinance at convenience stores which are required to have security cameras. The substitute ordinance changes the number of days from 30 to 15 days that pictures must be stored and maintained after capturing an image. Information was discussed on the cost of cameras for convenience stores and the number of storage days and whether 15 days was long enough to hold videos in storage.  
  
Alder Skidmore made a motion to go with the substitute ordinance as written. Alder Zellers seconded the motion. The motion passed by the following:  
Absent: 4 Syed (John) Mustajab Abbas; Mary T. Anglim; Barbara Harrington-McKinney and Charles Myadze  
Ayes: 5 Paul E. Skidmore; Ledell Zellers; Debra F. Julian; Margaret Anderson and Gideon W. Amoah  
Noes: 1 Sara J. Petzold
- 3 COMMON COUNCIL 04/10/2018 Adopt Pass  
**Action Text:** A motion was made by Baldeh, seconded by Verveer, to Adopt. The motion passed by voice vote/other.  
**Notes:**
- 

## Text of Legislative File 49284

### Fiscal Note

The proposed ordinance establishes guidelines for the operation of security cameras at convenience stores and establishes a bail deposit schedule for violation of this ordinance. There are no direct costs for the City associated with the creation of the ordinance. It is not anticipated that there will be many citations. MPD may incur additional expenses to take in video as evidence (i.e., preservation, redaction, open records) in those instances where the cameras help to identify suspects engaged in crimes. However, efficiencies gained in getting the evidence should offset any additional processing costs. No appropriation is required.

### Title

2nd SUBSTITUTE Creating Section 23.52 of the Madison General Ordinances to establish guidelines for the operation of security cameras at convenience stores and amending Section 1.08 to establish a bail deposit schedule for violation of this ordinance.

**Body**

DRAFTER'S ANALYSIS: This ordinance requires all convenience stores to have security cameras. The ordinance further requires minimum lighting for the use of security cameras. Under this ordinance, convenience stores are required to have security cameras that provide an overview of transaction counter and register area, a camera that captures an individual's face as they enter or exit the store and cameras at all fuel areas. The cameras must have an image quality of at least fifty pixels per foot and a recorded resolution of 1280 x 720. Convenience stores are required to record images at a rate of at least fifteen frames per second and store the images captured on the cameras and be capable of duplication. The ordinance further requires a notice be posted at all entrances and exits informing individuals that they are being recorded. The ordinance also establishes a penalty and bail deposits for violations. This ordinance shall be effective six months after adoption. This second substitute corrects a typographical error, clarifies that all other ordinances regarding exterior lighting must be followed and provides clarification regarding the position of the security cameras.

\*\*\*\*\*

The Common Council of the City of Madison do hereby ordain as follows:  
Please see "2nd Substitute Body" in Attachments.

**LEGISTAR 49284 – 2<sup>nd</sup> Substitute Body**

DRAFTER'S ANALYSIS: This ordinance requires all convenience stores to have security cameras. The ordinance further requires minimum lighting for the use of security cameras. Under this ordinance, convenience stores are required to have security cameras that provide an overview of transaction counter and register area, a camera that captures an individual's face as they enter or exit the store and cameras at all fuel areas. The cameras must have an image quality of at least fifty pixels per foot and a recorded resolution of 1280 x 720. Convenience stores are required to record images at a rate of at least fifteen frames per second and store the images captured on the cameras and be capable of duplication. The ordinance further requires a notice be posted at all entrances and exits informing individuals that they are being recorded. The ordinance also establishes a penalty and bail deposits for violations. This ordinance shall be effective six months after adoption. This second substitute corrects a typographical error, clarifies that all other ordinances regarding exterior lighting must be followed and provides clarification regarding the position of the security cameras.

\*\*\*\*\*

The Common Council of the City of Madison do hereby ordain as follows:

1. Section 23.52 entitled "Security Cameras at Convenience Stores" of the Madison General Ordinances is created to read as follows:

**"23.52 SECURITY CAMERAS AT CONVENIENCE STORES.**

(1) Definitions.

"Convenience Store" shall mean an establishment where motor fuel products or other minor accessories are retailed directly to the public on the premises, in combination with the sale of items typically found in a convenience market or supermarket.

"Lighting" shall mean sufficient lighting to ensure that the security camera is able to produce discernable images, including imagery sufficient to identify persons.

"Security camera" shall mean a high resolution camera that can produce reproducible digital color images and shall display a date and time stamp on each image and that has an image quality of at least fifty (50) pixels per foot and a recorded resolution of 1280 x 720.

(2) All owners of convenience stores shall maintain and operate security cameras during all hours the convenience store is open to customers. Subject to all other ordinances regulating lighting, owners of convenience stores must maintain adequate lighting to ensure that the security camera captures a clear, identifiable image. Security cameras shall be located at all of the following locations:

- (a) At least one security camera shall be positioned to capture an overview of each transaction counter and register area;
- (b) At least one security camera shall be positioned to capture a clear, identifiable full-frame image of an individual's face as they enter or exit the convenience store; and
- (c) At least one security camera shall be positioned to capture the general area surrounding any fuel area to capture an image which identifies the operator and the vehicle.

(3) Storage and Preservation of Records. All digital video records from security cameras must be recorded at a rate of at least fifteen (15) frames per second and stored and maintained in good viewing order for fifteen (15) days after capturing an image. The digital video recorder must be capable of exporting exact duplicates of their recordings to a standard removable media format (e.g. CD, DVD, Flash Drive). When requested by the Madison Police Department, the convenience store owner shall insure that requested record is stored and maintained adequately until retrieved by the Madison Police Department. The convenience store owner shall insure that they are adequate staff trained in the retrieval of digital video records to appropriately respond to a request for said record.

- (4) Notice. All convenience store owners shall conspicuously post a sign at all entrances and exits (excluding emergency exits and employee-only entrances). The sign must contain at least the following language, in lettering that shall be bold and a minimum of two (2) inches in height:

VIDEO RECORDING EQUIPMENT IN USE. YOU MAY BE RECORDED

- (5) Penalty. Whoever violates any provision of this ordinance shall be subject to a penalty of not less than one hundred dollars (\$100) and not more than one thousand dollars (\$1000). Each and every day that a violation exists shall constitute a separate offense.”

2. Subdivision (a) of Subsection (3) entitled “Schedule of Deposits” of Section 1.08 entitled “Issuance of Citations for Violations of Certain Ordinances and Providing a Schedule of Cash Deposits” of the Madison General Ordinances is amended by creating and amending therein the following:

<u>“Offense</u>	<u>Ord. No./Adopted Statute No.</u>	<u>Deposit</u>
Security cameras in convenience stores.	23.52	\$200, 1st \$500, 2nd \$750, 3rd & sub.”

3. This ordinance shall be effective six months after adoption.

EDITOR’S NOTE: New bail deposits must be approved by the Municipal Judge prior to adoption. This deposit has been so approved.

**SUBJECT: APPROPRIATE USE OF COMPUTER NETWORK RESOURCES**

Purpose: The City of Madison computer network provides mission critical application, telephone, data, and storage services to first responders and all other City agencies. These network resources have become an invaluable asset which must be protected and managed to ensure that they are secure, reliable, maintainable and supportable.

Policy: The use of computer network resources including the Internet and/or e-mail, whether in-house or external, for any of the following purposes is strictly prohibited:

1. To create or transmit material which is designed or likely to threaten, disturb, intimidate or otherwise annoy or offend another, including, but not limited to, broadcasting unsolicited messages or sending unwanted mail after being advised it is unwanted.
2. To create or transmit defamatory material.
3. Using the enterprise City e-mail system to transmit material to "all e-mail users" or mass distribution of non-work related material without prior approval from a department or division head.
4. To gain unauthorized access, including the use of hacking or packet sniffing software, to facilities or services on the City network or to use such facilities or services in an unauthorized manner.
5. To conduct business or engage in any "for profit" communications or activities.
6. To access, view or obtain any "adult entertainment," pornographic or obscene material, unless it is for work-related investigatory purposes and with the approval of the department head.
7. For political campaign purposes, including, but not limited to, using e-mail to circulate advertising for political candidates or relating to political campaign issues.
8. Sharing your network credentials (login ID and password) with anyone, with the exception of your supervisor.
9. Downloading software from the Internet to City PCs without authorization from Information Technology (IT).
10. Placing one's City-issued Internet e-mail address on any Internet-related service for other than business purposes. If an employee becomes aware that his/her City-issued Internet e-mail address is on a non-business related service, he/she should promptly request that it be removed and/or unsubscribe.
11. Opening attachments or clicking on embedded links contained in e-mail from unknown sources.
12. To gain commercial or personal profit or advantage, including, but not limited to, selling lists of names, addresses, telephone numbers or other information generated from City files.
13. To create or transmit material in violation of APM 3-5.
14. To represent oneself directly or indirectly as conducting City business when using such equipment for incidental personal purposes.
15. Creation of web pages, without the approval of IT, that purports to officially represent the City of Madison, personal or otherwise, regardless upon what server they may reside.
16. To print lengthy documents except for business purposes.
17. To use the Internet and speakers or headsets for the purpose of listening to audio or viewing video unless it is for City business.
18. Attach any device, except via the City's public wireless network, to the City network including: servers, laptops, computers, monitors, printers, multi-function devices, scanners, telephones, mobile computing devices, surveillance cameras, wireless routers, switches, hubs, or any other networking devices without the formal approval of IT.
19. Affix non-business related political and/or decorative stickers, banners, or other substances of any nature to the surfaces of any City-owned computer network resources.
20. Use of social media in violation of APM 3-16.
21. Unauthorized distribution of confidential or sensitive information, including the use of Internet-based storage facilities, personal computing devices, external storage media or cameras to take pictures or make copies of sensitive materials.
22. Unauthorized use or viewing of City-owned surveillance cameras in violation of APM 3-17.
23. For any purpose which would be a violation of any City work rules, City ordinance, City APM, state law or federal law.

All IT-related equipment and software purchases, including software as a service, must be approved by the IT Director. Software to be installed or used on the City network must be properly licensed and proof of this licensing must be available. (See Attachment A.)

Although occasional and limited personal use of computers is permitted, it is subject to the limitations, conditions, and regulations contained in this APM. Use of computer resources for incidental personal purposes is a privilege and can be withdrawn by a supervisor at any time. Employees may not use IT resources in any way that:

1. Directly or indirectly interferes with City operations of computing facilities or e-mail services.
2. Is contrary to or damages the City's interest.
3. Interferes with the employee's work duties, performance or other obligations to the City. Examples include, but are not limited to, excessive use of games, surfing the net, etc.

All network hardware is the property of the City of Madison. Purchase and disposal of all electronic devices must be in compliance with APM 4-7.

Access to electronic mail (e-mail), both internal and Internet, and access to the World Wide Web is only granted by approval of the agency head. Connecting any City-owned device directly to the Internet or to any other external computer system, without approval of IT, is prohibited. E-mail messages from unknown sources may contain malware and should either be deleted immediately or opened with caution. Transmission of sensitive information via the City's e-mail system must use the secure encryption feature of the system.

Unless specifically exempted by MGO 3.70, information stored in any automated format is considered to be a public record and will be retained according to local, state, or federal statute.

Employees are required to follow all Network Security Policies and Procedures. (See Attachment B.)

Failure by a City employee to comply with these policies may result in disciplinary action up to and including termination of employment.

Authority: Information Technology Director

  
Paul R. Soglin  
Mayor

APM No. 3-9  
August 26, 2015

Original APM dated 1/18/1996  
(Revised 11/8/1999)

**SUBJECT: USE OF SURVEILLANCE CAMERAS**

Purpose: City of Madison agencies have identified a wide variety of legitimate business reasons to use surveillance cameras. The primary purpose of this policy is to protect the privacy rights of the public and the associational/collective action rights of City employees. This policy promotes security for the public and for City employees through timely surveillance of areas otherwise difficult to monitor.

Responsibilities:

*Department of Information Technology (IT)*

Shall design, acquire, manage and maintain the network infrastructure to support a City-wide enterprise surveillance camera system. IT shall, in accordance with APM 4-7 (Policy for the Procurement and Disposal of Electronic Products), assist agencies in obtaining surveillance systems that meets the agency's technical requirements and complies with the City's enterprise system technological standards and policies.

IT shall manage network connectivity issues, coordinate problem remediation, maintenance and replacement of devices connected to the enterprise camera system. Agencies that have their own IT and/or facilities maintenance staff capable of maintaining camera devices may provide their own maintenance and problem remediation support.

IT shall ensure that the enterprise camera system is capable of complying with all Wisconsin Public Records Laws for the capturing, retention and timely production of public records.

*Department/Division Head Responsibility*

City agencies may develop their own surveillance camera programs to address the security issues. However, agencies shall not purchase, create or maintain their own independent surveillance camera systems but rather they shall work with IT.

Department/Division Heads must adopt a written surveillance camera policy on the use of surveillance cameras. Such written policy shall be on file and available to the public for review with the City Clerk within 30 days of implementation of the surveillance camera system (See Common Council Resolution RES-08-00863). The policy must be reviewed by the IT Director, the City Attorney and the Human Resources Director prior to its implementation.

*Owner Agencies*

The authorized security contacts for owner agencies may grant access to their surveillance cameras for others outside the owner agency. The authority to manipulate the cameras will be restricted to owner agencies, unless otherwise specified by the owner agency. Others may be provided view only permissions to specified surveillance cameras by the owner agency. Owner agencies are responsible for determining whether there is potential evidence of a law violation that was captured by their surveillance cameras, generate a police case number, and complete the form requesting preservation of evidence.

Agencies must provide Information Technology with at least 30 days advance notice of their intent to purchase cameras in order to afford adequate time to provision the network infrastructure required to support the new devices.

Agency policies must address the following considerations:

- The circumstances which necessitate the use of surveillance cameras;
- Whether the agency will utilize the City's standardized enterprise camera system and if not, specify business/technical reasons prohibiting such use;
- The personnel, by name or position, that will have access to either the cameras or the data recorded by such cameras;

- The circumstances under which such personnel will have access to either the cameras and/or the recorded data;
- Whether the cameras will be recording video or both audio and video;
- The physical location of cameras and a description of the areas to be observed by such cameras;
- The corresponding location and the verbiage of signage alerting persons that their actions are subject to audio-visual recording. Such signage shall be conspicuous and shall clearly inform all persons that their actions are being both audibly and visually recorded;
- Unless otherwise prohibited by law, the Madison Police Department will be provided with immediate access to all data or recordings that may constitute evidence of a crime. The Madison Police Department shall determine, in consultation with the Dane County District Attorney's Office, whether to obtain a warrant to take custody of such data or recording;
- The time period that recorded audio/video will be retained and available. No retention period of less than fourteen days may be approved under this policy;
- Procedures for ensuring that records are not destroyed during the pendency of any public records request, investigation or civil/criminal litigation.

Every agency policy shall comply and each use of surveillance cameras shall comply with the Fourth Amendment to the United States Constitution and Article 1, Section 11 of the Wisconsin Constitution. Furthermore, agencies shall comply with the requirements of sec. 968.31, Wis. Stats. This requires close consultation with the Office of the City Attorney.

Each agency policy shall address any laws unique to that agency. For example, the Library's policy shall reflect consideration of sec. 43.30(5)(a), Wis. Stats. concerning the disclosure of library patron identities.

Every policy shall address the implications of any applicable collective bargaining agreement. Compliance with this provision requires close consultation with the Labor Relations Unit of Human Resources.

Agencies shall be responsible for the costs of procuring and operating the surveillance cameras they employ. Agencies shall use their budgeted funds to purchase all new camera devices, equipment, licenses, and services required to install and connect (fiber-optics, point-to-point radios, or any other network connectivity technologies) the devices to the enterprise camera system.

All enterprise cameras located in the street right-of-way will be owned by Traffic Engineering. Traffic Engineering shall provide maintenance and remediation support for cameras located in the street right-of-way.

Authority: Information Technology will interpret and maintain this APM.

  
Paul R. Soglin  
Mayor

APM No. 3-17  
December 13, 2012

Original APM dated 12/13/2012



**An Act To Promote Transparency and Protect Civil Rights and Civil Liberties  
With Respect to Surveillance Technology**

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology.

**Comment [A1]:** NOTE TO LOCALITIES:  
Throughout the document, make sure the proper name for your local legislative body is used. For Counties, "City" will also need to be replaced with "County" throughout.

WHEREAS, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution.

**Comment [A2]:** NOTE TO LOCALITIES:  
Consider adding references to relevant provisions of the State Constitution and/or City Charter here.

WHEREAS, the City Council finds that, while surveillance technology may threaten the privacy of all of us, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

WHEREAS, the City Council finds that decisions regarding if and how surveillance technologies should be funded, acquired, or used, and whether data from such technologies should be shared, should not be made until meaningful public input has been solicited and given significant weight.

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed; and

WHEREAS, the City Council finds that, if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

THEREFORE BE IT RESOLVED, that the City Council adopts the following:

**Section 1. City Council Approval Mandatory for Surveillance Technology Funding, Acquisition, or Use**

(A) A municipal entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public City Council hearing at which the public is afforded a fair and adequate opportunity to provide online, written and oral testimony, prior to engaging in any of the following:

- (1) Seeking funds for new surveillance technology, including but not limited to applying for a grant, or soliciting or accepting state or federal funds or in-kind or other donations;
- (2) Acquiring or borrowing new surveillance technology, whether or not that acquisition is made through the exchange of monies or other consideration;

- (3) Using new or existing surveillance technology for a purpose or in a manner not previously approved by the City Council in accordance with this Act, including the sharing of surveillance data therefrom; or
- (4) Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share or otherwise use surveillance technology or surveillance data.

**Section 2. Surveillance Impact Report and Surveillance Use Policy Submission**

- (A) As a part of the process of seeking City Council approval, pursuant to Section 1(A), to fund, acquire, or use surveillance technology or to enter into an agreement concerning such funding, acquisition, or use, a municipal entity shall submit to the City Council and make publicly available a Surveillance Impact Report and Surveillance Use Policy concerning the technology at issue.
- (1) No use of surveillance technology by a municipal entity pursuant to Section 1(A) shall be permitted without the City Council's express approval of the related Surveillance Impact Report and Surveillance Use Policy submitted by the municipal entity pursuant to Section 2(A).
  - (2) Prior to approving or rejecting a Surveillance Impact Report or Surveillance Use Policy submitted pursuant to Section 2(A), the City Council may request revisions be made by the submitting municipal entity.
- (B) Surveillance Impact Report: A Surveillance Impact Report submitted pursuant to Section 2(A) shall be a publicly-released, legally enforceable written report that includes, at a minimum, the following:
- (1) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
  - (2) Information on the proposed purpose(s) of the surveillance technology;
  - (3) If the surveillance technology will not be uniformly deployed or targeted throughout the city, what factors will be used to determine where the technology is deployed or targeted;
  - (4) The fiscal impact of the surveillance technology; and
  - (5) An assessment identifying with specificity:
    - (a) Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and
    - (b) What specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts identified pursuant to Section 2(B)(5)(a).
- (C) Surveillance Use Policy: A Surveillance Use Policy submitted pursuant to Section 2(A) shall be a publicly-released, legally enforceable written policy governing the municipal entity's use of the surveillance technology that, at a minimum, includes and addresses the following:
- (1) Purpose: What specific purpose(s) the surveillance technology is intended to advance.
  - (2) Authorized Use: For what specific capabilities and uses of the surveillance technology is authorization being sought, and

- (a) What legal and procedural rules will govern each authorized use;
  - (b) What potential uses of the surveillance technology will be expressly prohibited, such as the warrantless surveillance of public events and gatherings; and
  - (c) How and under what circumstances will surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology be analyzed and reviewed.
- (3) Data Collection:
- (a) What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology;
  - (b) What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and
  - (c) How inadvertently collected surveillance data will be expeditiously identified and deleted.
- (4) Data Protection: What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.
- (5) Data Retention: Insofar as the privacy of the public can be severely compromised by the long-term storage of mass surveillance data, what rules and procedures will govern the retention of surveillance data, including those governing:
- (a) For what limited time period, if any, surveillance data will be retained. Such information shall include a statement explaining why the designated retention period is no greater than that which is absolutely necessary to achieve the specific purpose(s) enumerated in the Surveillance Use Policy;
  - (b) What specific conditions must be met to retain surveillance data beyond the retention period stated in Section 2(C)(5)(a);
  - (c) By what process surveillance data will be regularly deleted after the retention period stated in Section 2(C)(5)(a) elapses and what auditing procedures will be implemented to ensure data is not improperly retained;
- (6) Surveillance Data Sharing: If a municipal entity is seeking authorization to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, it shall detail:
- (a) How it will require that the collection, retention, and storage of surveillance data be conducted in compliance with the principles set forth in 28 C.F.R. Part 23, including but not limited to 28 C.F.R. Part 23.20(a), which states that a government entity operating a surveillance program “shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.”

- (b) Which governmental agencies, departments, bureaus, divisions, or units will be approved for (i) surveillance technology sharing, and for (ii) surveillance data sharing;
  - (c) How such sharing is necessary for the stated purpose and use of the surveillance technology;
  - (d) How it will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable Surveillance Use Policy and does not further disclose the surveillance data to unauthorized persons and entities; and
  - (e) What processes will be used to seek approval of future surveillance technology or surveillance data sharing agreements from the municipal entity and City Council.
- (7) Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.
- (8) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use Policy is followed, including what independent persons or entities will be given oversight authority, and what legally enforceable sanctions will be put in place for violations of the policy.
- (9) Complaints: What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and how the municipal entity will ensure each question and complaint is responded to in a timely manner.

### **Section 3. Review of Preexisting Uses Mandatory**

No later than one hundred twenty (120) days following the effective date of this Act, any municipal entity seeking to continue the use of any surveillance technology that was in use prior to the effective date of this Act, or the sharing of surveillance data therefrom, must commence a City Council approval process in accordance with Section 1(A)(3). If the City Council has not approved the continuing use of the surveillance technology, including the Surveillance Impact Report and Surveillance Use Policy submitted pursuant to Section 2(A), within one hundred eighty (180) days of their submission to the City Council, the municipal entity shall cease its use of the surveillance technology and the sharing of surveillance data therefrom until such time as City Council approval is obtained in accordance with this Act.

### **Section 4. Lead Entity Identification**

If more than one municipal entity will have access to the surveillance technology or surveillance data, a lead municipal entity shall be identified. The lead municipal entity shall be responsible for maintaining the surveillance technology and ensuring compliance with all related laws, regulations and protocols.

### **Section 5. Standard for Approval**

The City Council shall only approve a request to fund, acquire, or use a surveillance technology if it determines the benefits of the surveillance technology outweigh its costs, that the proposal will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact

on any community or group. To assist the public in participating in such an analysis, all approved Surveillance Impacts Reports and Surveillance Use Policies shall be made available to the public, at a designated page on the relevant municipal entity's public website, for as long as the related surveillance technology remains in use. An approval for the funding, acquisition and/or use of a surveillance technology by the City Council, where the risk of potential adverse impacts on civil rights or civil liberties has been identified in the Surveillance Impact Report pursuant to 2(B)(5)(a), shall not be interpreted as an acquiescence to such impacts, but rather as an acknowledgement that a risk of such impacts exists and must be proactively avoided.

### **Section 6. Annual Surveillance Report**

(A) A municipal entity that obtains approval for the use of a surveillance technology must submit to the City Council, and make available on its public website, an Annual Surveillance Report for each specific surveillance technology used by the municipal entity within twelve (12) months of City Council approval, and annually thereafter on or before March 15. The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:

- (1) A summary of how the surveillance technology was used;
- (2) Whether and how often collected surveillance data was shared with any external persons or entities, the name(s) of any recipient person or entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
- (3) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau. For each census tract, the municipal entity shall report how many individual days the surveillance technology was deployed and what percentage of those daily-reported deployments were subject to (A) a warrant, and (B) a non-warrant form of court authorization;
- (4) Where applicable, and with the greatest precision that is reasonably practicable, the amount of time the surveillance technology was used to monitor Internet activity, the number of people affected, and what percentage of the reported monitoring was subject to (A) a warrant, and (B) a non-warrant form of court authorization;
- (5) A summary of complaints or concerns that were received about the surveillance technology;
- (6) The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
- (7) An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology may have had on the public's civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendment to the United States Constitution; and
- (8) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

**Comment [A3]:** NOTE TO LOCALITIES:  
Considerer adding references to relevant provisions of the State Constitution and/or City Charter here.

- (B) Within thirty (30) days of submitting and publicly releasing an Annual Surveillance Report pursuant to Section 6(A), the municipal agency shall hold one or more well-publicized and conveniently located community engagement meetings at which the general public is invited to discuss and ask questions regarding the Annual Surveillance Report and the municipal agency's use of surveillance technologies.
- (C) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether each surveillance technology identified in response to Section 6(A), as used by the report-submitting entity, has met the standard for approval set forth in Section 5. If it has not, the City Council shall direct the use of the surveillance technology be discontinued or shall require modifications to the Surveillance Use Policy that will resolve the observed failures.

### **Section 7. Annual Public Reporting**

Not later than April 15 of each year, the City Council or its appointed designee shall release an annual public report, in print and on its public website, containing the following information for the proceeding calendar year:

- (A) The number of requests for approval submitted to the City Council under this Act for the funding, acquisition, or new use of surveillance technology;
- (B) The number of times the City Council approved requests submitted under this Act for the funding, acquisition, or new use of surveillance technology;
- (C) The number of times the City Council rejected requests submitted under this Act for the funding, acquisition, or new use of surveillance technology;
- (D) The number of times the City Council requested modifications be made to Surveillance Impact Reports and Surveillance Use Policies before approving the funding, acquisition, or new use of surveillance technology; and
- (E) All Annual Surveillance Reports submitted pursuant to Section 6. Printed copies of the public report may contain pinpoint references to online locations where the Annual Surveillance Reports are located, in lieu of reprinting the full reports.

### **Section 8. Community Advisory Committee on Surveillance**

- (A) Within three (3) months of the adoption of this Act, the City Council shall appoint a Community Advisory Committee on Surveillance to provide the City Council with broad principles to help guide decisions about if and how surveillance technologies should be used by the City and its municipal agencies.
  - (1) The membership of the Community Advisory Committee on Surveillance should reflect the diversity of the City's residents, and special efforts should be made to ensure communities that have historically been disproportionately subjected to government surveillance are well-represented.
  - (2) The Community Advisory Committee on Surveillance shall have a Chair and Vice Chair, who shall be elected annually by the members of the Committee.

- (B) Every year, by no later than September 15, the Community Advisory Committee on Surveillance shall produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance, which shall address, at a minimum, the following:
- (1) What communities and groups in the City, if any, are disproportionately impacted by the use of surveillance technologies, what disparities were perceived and/or experienced, and what were the resulting adverse impacts on the community's or group's civil rights and/or civil liberties;
  - (2) With respect to each perceived or experienced disparity identified in response to Section 8(B)(1), what remedial adjustments to laws and policies, including but not limited to prior approvals granted pursuant to Section 1(A), should be made so as to achieve a more just and equitable outcome in the future.
  - (3) With respect to each remedial adjustment identified in response to Section 8(B)(2), what additional funding, implementation strategies, and/or accountability mechanisms would be needed to effectuate the adjustment; and
  - (4) In light of the collective responses to Section 8(B)(1)-(3), what new approaches and considerations should the City Council bring to future reviews of applications submitted pursuant to Section 1(A).

**Section 9. Remedies; Penalties; Whistleblower Protections.**

- (A) Any violation of this Act, including but not limited to funding, acquiring, or utilizing surveillance technology that has not been approved pursuant to this Act or utilizing surveillance technology in a manner or for a purpose that has not been approved pursuant to this Act, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, writ of mandate, or evidence suppression in any court of competent jurisdiction to enforce this Act.
- (B) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought to enforce this Act.
- (C) Municipal employees or agents, except in response to a declared municipal, state, or federal state of emergency, shall not use any surveillance technology except in a manner consistent with policies approved pursuant to the terms of this Act, and may in no circumstances utilize surveillance technology in a manner which is discriminatory, viewpoint-based, or violates the City Charter, State Constitution, or United States Constitution.
- (D) Any person who knowingly violates this Act shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$2,500 per violation, imprisonment of not more than six months, or both.
- (E) Whistleblower protections.
- (1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or

**Comment [A4]:** NOTE TO LOCALITIES: Insert proper name if "City Charter" is not the name used by your city.

civil or criminal liability, because the employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Act.

**Section 10. Conflicting Contractual Agreements Prohibited**

It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Act, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Act shall be deemed void and legally unenforceable to the extent permitted by law.

**Section 11. Certain Public-Private Contracts Prohibited**

It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that facilitates the receipt of privately generated and owned surveillance data from, or provision of government generated and owned surveillance data to any non-governmental entity in exchange for any monetary or any other form of consideration from any source, including the assessment of any additional fees, interest, or surcharges on unpaid fines or debts. Any contracts or agreements signed prior to the enactment of this Act that violate this section shall be terminated as soon as is legally permissible.

**Section 12. Definitions**

For the purposes of this Act:

- (A) “Discriminatory” shall mean (1) disparate treatment of any individual(s) because of any real or perceived traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the **State of XXX**, or the **City Charter** or any law of the **City of YYY**, or because of their association with such individual(s), or (2) disparate impact on any such individual(s) having traits, characteristics, or status as described in subsection (1).
- (B) “Disparate impact” shall mean an adverse effect that is disproportionately experienced by individual(s) having any traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the **State of XXX**, or the **City Charter** or any law of the **City of YYY** than by similarly situated individual(s) not having such traits, characteristics, or status.
- (C) “Municipal entity” shall mean any municipal government, agency, department, bureau, division, or unit of this City.
- (D) “Surveillance data” shall mean any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance technology.
- (E) “Surveillance technology” shall mean any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing,

**Comment [A5]:** NOTE TO LOCALITIES: Insert state name here.

**Comment [A6]:** NOTE TO LOCALITIES: Insert proper name if “City Charter” is not the name used by your city.

**Comment [A7]:** NOTE TO LOCALITIES: Insert city name here.

**Comment [A8]:** NOTE TO LOCALITIES: Insert state name here.

**Comment [A9]:** NOTE TO LOCALITIES: Insert proper name if “City Charter” is not the name used by your city.

**Comment [A10]:** NOTE TO LOCALITIES: Insert city name here.

monitoring, or sharing audio, visual, digital, location, thermal, biometric, behavioral, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

(1) “Surveillance technology” includes, but is not limited to: (a) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (b) automatic license plate readers; (c) electronic toll readers; (d) closed-circuit television cameras; (e) biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; (f) mobile DNA capture technology; (g) gunshot detection and location hardware and services; (h) x-ray vans; (i) video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; (j) surveillance enabled or capable lightbulbs or light fixtures; (k) tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network; (l) social media monitoring software; (m) through-the-wall radar or similar imaging technology, (n) passive scanners of radio networks, (o) long-range Bluetooth and other wireless-scanning devices, (p) radio-frequency I.D. (RFID) scanners, and (q) software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software. The enumeration of surveillance technology examples in this subsection shall not be interpreted as an endorsement or approval of their use by any municipal entity.

(2) “Surveillance technology” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 12(E): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or surveillance-related functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) municipal agency databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology; and (f) manually-operated technological devices that are used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems.

(F) “Viewpoint-based” shall mean targeted at any community or group or its members because of their exercise of rights protected under the First Amendment of the United States Constitution.

### **Section 13. Severability**

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person or circumstance, is held invalid, the remainder of this Act, including the application of

*October 2018*

such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

**Section 14. Effective Date**

This Act shall take effect on [DATE].

---

REPORT OF: President's Work Group on Police and Community Relations

TITLE: Recommendations on Police Policies and Procedures

DATE: May 12, 2017

---

## Introduction

The Common Council Organizational Committee<sup>1</sup> Subcommittee on Police and Community Relations (the Subcommittee) held its first meeting on September 14, 2016 and confirmed the following objectives:

- a) Provide a forum for residents and members of the Common Council to discuss police and community goals, priorities and interactions. Build a deeper understanding of policing for elected officials and members of the public; and,
- b) Explore models and options from other communities related to policing and other police policies; and,
- c) Provide a forum for information sharing regarding police training, policies, data and trends including detailed presentations from the Madison Police Department (MPD) related to policing; and,
- d) Make recommendations to the Common Council on short-term policy, procedure and training while waiting for the results of the Madison Police Department Policy and Procedure Review Ad Hoc Committee (Ad Hoc Committee).

Common Council President Marsha Rummel chairs the Subcommittee and Ald. Shiva Bidar-Sielaff serves as vice chair. Ald. Rebecca Kemble, Ald. Sheri Carter and Ald. Denise DeMarb are members of the Subcommittee. The April election required the Subcommittee to conclude its efforts, despite the fact that the report to Common Council had not been finalized. On April 18, 2017 the Subcommittee was reconstituted as the President's Work Group on Police and Community Relations with the same membership and charge. The remainder of this memo utilizes the name of President's Work Group rather than Subcommittee.

---

<sup>1</sup> In April of 2017, the name of the Common Council Organizational Committee was changed to the Common Council Executive Committee.

## Overview of Activities

The President's Work Group has received several presentations from experts on policing, including the following:

### Internal Investigations and Discipline

On Monday, October 17, 2016, Capt. James Wheeler and Sgt. Erik Fuhreman presented information on the Madison Police Department (MPD) investigation and discipline process. The officers detailed the process MPD uses to conduct investigations of police misconduct. The vast majority of investigations are handled internally under the leadership of Professional Standards/Internal Affairs (PS/IA). PS/IA is staffed with two officers who rotate into that position for a period of two years.

On occasion, the Chief may conduct special investigations utilizing other departments, such as the Dane County Sheriff. Under Wis. Stats. § 175.47(3) investigations of officer involved deaths must be conducted by at least one investigator that is not employed by MPD. To date all officer-involved fatalities have been investigated by the Wisconsin Department of Criminal Investigation. Wis. Stats. § 175.47(3)(c) permits MPD to conduct an internal review of the incident to determine whether there were any policy violations and whether any discipline should occur. MPD compiles summary information regarding sustained complaints that resulted in discipline in a quarterly report to the Police and Fire Commission. The reports include a final disposition of complaints. However, other information, such as the number of complaints deemed 'non-sustained,' is not readily available to the public.

### Legal Authority of the Common Council Related to the MPD

On Wednesday, November 9, 2016, City Attorney Michael May and Assistant City Attorney Marci Paulsen presented information regarding the division of legal authority between the Police Chief, the Mayor and the Common Council in the operation of the police department. Analysts have identified this issue as an area of overlapping authority, which is not resolved by case law or statutes.<sup>2</sup>

Wisconsin State Statute §62.09(13)(a) states that the chief of police "has the command of the police force" and that command is "under the direction of the mayor." Wis. Stat §62.09(13)(a) also affirms that the police chief must follow the lawful orders of the Mayor or the Common Council.

(a) The chief of police shall have command of the police force of the city, or the chief of a combined protective services department created under s. 62.13 (2e) (a) 1. shall have command of the combined protective services force, under the direction of the mayor. The chief shall obey all lawful written orders of the mayor or common council.<sup>3</sup>

These various authorities are further informed by Wis. Stat §62.11(5) which details the power of the common council to control the affairs of the city and to act for the health, safety and welfare of the public.

---

<sup>2</sup> Flynn, Matthew J., Police Accountability in Wisconsin. Wisconsin Law Review. Vol. 1974: p. 1131-1166.

Moore, David. Authority of Common Council to Make Changes to the City Police Department's Use-of-Force Policy. Memorandum to Representative Chris Taylor from the Wisconsin Legislative Council. October 26, 2016.

<sup>3</sup> Emphasis added.

Except as elsewhere in the statutes specifically provided, the council shall have the management and control of the city property, finances, highways, navigable waters, and the public service, and shall have power to act for the government and good order of the city, for its commercial benefit, and for the health, safety, and welfare of the public,<sup>4</sup> and may carry out its powers by license, regulation, suppression, borrowing of money, tax levy, appropriation, fine, imprisonment, confiscation, and other necessary or convenient means.

Addressing these overlapping authorities with a specific example, the City Attorney referenced a report concerning the legal authority of the Common Council to prevent MPD from utilizing tasers. The report to the Mayor and the Common Council dated April 7, 2005 explains that “[t]here is nothing in the law that prohibits the Mayor and Common Council, by means of an adopted resolution, from requesting that the Police Department cease engaging in a particular practice. The Police Chief is then free to consider such request and exercise his discretion to accept or reject it based upon his assessment of its wisdom, usefulness, practicality, hazard and other such relevant criteria.” The report goes on to explain that these are not simple questions.

The report concluded with the statement that Common Council likely has the authority to adopt a resolution prohibiting the use of tasers, nevertheless there are legal reservations. “Having the Council interject itself into areas which call for technical law enforcement expertise ... may not ultimately be the most prudent and safest course of action for officers and citizens alike. However, the Council’s authority is not limited merely to those actions which outsiders might believe are wise or correct—otherwise its jurisdiction would be unnaturally narrowed indeed.”

#### **Implementation of the United Way/MPD Task Force Report on Use of Force**

On November 21, 2016, Capt. Kristen Roman presented information about the 2016 *Special Community/Police Task Force Recommendations Regarding Police ‘Use of Force.’* The United Way of Dane County, the Dane County Chiefs of Police Association and the Dane County Branch of the NAACP issued the report. The City of Madison and MPD contributed to the development of the report and recommendations.

Since the publication of the Report in February of 2016, MPD has implemented some of the recommendations including creating a new Use of Force Coordinator position to track all use of force incidents and provide regular reporting to the Chief on these incidents. Sgt. Kimba Tieu is the new Coordinator and he presented to the President’s Work Group at a later date. Additionally, MPD acquired new software, IA Pro, which provides data management for internal investigations. The Department also developed a new foot pursuit policy and a new Standard Operating Procedure (SOP) on de-escalation.

#### **Use of Force Policies from Other Communities**

On December 13, 2016, State Representative Chris Taylor presented her research regarding best practices from other communities and her planned legislative proposals to change use of force policies across WI. She highlighted several principles found in policies and procedures from other communities that she deemed important for Wisconsin communities. Representative Taylor highlighted the following principles:

---

<sup>4</sup> Emphasis added.

- *A duty to preserve life* is included as part of NYPD policy. The MPD policy recognizes the “value of life” but does not affirm a duty to preserve life.
- *Deadly force as a last resort* is part of the Department of Justice guidelines. The U.S. DOJ guidelines say that deadly force is reasonable when all other means have failed or would be likely to fail. Madison’s deadly force policy says that such force is authorized when “an officer reasonably believes a lesser degree of force would be insufficient.”
- *The principle of proportionality* is the requirement to only respond at the level of threat. This principle is not included in MPD’s use of force policies.
- *Tailored guidelines for managing resistant subjects who may be mentally ill or intoxicated.* NYPD has an extensive policy related to “emotionally disturbed persons” or EDPs. The NYPD policy provides guidelines for officers to assess, de-escalate, create safety zones, and “if the emotionally disturbed person is armed or violent, no attempt will be made to take the EDP into custody without the specific direction of a supervisor unless there is an immediate threat of physical harm to the EDP or others present.”<sup>5</sup>

### **A Proposal for Community Control of the Police**

On Monday, January 18, 2016, representatives of Freedom Inc., provided a presentation of their proposal regarding community control of the police. The proposal would restructure policing districts to reflect “existing social cohesion of neighborhoods and communities therein.” The residents of those districts would then vote on whether they would like to retain the existing police department or replace the department with a force controlled by district residents. New forces would be run by a Community Police Control Board with the power to establish policies and priorities. Members of the Control Board would be chosen randomly from the districts rather than elected or appointed. Freedom Inc. stated that this proposal is legally plausible under existing state statute § 62.13(2e) which “allows cities to forgo the traditional police department and accompanying board in favor of a Combined Protective Services department.”<sup>6</sup>

### **Surveillance Technologies and Policies**

Also on January 18, 2016, representatives from the ACLU provided a presentation on surveillance technologies and related policies. The ACLU shared information about new technologies related to video and audio surveillance, as well as GPS and drones now in use by some police departments. The ACLU provided a proposal for the City of Madison to consider clarifying rules related to the acquisition, purchase, and use of technology, as well as the management of surveillance technology and data.

### **Dane County’s Efforts to Reduce Disparities in Arrests**

On Thursday, February 16, 2017, Colleen Clark-Bernhard, Equity and Criminal Justice Council Coordinator, presented information on the initiatives from the Dane County Criminal Justice Council (CJC) to expand collaboration, data driven justice, and innovation. The CJC has focused on improving data management and capabilities as the foundation of their work and in 2016 hired a research analyst in the County Board Office to add analytical capacity to address issues of equity and transparency. Also in 2016, the CJC announced their partnership with the White House Data Driven Justice Initiative to use data to divert people with mental illness away from the criminal

---

<sup>5</sup> NYPD Patrol Guide Tactical Operations Procedure No: 221-12 Mentally Ill or Emotionally Disturbed Persons. Issued 06/01/2016.

<sup>6</sup> Freedom Inc. Community Control Over the Police Brochure.

<https://madison.legistar.com/View.ashx?M=F&ID=4970445&GUID=892D6EDB-7B83-4727-90AF-D35A1B70B570>

justice system and into community-based treatment. Additionally, Dane County is expanding the Community Restorative Court to all of Dane County. This is an existing area of collaboration with Madison and Dane County. As the CRC expands to serve more local residents Madison and Dane County will have the opportunity to strengthen their collaboration.

### **Weapons and Use of Force and Use of Deadly Force Policies at MPD**

On March 2, 2016 at a special meeting of the Common Council (not a meeting of the President's Work Group), Sgt. Kimba Tieu presented a demonstration of the tools in an officers' belt including a taser, baton, hobble restraints, pepper spray, shotguns with non-lethal rounds and handguns. Sgt. Kimba Tieu also answered questions regarding MPD's Use of Force policies and procedures. Sgt. Tieu explained that MPD believes that policing is done in partnership with the community. The use of force data is now available on the MPD website and Sgt. Tieu is responsible for the data as the Use of Force Coordinator. He is watching for trends in force tactics and analyzes whether officers are getting hurt using a particular type of force as well as the relative effectiveness of the tactics. When asked about specific scenarios and use of force Sgt. Kimba reiterated that officers are authorized to use force if they are acting "reasonably" given the totality of circumstances.

### **IA Pro Software (internal investigations software)**

On Monday, March 20, 2017, Lt. Amy Chamberlin and Assistant Chief Vic Wahl presented detailed information on the implementation of IA Pro Software and the plan to implement an Early Warning System utilizing the IA Pro Software to support internal investigations and personnel management. The program has been in place for one year and all complaints and all use of force data have been entered into the system since 1/1/2016. The use of force data is reviewed daily and the Chief is briefed every Monday about the data. Other data entered into the system includes information related to pursuits and squad crashes, as well as audit results related to squad cars, email and messages. IA Pro allows PS/IA the ability to monitor officers who are on probation or "work rules". IA Pro has a great deal more capability than is currently in use. PS/IA is looking at how best to utilize IA Pro to implement an Early Warning System.

### **Employee Assistance and Stress Management**

On Wednesday, April 12, 2017 Tresa Martinez, EAP Administrator and Lt. Kelly Donahue provided information on the types of services provided to MPD officers through the Employee Assistance Program, Peer Support Program, and Critical Incident Stress Management. The programs provide support for officers who experience trauma or stress, both on and off the job. The programs and participation have grown over the last twenty years. The MPD now helps to lead the programming and MPD culture is supportive of officers accessing these resources.

### **Neighborhood Associations Weigh In**

The President's Work Group has also reached out to neighborhood associations directly with a short survey. The goal of the survey was to better understand the types of cooperative activities neighborhood associations have with MPD and to learn more about existing neighborhood watch programs, as well as perceptions of public safety. Over 26 neighborhood associations responded. The most frequent public safety concerns cited were pedestrian safety and traffic/speeding issues, as well as petty theft from autos/garages at night. Other public safety concerns cited by more than one neighborhood included gun violence, vagrancy, home burglaries, vandalism, and drug violence/activity. Many neighborhood associations noted that they have frequent positive interactions with MPD, though few have certified neighborhood watch programs.

## Actions To Be Taken

The President's Work Group reviewed a wide range of subjects relating to community and police relations throughout the course of their work. The President's Work Group noted that some of the issues are most appropriate for action by the Ad Hoc Committee while other issues could be addressed directly to MPD or the Common Council.

### Safeguarding Emotionally Disturbed People

The majority of officer-involved shootings in the last three years in the City of Madison have involved a person with a mental health issue or an intoxicated person. The President's Work Group would appreciate further clarification of policies relating to people exhibiting signs of mental illness or intoxication who are resistant to medical assistance or arrest. The New York Police Department (NYPD) defines an Emotionally Disturbed Person (EDP) as "a person who appears to be mentally ill or temporarily deranged and is conducting himself in a manner which a police officer reasonably believes is likely to result in serious injury to himself or others."<sup>7</sup>

The MPD SOP on Mental Health Incidents/Crises<sup>8</sup> provides some degree of guidance related to this issue. The SOP describes the value in de-escalating crisis situations, the role of Mental Health Officers and the process to assess a person in crisis. However, the SOP does not detail tactics or procedures to de-escalate the situation or establish safety for all people in the area. A specific protocol is needed to clarify how an officer should interact with EDPs.

**Action Item 1:** The Common Council hereby issues a lawful order to the Chief of Police to issue a SOP that explicitly details the goals, tactics, policies, and procedures to deal with an EDP (including those who are intoxicated). In order to do so MPD should refer to the International Association of Chief of Police's model policy Responding to Persons Affected by Mental Illness or in Crisis (see Appendix) and the NYPD Patrol Guide related to Mentally Ill or Emotionally Disturbed Persons (see Appendix).

The President's Work Group requests that MPD consider incorporating Fyfe's principles for interacting with EDPs. Those principles include 1) keeping a safe distance, 2) avoiding unnecessary and provocative displays of force, 3) working with backup, 4) one officer should interact with the subject, others should remain quiet, 5) the officer interacting with the subject is in charge, no one else should take unplanned action, 6) make it clear officers are there to help not threaten, and finally, 7) officers should take as much time as necessary for an arrest, even hours or days if that is that is what is required.<sup>9</sup>

**Action Item 2:** The Common Council directs the Ad Hoc Committee to investigate other possible supports for MPD officers interacting with EDPs. EDPs include individuals whose behavior is altered as a result of intoxication caused by drugs or alcohol. The President's Work Group would encourage further exploration into the types of training and ongoing training strategies that will improve interactions with EDPs. In particular, the President's Work Group would recommend a

---

<sup>7</sup> NYPD Patrol Guide Mentally Ill or Emotionally Disturbed Persons. Tactical Operations Procedure No: 221-13. 06/01/2016.

<sup>8</sup> Effective Date 12/22/2016.

<sup>9</sup> Fyfe, James J. PhD. Policing the Emotionally Disturbed. Journal of American Academy of Psychiatry and the Law. 28:345-7, 2000.

detailed analysis of ProTraining<sup>10</sup> which is an evidence based practice proven to reduce overall use of physical force and the use of weapon force in police calls.<sup>11</sup> The President's Work Group would recommend the Ad Hoc Committee undertake an evaluation of the feasibility of hiring social workers to work with officers to support interactions with EDPs.

### Use of Force Policies

The President's Work Group found that the principles of de-escalation and the duty to intercede are included in certain MPD policies but are not incorporated into the MPD Use of Force and Use of Deadly Force SOPs. Incorporation of these principles into the Use of Force SOPs would clarify the duties of officers to put these principles into action especially in scenarios that may require force.

De-escalation tactics and techniques are actions used by officers which seek to minimize the likelihood of the need to use force during an incident. Officers shall attempt to slow down or stabilize the situation so that more time, options and resources are available for incident resolution. The duty to intercede is the principle that officers have a duty to stop other officers who are using excessive force and report them to a supervisor.

Additionally, the President's Work Group found that the MPD Use of Deadly Force SOP recognizes "the dignity of all people and the value of human life" which are important principles. However, other cities' policies utilize stronger language that clarifies an officer's "duty to preserve life." For example NYPD's policy includes the language, "The primary duty of all NYPD officers is to protect human life, including the lives of individuals being placed in police custody."<sup>12</sup>

The President's Work Group appreciated learning about other precautionary use of force principles found in some cities' policies. Those principles presented to the President's Work Group by Representative Chris Taylor included the previously addressed duty to preserve life, duty to intercede and the duty to de-escalate. Additionally, the President's Work Group would like to reiterate the importance of other precautionary principles including:

- Necessity: Deadly force should only be used as a last resort. The necessity to use deadly force arises when all other available means of preventing immediate and grave danger to officers or other persons have failed or would be likely to fail.
- Proportionality: When force is needed, the force used shall be in proportion to the threat posed.
- Reassessment: Officers shall reassess the situation after each discharge of their firearm.
- Totality of officer conduct: The reasonableness of an officer's use of force includes consideration of the officer's tactical conduct and decisions leading up to the use of

---

<sup>10</sup> Coleman, T. G. and D. Cotton (2014). "TEMPO: Police Interactions. A Report towards improving interaction between police and people living with mental health problems." Mental Health Commission of Canada.

<sup>11</sup> Frierson, R. L. (2013). "Commentary: Police Officers and Persons with Mental Illness." Journal of the American Academy of Psychiatry and the Law Online 41(3): 356-358.

<sup>12</sup> Adapted from NYPD Patrol Guide Tactical Operations Force Guidelines Procedure No. 221-01.

force. Police officers shall ensure their actions do not precipitate the use of deadly force by placing themselves or others in jeopardy by taking unnecessary, overly aggressive, or improper actions. It is often a tactically superior police procedure to withdraw, take cover or reposition, rather than the immediate use of force.

- Immediate threat: Deadly force is only authorized if the threat is immediate. A threshold of “immediate threat” reflects language in United States Supreme Court decisions. The latest model use of force policy published by the International Association of Chiefs of Police eliminates the term “imminent”.

**Action Item 3.** The Common Council hereby issues a lawful order to the Chief of Police to issue updated MPD Use of Force and the Use of Deadly Force SOPs that explicitly incorporate the duty to intercede and de-escalate which are already included in MPD's Code of Conduct and Core Values and the de-escalation SOP.

**Action Item 4.** The Common Council hereby issues a lawful order to the Chief of Police to incorporate language to emphasize an officer's duty to preserve life, including the lives of those being placed into police custody into the MPD Use of Force and the Use of Deadly Force SOPs.

**Action Item 5.** The Common Council directs the Ad Hoc Committee to evaluate the precautionary principles detailed above and determine whether and how they may be addressed in MPD policies, practices and procedures.

### **Ensuring Officer Well-Being**

Officers are regularly exposed to traumatic events at work. In addition, officers must be ever vigilant for life-threatening situations. These conditions can increase the risk for physical and mental illnesses such as PTSD, depression, alcohol and drug abuse and sleep disruptions. In an effort to support officer's physical and mental well being the MPD and the Center for Healthy Minds at the University of Wisconsin-Madison launched a successful pilot project to offer Mindfulness-Based Stress Reduction training.

**Action Item 6.** The Common Council hereby issues a lawful order to the Chief of Police to develop programming to build officers' mental health and resilience utilizing evidence based practices, which may include Mindfulness-Based Stress Reduction, and to provide cost estimates and a timeline for this work. The description of programming, timeline and cost-estimates shall be presented at the third quarter (September 2017) report to the Common Council (see Action Item 8).

### **Waiting for Backup**

Officers are at higher risk, and may be more likely to use deadly force because of that risk, when they engage alone in a potentially dangerous situation. Backup is a tactic employed by MPD to increase officer and public safety. Backup is assigned by dispatch to priority calls.

MPD's de-escalation SOP<sup>13</sup> highlights the importance of backup for safety. The policy states that backup is a strategy to decrease exposure to a potential threat. Also worthy of note, MPD's Use of Non-Deadly Force SOP<sup>14</sup> clarifies the value of backup to allow officers to utilize less lethal weapons. The policy states that if a subject is believed to be armed with a dangerous weapon an officer may not employ an electronic control device, also known as a taser, "unless another officer at the scene has the immediate ability to deliver deadly force. Officers armed with an ECD should continuously monitor and evaluate the ability of other officers present to deliver deadly force."<sup>15</sup> Therefore both MPD's de-escalation and less lethal force procedures demonstrate the value of backup to protect officers and the public.

Previously, MPD officers had the discretion to "call off" backup by telling dispatchers that they could handle the incident on their own. In September 30, 2016 Police Chief Koval issued an email to command staff and sergeants directing them to implement a new policy (effective October 3, 2016) that prevented officers from disregarding backup. In his email Koval noted that officers were calling off backup in an effort to address a large volume of calls quickly. But Chief Koval expressed concern that "'business efficiency' was trumping and potentially compromising officer/public safety."<sup>16</sup>

The language that became effective October 3, 2016 reads:

"Officers shall not disregard backup, if so assigned by dispatch. Additionally, officers shall wait for backup before physically approaching any involved subject(s), unless an officer reasonably believes there is a significant risk of bodily injury to any person(s).

Supervisors are expected to routinely monitor calls for service to ensure these guidelines and protocols are being followed. It is realized, however, that it may occasionally be necessary, when circumstances dictate, for a supervisor to direct a course of action outside of these guidelines."

The policy was intended to promote safety of officers and the public by both reducing the vulnerability of officers and reducing the need to utilize force against subjects.<sup>17</sup>

Portions of the October 2016 policy have since been rescinded, raising the concern that officers will once again have the discretion to disregard backup. MPD made the most recent change to address concerns from MPD officers regarding an inability to provide service at the scene of an incident once they had assessed it to be safe. The current MPD policy related to back-up states, "*Officers shall not disregard backup, if so assigned by dispatch, prior to arrival at the scene and assessment of the situation.*" This policy allows for officers to assess a scenario and call-off backup.

---

<sup>13</sup> Eff. Date 11/16/2016

<sup>14</sup> Eff. Date 05/26/2016

<sup>15</sup> MPD's Use of Non-Deadly Force Standard Operating Procedure. Eff. Date 05/26/2016.

<sup>16</sup> Madison Police Officers No Longer Free to "Call Off" Backup. Lawofficer.com November 13, 2016 <http://lawofficer.com/special-assignment-teams/officer-safety/madison-police-officers-no-longer-free-to-call-off-backup/>

<sup>17</sup>Rivedal, Karen. Internal memos show Madison police officers no longer free to 'call off' backup. Wisconsin State Journal. Nov 13, 2016.

**Action Item 7.** The Common Council hereby issues a lawful order to the Chief of Police to develop a comprehensive backup policy that addresses the need to protect public safety and officer safety. The backup policy should incorporate the principles of de-escalation and judicious use of force, as described in the relevant SOPs. The backup policy should clearly define procedures to ensure officers request and wait for backup in specific relevant scenarios such as:

- When an officer anticipates a need to use force, but has an opportunity to retreat or is not facing immediate threat;
- When an officer is dealing with an EDP or a resistant intoxicated person;
- When backup is expected to arrive within a certain amount of time;
- When an incident involves violence or violence is anticipated;
- An occurrence involving the use, display or threatened use of a weapon;
- Domestic disputes;
- Areas where communications are known to be deficient; or
- Any occurrence involving a subject posing a threat to self or others.<sup>18</sup>

### **Communication with Common Council**

MPD and the Common Council could work together more closely if communication was enhanced. The President's Work Group found great value in the presentations from MPD relating to internal investigations, use of force, data analysis with IA Pro software and implementation of the community task force recommendations on use of force. The Common Council recognizes that MPD is a department that generates a high level of interest for members of the public and hopes that increased reporting will allow for greater understanding and transparency of the work of MPD.

**Action Item 8.** The Common Council hereby issues a lawful order to the Chief of Police to personally provide quarterly written and verbal updates to Common Council. The updates will be a regular agenda item at the Common Council and will include the following information: 1) any changes to the Code of Conduct or SOPs, 2) any changes in training, 3) any new initiatives, 4) MPD arrest data by reason for arrest and race/ethnicity, and 4) use of force incidents.

### **Surveillance Policies**

Surveillance technologies are rapidly expanding governmental capabilities to gather data on individuals. The City of Madison values the principles of transparency, oversight and accountability and seeks to ensure that residents' civil rights and civil liberties are protected even as the City utilizes surveillance technology to protect public safety. A comprehensive policy governing the purchase and use of surveillance technology is required to ensure these protections.

MPD does have a policy governing use of audio and video surveillance. However, the City of Madison does not yet have citywide surveillance policies. Departments outside of MPD may purchase their own surveillance equipment or utilize equipment borrowed from other departments; this usage is not governed by any existing framework. The proposed policies would address all City employees' and departments' purchase and use of surveillance equipment.

---

<sup>18</sup> Adapted from the Royal Canadian Mounted Police Operational Manual.

**Action Item 9:** The Common Council will develop a policy governing the purchase and use of all surveillance equipment employed by all City agencies including MPD. The policy will also address data management and storage as well as clear consequences for policy violations. The policy will include an inventory of all City of Madison surveillance equipment as of 12/2017, and the surveillance equipment inventory will be updated annually thereafter.

### Oversight of Internal Investigations

Oversight of internal investigations may take many forms. Two ideas presented here include an audit mechanism of internal investigations and external investigations of complaints.

As noted earlier, investigations into police misconduct are traditionally handled internally, however, all officer-involved deaths must be investigated independently as required by state statute. The majority of other Madison cases are handled internally by the MPD PS/IA.

Cities such as Portland, Los Angeles and Tucson utilize auditors outside of the police departments<sup>19</sup> to provide reviews and reports of the investigation process by their police departments and to provide recommendations on a regular basis. Such a system provides the benefits of external accountability at a minimal cost. The auditor would regularly review the process for submitting complaints, investigating and disposing of complaints. Such an auditor can help provide the public and elected officials with an impartial analysis of the department's handling of complaints.

Alternatively, the City may consider external investigations. Given the public interest surrounding policing and the public's frequent demand for independent investigations into misconduct, a policy which directs an external investigator to investigate certain complaints may enhance community trust. There is also a benefit to innocent officers when they are investigated externally. Officers declared innocent of the complaint charge by an external body are more likely to be considered innocent by the public, rather than those officers declared innocent by their own departments. External investigations may "help reassure a skeptical public that the department already investigates citizen complaints thoroughly and fairly."<sup>20</sup> Hiring an investigator to investigate complaints submitted to the Police and Fire Commission (PFC) would also provide an independent report on the facts of a case which may prove beneficial since the PFC does not conduct investigations.

**Action Item 10:** The Common Council directs the Ad Hoc Committee to provide a review of the feasibility of external oversight of MPD internal investigations.

---

<sup>19</sup> The Portland Auditor is tasked with reviewing investigations of police conduct as well as managing reviews for other city agencies. The Portland Auditor Mary Caballero is elected to her position and has a background in auditing performance management. <https://www.portlandoregon.gov/auditor/27392>. This is not staffed by former law enforcement.

The Tucson Independent Police Auditor is managed by a long-time city employee who previously investigated equal opportunity claims and has an investigator on staff. This is not staffed by former law enforcement.

<https://www.tucsonaz.gov/manager/independent-police-auditor-civilian-investigator>

The Los Angeles Audit Division was established in 2001 as a result of the Consent Decree and is now staffed by over 30 sworn officers and civilian professionals including CPAs, fraud examiners, and professional auditors.

[http://www.lapdonline.org/inside\\_the\\_lapd/content\\_basic\\_view/8772](http://www.lapdonline.org/inside_the_lapd/content_basic_view/8772)

<sup>20</sup> Peter Finn. Citizen Review of Police: Approaches and Implementation. U.S. Department of Justice. National Institute of Justice March 2001. NCJ 184430.

### **Early Intervention Warning System**

Early Warning Systems, also called Early Intervention Systems, are tools to monitor officers who are frequently the subject of citizen complaints or demonstrate behavioral issues. Early Warning Systems are becoming increasingly popular, as of 1999 the most recent survey on early warning systems, 39% of all police forces serving communities of more than 50,000 have a system in place or are planning to implement one.<sup>21</sup> MPD has purchased police data tracking system called IA Pro, which includes the capabilities of an Early Intervention Warning System. As the Department prepares to implement the early intervention program within IA Pro, it will be valuable to monitor the implementation and the use of the tool.

**Action Item 11:** The Common Council directs the Ad Hoc Committee to further explore the IA Pro capabilities for early warning and intervention. In addition, the President's Work Group recommends the Ad Hoc Committee speak with the University of Chicago Data Science for Social Good statisticians to explore collaboration to develop a predictive early warning system.

### **Thorough and Credible Root Cause Analysis**

The National Transportation Safety Board and many hospitals utilize root cause analysis processes to determine the factors that may have contributed to an adverse event such as a plane crash or an outbreak of disease. The purpose of root cause analysis is not to assign blame but to enable complex organizations to identify opportunities for improvement. The President's Work Group encourages the Ad Hoc Committee to consider the value of a root cause analysis process and protocol for MPD to examine critical incidents and broader trends.

Best practices for root cause analysis require that such analysis be both "thorough and credible". The Ad Hoc Committee should ensure it utilizes the specific criteria for "thorough and credible" as they apply to root cause analysis. For example criteria for a thorough root cause analysis would include the following elements 1) an analysis of the underlying symptoms, 2) determination of the factors and systems most directly related to the event under investigation, 3) identification of the risk points and their potential contributions to this type of event.<sup>22</sup> A root cause analysis process would require robust data analytics, which may be available through expansion of the IA Pro system or other data systems.

**Action Item 12:** The Common Council directs the Ad Hoc Committee to provide an implementation plan for a root cause analysis process at MPD.

### **Review the Ordinance and Revise the Charge of the Public Safety Review Committee**

The Public Safety Review Committee (PSRC) is a City of Madison Committee established to provide advice to the Mayor and Common Council related to public safety. The PSRC has the authority to "review and make recommendations concerning departmental budgets; review service priorities and capital budget priorities of the Police and Fire Departments; serve as liaison

---

<sup>21</sup> Shultz, Ashley. Early Warning Systems: What's New? What's Working. CNA Analysis & Solutions. December 2015. [https://www.cna.org/cna\\_files/pdf/CRM-2015-U-012182.pdf](https://www.cna.org/cna_files/pdf/CRM-2015-U-012182.pdf)

<sup>22</sup> Joint Commission Resources. Root Cause Analysis in Health Care: Tools and Techniques. 5th Edition. 2015. <http://www.jcrinc.com/assets/1/14/EBRCA15Sample.pdf>

between the community and the city on public safety issues; and review annually and make recommendations to the Common Council regarding the annual work plans and long-range goals of the departments.”<sup>23</sup>

The President’s Work Group discussed the important role the PSRC could play in ensuring that a permanent city committee regularly examines public safety issues, as well as police and community relations, and provides advice on these issues to the Mayor and the Common Council.

**Action Item 13:** The Common Council directs the Common Council Executive Committee to undertake a review of the role, membership and charges under ordinance(s) for the Public Safety Review Committee.

## Conclusion

The President’s Work Group achieved the objectives established in September 2016 and has created a series of actions to be taken up by the Common Council, the Chief of Police and the Ad Hoc Committee.

The President’s Work Group intends for those actions addressed to the Chief of Police and the Common Council to be implemented as soon as possible. The President’s Work Group also evaluated several other areas of interest related to the ongoing work of the Ad Hoc Committee and has crafted specific action items for those issues. These issues require a more in-depth analysis and familiarity with police policies and procedures for successful completion.

The President’s Work Group learned a great deal through its work and wishes to express its gratitude to the residents of Madison, the MPD, the Ad Hoc Committee and the Common Council for their participation and support of this effort.

---

<sup>23</sup> Madison General Ordinance Sec. 33.22

## APPENDIX

### Madison Police Oversight Committees

Madison Police and Fire Commission	Public Safety Review Committee	MPD Policy and Procedure Review Ad Hoc Committee	Common Council Executive Committee President's Work Group on Police and Community Relations
Permanent, established by WI Statute	Permanent, established by Common Council	Temporary, established by Common Council	Temporary, established by Common Council
Madison General Ordinance Sec. 33.06 and State Statutes 62.13 - Appoints the chief of each department; approves or disapproves promotions and supervision of the hiring process, with certification of an eligibility list and approval of those who are finally hired; holds hearings on disciplinary matters brought to its attention either directly or through appeal and imposes discipline if appropriate.	Madison General Ordinance Sec. 33.22 - The board shall be advisory to the mayor and Common Council to assist them in the performance of their statutory duties. The board may review and make recommendations concerning departmental budgets; review service priorities and capital budget priorities of the Police and Fire Departments; serve as liaison between the community and the city on public safety issues; and review annually and make recommendations to the Common Council regarding the annual work plans and long-range goals of the departments.	The Committee's objective is to complete a thorough review of the MPD's policies, procedures, culture and training using the consultant report, other resources and testimony. Creating resolution RES-15-00477, File ID# 37863; effective 5/21/2015	The President's Work Group's objective is to provide a forum for residents, to share information on Madison policies and procedures, to explore police policies and procedures from other communities, and to make short-term policy recommendations while waiting for the results of the MPD Policy and Procedure Review Ad Hoc Committee. Established 9/14/2016.



**RESPONDING TO PERSONS  
AFFECTED BY MENTAL ILLNESS  
OR IN CRISIS**

**Model Policy**

<i>Effective Date</i> January 2014		<i>Number</i>	
<i>Subject</i> Responding to Persons Affected by Mental Illness or in Crisis			
<i>Reference</i>		<i>Special Instructions</i>	
<i>Distribution</i>		<i>Reevaluation Date</i>	<i>No. Pages</i> 4

**I. PURPOSE**

It is the purpose of this policy to provide guidance to law enforcement officers when responding to or encountering situations involving persons displaying behaviors consistent with mental illness or crisis.

**II. POLICY**

Responding to situations involving individuals who officers reasonably believe to be affected by mental illness or in crisis carries potential for violence; requires an officer to make difficult judgments about the mental state and intent of the individual; and necessitates the use of special police skills, techniques, and abilities to effectively and appropriately resolve the situation, while avoiding unnecessary violence and potential civil liability. The goal shall be to de-escalate the situation safely for all individuals involved when reasonable, practical, and consistent with established safety priorities. In the context of enforcement and related activities, officers shall be guided by this state’s law regarding the detention of persons affected by mental illness or in crises. Officers shall use this policy to assist them in determining whether a person’s behavior is indicative of mental illness or crisis and to provide guidance, techniques, and resources so that the situation may be resolved in as constructive and humane a manner as possible.

**III. DEFINITIONS**

*Mental Illness:* An impairment of an individual’s normal cognitive, emotional, or behavioral functioning, caused by physiological or psychosocial factors. A person may be affected by mental illness if he or she displays an inability to think rationally (e.g.,

delusions or hallucinations); exercise adequate control over behavior or impulses (e.g., aggressive, suicidal, homicidal, sexual); and/or take reasonable care of his or her welfare with regard to basic provisions for clothing, food, shelter, or safety.

*Crisis:* An individual’s emotional, physical, mental, or behavioral response to an event or experience that results in trauma. A person may experience crisis during times of stress in response to real or perceived threats and/or loss of control and when normal coping mechanisms are ineffective. Symptoms may include emotional reactions such as fear, anger, or excessive giddiness; psychological impairments such as inability to focus, confusion, nightmares, and potentially even psychosis; physical reactions like vomiting/stomach issues, headaches, dizziness, excessive tiredness, or insomnia; and/or behavioral reactions including the trigger of a “fight or flight” response. Any individual can experience a crisis reaction regardless of previous history of mental illness.

**IV. PROCEDURES**

**A. Recognizing Abnormal Behavior**

Only a trained mental health professional can diagnose mental illness, and even they may sometimes find it difficult to make a diagnosis. Officers are not expected to diagnose mental or emotional conditions, but rather to recognize behaviors that are indicative of persons affected by mental illness or in crisis, with special emphasis on those that suggest potential violence and/or danger. The following are generalized signs and symptoms of behavior that may suggest mental illness or

crisis, although officers should not rule out other potential causes such as reactions to alcohol or psychoactive drugs of abuse, temporary emotional disturbances that are situational, or medical conditions.

1. Strong and unrelenting fear of persons, places, or things. Extremely inappropriate behavior for a given context.
2. Frustration in new or unforeseen circumstances; inappropriate or aggressive behavior in dealing with the situation.
3. Abnormal memory loss related to such common facts as name or home address (although these may be signs of other physical ailments such as injury or Alzheimer's disease).
4. Delusions, the belief in thoughts or ideas that are false, such as delusions of grandeur ("I am Christ") or paranoid delusions ("Everyone is out to get me").
5. Hallucinations of any of the five senses (e.g., hearing voices commanding the person to act, feeling one's skin crawl, smelling strange odors); and/or
6. The belief that one suffers from extraordinary physical maladies that are not possible, such as persons who are convinced that their heart has stopped beating for extended periods of time.

#### B. Assessing Risk

1. Most persons affected by mental illness or in crisis are not dangerous and some may only present dangerous behavior under certain circumstances or conditions. Officers may use several indicators to assess whether a person who reasonably appears to be affected by mental illness or in crisis represents potential danger to himself or herself, the officer, or others. These include the following:
  - a. The availability of any weapons.
  - b. Statements by the person that suggest that he or she is prepared to commit a violent or dangerous act. Such comments may range from subtle innuendo to direct threats that, when taken in conjunction with other information, paint a more complete picture of the potential for violence.
  - c. A personal history that reflects prior violence under similar or related circumstances. The person's history may already be known to the officer—or family, friends, or neighbors might provide such information.
  - d. The amount of self-control that the person, particularly the amount of physical control over emotions of rage, anger, fright, or agitation. Signs of a lack of self-control in-

clude extreme agitation, inability to sit still or communicate effectively, wide eyes, and rambling thoughts and speech. Clutching oneself or other objects to maintain control, begging to be left alone, or offering frantic assurances that one is all right may also suggest that the individual is close to losing control.

- e. The volatility of the environment is a particularly relevant concern that officers must continually evaluate. Agitators that may affect the person or create a particularly combustible environment or incite violence should be taken into account and mitigated.
2. Failure to exhibit violent or dangerous behavior prior to the arrival of the officer does not guarantee that there is no danger, but it might diminish the potential for danger.
  3. An individual affected by mental illness or emotional crisis may rapidly change his or her presentation from calm and command-responsive to physically active. This change in behavior may come from an external trigger (such as an officer stating "I have to handcuff you now") or from internal stimuli (delusions or hallucinations). A variation in the person's physical presentation does not necessarily mean he or she will become violent or threatening, but officers should be prepared at all times for a rapid change in behavior.

#### C. Response to Persons Affected by Mental Illness or in Crisis

If the officer determines that an individual is exhibiting symptoms of mental illness or in crisis and is a potential threat to himself or herself, the officer, or others, or may otherwise require law enforcement intervention as prescribed by statute, the following responses should be considered:

1. Request a backup officer. Always do so in cases where the individual will be taken into custody.
2. Take steps to calm the situation. Where possible, eliminate emergency lights and sirens, disperse crowds, and assume a quiet nonthreatening manner when approaching or conversing with the individual. Where violence or destructive acts have not occurred, avoid physical contact, and take time to assess the situation. Officers should operate with the understanding that time is an ally and there is no need to rush or force the situation.

3. Move slowly and do not excite the person. Provide reassurance that the police are there to help and that the person will be provided with appropriate care.
  4. Communicate with the individual in an attempt to determine what is bothering him or her. If possible, speak slowly and use a low tone of voice. Relate concern for the person's feelings and allow the person to express feelings without judgment. Where possible, gather information on the individual from acquaintances or family members and/or request professional assistance if available and appropriate to assist in communicating with and calming the person.
  5. Do not threaten the individual with arrest, or make other similar threats or demands, as this may create additional fright, stress, and potential aggression.
  6. Avoid topics that may agitate the person and guide the conversation toward subjects that help bring the individual back to reality.
  7. Always attempt to be truthful with the individual. If the person becomes aware of a deception, he or she may withdraw from the contact in distrust and may become hypersensitive or retaliate in anger. In the event an individual is experiencing delusions and/or hallucinations and asks the officer to validate these, statements such as "I am not seeing what you are seeing, but I believe that you are seeing (the hallucination, etc.)" is recommended. Validating and/or participating in the individual's delusion and/or hallucination is not advised.
  8. Request assistance from individuals with specialized training in dealing with mental illness or crisis situations (e.g., Crisis Intervention Training (CIT) officers, community crisis mental health personnel, Crisis Negotiator).
- D. Taking Custody or Making Referrals to Mental Health Professionals
1. Based on the totality of the circumstances and a reasonable belief of the potential for violence, the officer may provide the individual and/or family members with referral information on available community mental health resources, or take custody of the individual in order to seek an involuntary emergency evaluation. Officers should do the following:
    3. Summon an immediate supervisor or the officer-in-charge prior to taking custody of a potentially dangerous individual who may be affected by mental illness or in crisis or an individual who meets other legal requirements for involuntary admission for mental examination. When possible, summon crisis intervention specialists to assist in the custody and admission process.
    4. Continue to use de-escalation techniques and communication skills to avoid provoking a volatile situation once a decision has been made to take the individual into custody. Remove any dangerous weapons from the immediate area, and restrain the individual if necessary. Using restraints on persons affected by mental illness or in crisis can aggravate any aggression, so other measures of de-escalation and commands should be utilized if possible. Officers should be aware of this fact, but should take those measures necessary to protect their safety.
    5. Document the incident, regardless of whether or not the individual is taken into custody. Ensure that the report is as detailed and explicit as possible concerning the circumstances of the incident and the type of behavior that was observed. Terms such as "out of control" or "mentally disturbed" should be replaced with descriptions of the specific behaviors, statements, and actions exhibited by the person. The reasons why the subject was taken into custody or referred to other agencies should also be reported in detail.
  2. Offer mental health referral information to the individual and or/family members when the circumstances indicate that the individual should not be taken into custody.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this document incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no “model” policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

This project was supported by a grant awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the IACP.

IACP National Law Enforcement Policy Center Staff:  
Philip Lynn, Manager; Sara Dziejma, Project Specialist;  
and Vincent Talucci, Executive Director, International Association of Chiefs of Police.

© Copyright 2014. Departments are encouraged to use this policy to establish one customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.



# PATROL GUIDE

Section: Tactical Operations		Procedure No: 221-13	
<b>MENTALLY ILL OR EMOTIONALLY DISTURBED PERSONS</b>			
DATE ISSUED: 06/01/16	DATE EFFECTIVE: 06/01/16	REVISION NUMBER:	PAGE: 1 of 5

## PURPOSE

To safeguard a mentally ill or emotionally disturbed person who does not voluntarily seek medical assistance.

## SCOPE

The primary duty of all members of the service is to preserve human life. The safety of ALL persons involved is paramount in cases involving emotionally disturbed persons. If such person is dangerous to himself or others, necessary force may be used to prevent serious physical injury or death. Physical force will be used ONLY to the extent necessary to restrain the subject until delivered to a hospital or detention facility. Deadly physical force will be used ONLY as a last resort to protect the life of the uniformed member of the service assigned or any other person present. If the emotionally disturbed person is armed or violent, no attempt will be made to take the EDP into custody without the specific direction of a supervisor unless there is an immediate threat of physical harm to the EDP or others are present. If an EDP is not immediately dangerous, the person should be contained until assistance arrives. If the EDP is unarmed, not violent and willing to leave voluntarily, a uniformed member of the service may take such person into custody. When there is time to negotiate, all the time necessary to ensure the safety of all individuals will be used.

## DEFINITIONS

EMOTIONALLY DISTURBED PERSON (EDP) - A person who appears to be mentally ill or temporarily deranged and is conducting himself in a manner which a police officer reasonably believes is likely to result in serious injury to himself or others.

ZONE OF SAFETY - The distance to be maintained between the EDP and the responding member(s) of the service. This distance should be greater than the effective range of the weapon (other than a firearm), and it may vary with each situation (e.g., type of weapon possessed, condition of EDP, surrounding area, etc.). A minimum distance of twenty feet is recommended. An attempt will be made to maintain the “zone of safety” if the EDP does not remain stationary.

## PROCEDURE

When a uniformed member of the service reasonably believes that a person who is apparently mentally ill or emotionally disturbed, must be taken into protective custody because the person is conducting himself in a manner likely to result in a serious injury to himself or others:

## UNIFORMED MEMBER OF THE SERVICE

1. Upon arrival at scene, assess situation as to threat of immediate serious physical injury to EDP, other persons present, or members of the service. Take cover, utilize protective shield if available and request additional personnel, if necessary.
  - a. If emotionally disturbed person’s actions constitute immediate threat of serious physical injury or death to himself or others:
    - (1) Take reasonable measures to terminate or prevent such behavior. Deadly physical force will be used only as a last resort to protect the life of persons or officers present.

# PATROL GUIDE

PROCEDURE NUMBER:	DATE EFFECTIVE:	REVISION NUMBER:	PAGE:
221-13	06/01/16		2 of 5

**NOTE** *Damaging of property would not necessarily constitute an immediate threat of serious physical injury or death.*

**UNIFORMED  
MEMBER OF  
THE SERVICE  
(continued)**

- b. If EDP is unarmed, not violent and is willing to leave voluntarily:
  - (1) EDP may be taken into custody without the specific direction of a supervisor.
- c. In all other cases, if EDP's actions do not constitute an immediate threat of serious physical injury or death to himself or others:
  - (1) Attempt to isolate and contain the EDP while maintaining a zone of safety until arrival of patrol supervisor and Emergency Service Unit personnel.
  - (2) Do not attempt to take EDP into custody without the specific direction of a supervisor.
2. Request ambulance, if one has not already been dispatched.
  - a. Ascertain if patrol supervisor is responding, and, if not, request response.

**NOTE** *Communications Section will automatically direct the patrol supervisor and Emergency Service Unit to respond to scene in such cases. Patrol supervisors' vehicles are equipped with non-lethal devices to assist in the containment and control of EDP's, and will be used at the supervisor's direction, if necessary.*

3. Establish police lines.
4. Take EDP into custody if EDP is unarmed, not violent and willing to leave voluntarily.
5. Verify that Emergency Service Unit is responding, if required.
  - a. Cancel response of Emergency Service Unit if services not required.
6. Direct uniformed members of the service to take EDP into custody if unarmed, not violent, and willing to leave voluntarily.

**PATROL  
SUPERVISOR**

**NOTE** *When aided is safeguarded and restrained comply with steps 25 to 32 inclusive.*

**WHEN AIDED IS ISOLATED/CONTAINED BUT WILL NOT LEAVE VOLUNTARILY:**

**PATROL  
SUPERVISOR**

7. Establish firearms control.
  - a. Direct members concerned not to use their firearms or use any other deadly physical force unless their lives or the life of another is in imminent danger.
8. Deploy protective devices (shields, etc.).
  - a. Employ non-lethal devices to ensure the safety of all present (see "ADDITIONAL DATA" statement).
9. Comply with provisions of P.G. 221-14, "Hostage/Barricaded Person(s)," where appropriate.
10. Establish police lines if not already done.

# PATROL GUIDE

PROCEDURE NUMBER:	DATE EFFECTIVE:	REVISION NUMBER:	PAGE:
221-13	06/01/16		3 of 5

**PATROL SUPERVISOR (continued)**

11. Request response of hostage negotiation team and coordinator through Communications Section.
12. Notify desk officer that hostage negotiation team and coordinator have been notified and request response of precinct commander/duty captain.
13. Request Emergency Service Unit on scene to have supervisor respond.
14. If necessary, request assistance of:
  - a. Interpreter, if language barrier
  - b. Subject's family or friends
  - c. Local clergyman
  - d. Prominent local citizen
  - e. Any public or private agency deemed appropriate for possible assistance.

**NOTE**

*The highest ranking uniformed police supervisor at the scene is in command and will coordinate police operations. If the mentally ill or EDP is contained and is believed to be armed or violent but due to containment poses no immediate threat of danger to any person, no additional action will be taken without the authorization of the commanding officer or duty captain at the scene.*

**EMERGENCY SERVICE UNIT SUPERVISOR**

15. Report to and confer with ranking patrol supervisor on scene.
  - a. If there is no patrol supervisor present, request response forthwith, and perform duties of patrol supervisor pending his/her arrival.

**NOTE**

*The presence of a supervisor from any other police agency does not preclude the required response of the patrol supervisor.*

16. Evaluate the need and ensure that sufficient Emergency Service Unit personnel and equipment are present at the scene to deal with the situation.
17. Verify that hostage negotiation team and coordinator are responding, when necessary.
18. Devise plans and tactics to deal with the situation, after conferral with ranking patrol supervisor on scene.

**DESK OFFICER**

19. Verify that precinct commander/duty captain has been notified and is responding.
20. Notify Operations Unit and patrol borough command of facts.

**COMMANDING OFFICER/ DUTY CAPTAIN**

21. Assume command, including firearms control.
22. Confer with ranking Emergency Service Unit supervisor on scene and develop plans and tactics to be utilized.
23. Direct whatever further action is necessary, including use of negotiators.
24. Direct use of alternate means of restraint, if appropriate, according to circumstances.

# PATROL GUIDE

PROCEDURE NUMBER:	DATE EFFECTIVE:	REVISION NUMBER:	PAGE:
221-13	06/01/16		4 of 5

## WHEN PERSON HAS BEEN RESTRAINED:

### UNIFORMED MEMBER OF THE SERVICE

25. Remove property that is dangerous to life or will aid escape.
26. Have person removed to hospital in ambulance.
  - a. Restraining equipment including handcuffs may be used if patient is violent, resists, or upon direction of a physician examiner.
  - b. If unable to transport with reasonable restraint, ambulance attendant or doctor will request special ambulance.
  - c. When possible, a female patient being transported should be accompanied by another female or by an adult member of her immediate family.
27. Ride in body of ambulance with patient.
  - a. At least two uniformed members of the service will safeguard if more than one patient is being transported.

### NOTE

*If an ambulance is NOT available and the situation warrants, transport the EDP to the hospital by RMP if able to do so with reasonable restraint, at the direction of a supervisor. UNDER NO CIRCUMSTANCES WILL AN EDP BE TRANSPORTED TO A POLICE FACILITY.*

28. Inform examining physician, upon arrival at hospital, of use of non-lethal restraining devices, if applicable.
29. Safeguard patient at hospital until examined by psychiatrist.
  - a. When entering psychiatric ward of hospital, unload revolver at Firearm Safety Station, if available (see P.G. 216-07, "Firearms Safety Stations at Psychiatric Wards and Admitting Areas").
30. Inform psychiatrist of circumstances which brought patient into police custody:
  - a. Inform relieving uniformed member of circumstances if safeguarding extends beyond expiration of tour.
  - b. Relieving uniformed member will inform psychiatrist of details.
31. Enter details in **ACTIVITY LOG (PD112-145)** and prepare **AIDED REPORT WORKSHEET (PD304-152b)**.
  - a. Indicate on **AIDED REPORT WORKSHEET**, name of psychiatrist.
32. Deliver **AIDED REPORT WORKSHEET** to desk officer.

### ADDITIONAL DATA

*Refer persons who voluntarily seek psychiatric treatment to proper facility.*

*Prior to interviewing a patient confined to a facility of the NYC Health and Hospitals Corporation, a uniformed member of the service must obtain permission from the hospital administrator who will ascertain if the patient is mentally competent to give a statement.*

*Upon receipt of a request from a qualified psychiatrist, or from a director of a general hospital or his/her designee, uniformed members of the service shall take into custody and transport an apparently mentally ill or emotionally disturbed person from a facility licensed or operated by the NYS Office of Mental Health which does not have an inpatient psychiatric service, or from a general hospital which does not have an inpatient psychiatric service, to a hospital approved under Section 9.39 of the Mental Hygiene Law.*

# PATROL GUIDE

PROCEDURE NUMBER:	DATE EFFECTIVE:	REVISION NUMBER:	PAGE:
221-13	06/01/16		5 of 5

**ADDITIONAL  
DATA  
(continued)**

*Uniformed members of the service will also comply with the above procedure upon direction of the Commissioner of Mental Health, Mental Retardation and Alcoholism Services or his/her designee.*

**USE OF NON-LETHAL DEVICES TO ASSIST IN RESTRAINING EMOTIONALLY DISTURBED PERSONS**

*Authorized uniformed members of the service may use a conducted energy weapon (CEW) to assist in restraining emotionally disturbed persons, if necessary.*

*Authorized uniformed members of the service will be guided by Patrol Guide 221-08, 'Use of Conducted Electrical Weapons (CEW),' when a CEW has been utilized.*

***THREAT, RESISTANCE OR INJURY (T.R.I.) INCIDENT WORKSHEET (PD370-154)***  
*will be prepared whenever a less lethal device is used by a uniformed member of the service in the performance of duty.*

**RELATED  
PROCEDURES**

*Unusual Occurrence Reports (P.G. 212-09)*  
*Hostage/Barricaded Person(s) (P.G. 221-14)*  
*Unlawful Evictions (P.G. 214-12)*  
*Aided Cases General Procedure (P.G. 216-01)*  
*Mental Health Removal Orders (P.G. 216-06)*  
*Use of Conducted Electrical Weapons (CEW) (P.G. 221-08)*

**FORMS AND  
REPORTS**

***ACTIVITY LOG (PD112-145)***  
***AIDED REPORT WORKSHEET (PD304-152b)***  
***THREAT, RESISTANCE OR INJURY (T.R.I.) INCIDENT WORKSHEET (PD370-154)***  
***UNUSUAL OCCURRENCE REPORT (PD370-152)***

# City of Madison Camera System



CITY OF  
**MADISON**

City of Madison cameras are remotely controllable video cameras dedicated to observing vehicle road traffic, road conditions, and public safety. The cameras provide live video in real time to City Agencies for public safety.

---

## Types of Cameras

- **Fixed Cameras:** These are cameras that cannot be panned, tilted, or zoomed. Used to monitor a specific site at all times.
- **PTZ Cameras (Pan, Tilt, Zoom):** These cameras can be panned, tilted, and zoomed. PTZ cameras are often used when a single camera needs to be able to look at multiple subjects or areas, but not at the same time. They can be set to point in a particular direction for a set amount of time, then shift to point in another direction for a set amount of time, etc. This pattern is typically repeated in a loop. It may also be useful, for example, for a traffic camera to look at one side of an intersection during the morning rush hour, and the other side during the afternoon rush hour.
- **Panoramic Cameras:** These cameras capture a 180-degree or 360-degree panorama, depending on how they are mounted. They are often used for lobbies where there are multiple areas of importance that cannot all be captured by a fixed camera and or a PTZ camera.



Fixed Camera



Pan, Tilt and Zoom Camera



Panoramic Camera

# Examples of surveillance cameras on city facilities

West Washington Avenue & Broom St



West Washington & Fairchild St



Mifflin St & Fairchild St



100 Block of State St (Veteran's Museum)



100 Block of State Street



Overture Parking Garage (Dayton side)



# City of Madison Camera Locations

The list below includes all public camera location, but does not provide information on cameras in City facilities or cameras that are used to protect City infrastructure.

## Location

18 N. Carroll St.  
400 Block West Gilman  
400 N. Frances  
500 Block State St  
600 Block State St 1  
800 Block State St.  
Aberg Ave & Shopko Dr  
American Family Pkwy & Eastpark  
Bassett St & Mifflin  
Bassett St & W Washington Ave  
S Blair St & E Main  
Beltline & Fish Hatchery North  
Beltline & Fish Hatchery South  
Beltline & Gammon North  
Beltline & Gammon South  
Beltline & Mineral Point East  
Beltline & Mineral Point West  
Beltline & Old Sauk East  
Beltline & Old Sauk West  
Beltline & Park North  
Beltline & Rimrock North  
Beltline & Rimrock South  
Beltline & Todd Dr. East  
Beltline & Whitney North  
Beltline & Whitney South  
Brittingham Park Shelter  
Broadway & Monona Dr  
Broadway & Copps Ave  
Broadway & Frazier Ave  
Broom St & Mifflin St  
Buckeye Gilman  
Buckeye Gorham  
Carroll & Main  
Carroll St & Dayton St  
Carroll W Washington  
Charter St & Spring St  
Cold Spring East A  
Coldspring Bainbridge Gate  
ColdSpring East

ColdSpring Jerome St. Gate  
ColdSpring North  
ColdSpring North A  
Cottage Grove & Acewood  
Cottage Grove & Atlas  
Doty St & Carroll St  
Doty St & King St  
Doty St & S Hamilton & Fairchild  
E Washington & Marquette St  
E Washington & Webster St  
E. Washington & First St.  
E. Washington & Lien Rd.  
E. Washington & Pinckney  
E. Washington & Thierer  
E. Washington & Zeier Rd  
Elver Park & McKenna Blvd  
Fair Oaks Ave & E Washington Ave  
Fairchild & Mifflin  
Fish Hatchery & Badger Rd  
Fish Hatchery Rd & Mckee Rd  
Fluno 1  
Fluno 2  
Fluno 3  
Frances Dayton  
Frances Langdon  
Frances State South  
Gammon Rd & Odana Rd  
Gilman St & Henry St  
300 E Gorham St  
Gorham at N Blair St  
Gorham St & Broom St  
Gorham St & Franklin St  
Gorham St & Wisconsin Ave  
Hawthorne Court 1  
Hawthorne Court 2  
Hawthorne Court 3  
Hawthorne Court 4  
James Madison Park 1  
James Madison Park 2  
James Madison Park 3  
John Nolen & Blair & Wilson  
John Nolen & Broom St  
John Nolen & North Shore Dr  
John Nolen & Olin  
John Nolen & Rimrock Rd  
Johnson St & Baldwin St

Johnson St & Bassett St  
Johnson St & Blair St  
Johnson St & Butler & Hamilton  
Johnson St & First St  
Johnson St & Park St  
Johnson St & Wisconsin Ave  
Johnson St and Frances  
Junction Rd at Mineral Pt Rd  
King St & Pinckney St & Main St  
Lake Mendota & Carroll  
Lake Mendota & Frances  
Lake Mendota & Henry  
Lake Mendota & Lake  
Lake St & Langdon  
Langdon & Henry  
Langdon & Howard  
Langdon St & Carroll St  
Langdon St & Wisconsin Ave  
Mckee Rd & Seminole Hwy  
E. Wash & Ingersoll  
Mifflin & Bedford  
Mifflin St & Pinckney  
Mineral Point and Gammon  
Mineral Point Rd & Midvale Blvd  
Mineral Point Rd & South Point  
Mineral Pt Rd & Whitney Way  
MLK & Doty  
MLK Jr Blvd & Main St  
Northport & Dryden  
Northport & Sherman Ave  
Northport Dr & Troy Drive  
Old Sauk & Excelsior  
Old Sauk & High Point  
Old Sauk & Junction Rd  
Old Sauk & Pleasant View  
Packers & Commercial Ave  
Packers & International Lane  
Packers & Northport Dr  
Park & Badger  
Park & W Washington  
Park St & Fish Hatchery Rd  
Park St. & Buick  
Park St. & Olin  
Peace Park & State  
Peace Park & Gilman

Penn Park 1  
Penn Park 2  
Pinckney E. Washington  
Pleasant View & McKee  
Pleasant View & Midtown  
Raymond Rd & McKenna Blvd  
Raymond Rd & Whitney Way  
Regent St & Breese Terrace  
Regent St & Mills St  
Regent St & Monroe  
Regent St & Park St  
Regent St & Randall Ave  
Rimrock Rd & Moorland  
Schroeder Rd & Gammon Rd  
Sherman Ave & Aberg Ave  
State St & Dayton St  
State St & Frances North  
State St & Gilman St  
State St & Gorham St  
State St & Johnson St  
State St & Mifflin St cul-de-sac  
State St. & Lake St.  
State St. & Mifflin & Carroll 1  
State St. & Mifflin & Carroll 2  
State St. & Carroll St. Cul De Sac  
State St. 700 block  
SW Bike Path @ Verona Frontage  
Todd Dr & W. Beltline  
University Ave & Babcock Dr  
University Ave & Bassett St  
University Ave & Farley Ave  
University Ave & Frances St  
University Ave & Lake St  
University Ave & Midvale Blvd  
University Ave & Park St  
University Ave & Segoe Rd  
University Ave & Shorewood Blvd  
University Ave & Spring Harbor  
University Ave & Whitney Way  
Verona Rd Underpass East  
Verona Rd Underpass West  
W Washington & Bedford St  
W Washington & Fairchild St  
W. Washington & Broom  
W. Washington & Proudfit

Webster St & N Hamilton St  
Whitney Way & Odana Rd  
Wisconsin & Dayton  
Wisconsin & Mifflin

# Systems not included in the Surveillance Camera System

These are examples of devices and cameras on city facilities, which are used by Traffic Engineering and Public Safety staff on a daily basis.

## Traffic Detection Cameras

Traffic Detection Cameras monitors presence of vehicles and pedestrians, digitizes and processes the images and converts into traffic data to provide traffic count information and inputs for traffic signal controllers.



American Parkway and Buttonwood



Fish Hatchery and Beltline



M and PD

## Emergency Vehicle Detector

The traffic preemption device will cause properly equipped traffic lights in the path of emergency vehicles to cycle quickly, to grant right-of-way in the desired direction, after allowing for normal programmed time delays for signal changes and pedestrian crosswalks to clear. These devices do not include images or video.



Emergency Vehicle Detector (EVD) on Midvale and Mineral Point Rd.