**Specification Technology Specifications Report – Joe Louis Greenway Security Command Center**

**Section 17-5-453 Surveillance Technology Specification Reports.**

1. **The General Services Department certifies that this information contained in this document reflects the complete and accurate proposed use of the surveillance technology.**
2. **This report has been approved by the Director of the General Services Department and reviewed by the Detroit Police Department.**
3. ***Description:*** Information describing the surveillance technology and its capabilities

The proposed technology and its capabilities are described as follows:

Surveillance video equipment for the JLG’s Security Command Center located at

115 Erskine Street, Detroit, MI 48201. This specification includes all equipment, installation and integration work required for a Genetec video management system (VMS) to support the Joe Louis Greenway (JLG) security operations center (SOC). This work consists of the following.

* Furnish, install, and configure a Genetec a VMS server and software at a designated City of Detroit (CoD) Department of Information and Technologies (DoIT) Data Center.
* VMS shall have capability to support 500 internet protocol (IP) cameras and voice over internet protocol (VoIP) emergency phones. Furnish, install, and configure VMS desktop client workstations to control and view video streams and VoIP calls.
* Provide Genetec VMS Streamvault Appliance and two (2) Genetec Streamvault Workstations with the following general requirements.
	+ Supports H.265, H 264, Motion JPEG and MPEG-4, video compression format.
	+ Provide licenses for all required VMS modules for IP cameras and VoIP emergency phones.
	+ Supports ability to generate video feeds at different frame rates.
	+ Supports ONVIF open standard.
	+ 19-inch rack mountable with KVM.
	+ Supports built-in motion detection capability with the ability to notify the operator if motion is detected.
	+ Supports integration into the existing video wall equipment.
	+ Supports multicast video source.
	+ Supports VoIP protocol for VoIP emergency phone integration.
	+ Supports public notifications from the SOC through VoIP application.
	+ Supports iDrac or iLo remote management functionality.
	+ Supports configuration ability such as camera presets and event detection.
	+ Supports smart interactive multi-layer maps, Google maps, Bing maps, custom maps overlayed with camera field geographic locations.
	+ Supports native drivers for Axis CCTV cameras and Talkaphone VoIP emergency phones.
	+ Supports video recording for up to 15 days for each video feed integrated into the VMS.
	+ VMS must be compatible with Genetec Security Center 5.10.2
	+ VMS must support camera dewarping for 360-degree view camera.
	+ VMS must support the ability to federate with other Genetec systems.
	+ Provide 47” ultrawide monitors for the Streamvault.
	+ Provide 50 IP Camera licenses.
	+ Provide 50 VoIP emergency phones.
1. **Purpose:** Any specific purpose the surveillance technology is intended to advance:
* The purpose and intended uses of the proposed technology includes:
	+ Alert security if there is an event of medical or safety emergency;
	+ Alert third-party response teams depending on the issue;
	+ Public notification alerting users un the event the Greenway must be evacuated;
	+ Auto-theft prevention and deterrence;
	+ Apprehension of suspects and fugitives;
	+ Located AMBER Alert vehicles;
	+ Furthering investigations of serious crimes; and
	+ Other legitimate law enforcement purposes (e.g., crime analysis).
* The following uses of the technology are expressly prohibited:
	+ Willfully using the equipment for the specific purposes of taking photographs of personal property other than what would typically be expected from normal public safety use;
	+ Willfully using the equipment for the specific purposes of taking still-photographs of individuals other than what would typically be expected from normal public safety use;
	+ Traffic enforcement; or
	+ Track an individual’s movement outside of a vehicle.
1. **Deployment:** Deployment. If the surveillance technology will not be uniformly deployed
or targeted throughout the City, the factors that will be used to determine where the technology is deployed or targeted;
* The technology will be deployed on off-street section of the Joe Louis Greenway. See map below:

{Insert Map}

1. **Fiscal impact:** The fiscal impact of the surveillance technology
* The contract’s total cost is $150,000. The full amount has been allocated from the American Rescue Plan Act (ARPA) funds to cover this contract.
1. **Civil rights and liberties impacts:** An assessment identifying with specificity:

	1. ***Any potential adverse impacts the surveillance technology, if deployed, might
	have on civil rights and civil liberties; and***
* The SOC and all associated equipment, installation and integration work required for a Genetec video management system (VMS) does not intrude upon any constitutionally protected areas.
* Misuse of equipment or any information collected is strictly prohibited.
1. ***What specific, affirmative measures will be implemented to safeguard the public from potential adverse impacts identified in this section.***
* The SOC will strictly enforce it is security pertaining to the use of security equipment and technology.
1. **Authorized use:** A complete description of the purpose and intended uses of
the surveillance technology, including any uses that will be expressly prohibited.
2. **Data collection:**
	1. ***What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology;***
* *Surveillance from several different types of cameras will be collected. Below is a detailed description:*
	+ License plate readers are designed to detect license plates. The system includes high-speed cameras that have the capacity to collect an image of a license plate, information pertaining to the vehicle’s make and model, the state registration, as well as any distinguishing features of the vehicle.
	+ Pan-Tilt-Zoom (PTZ) Camera are designed for locations where wide field of view, high pixels-on-target, and long-distance zoom are all essential for maximum coverage. To reduce the chance of blind spot events occurring outside of the camera’s vision, PTZ cameras will be either be configured for pre-programmed tours or paired with fixed cameras focused on critical paths or chokepoints.
	+ 360° cameras will be installed to maximize visibility coverage while maintaining a small footprint. These cameras allow easy coverage of multiple areas at once and can even handle challenging lighting environments with ease. Ideal for complex coverage areas like road intersections and the corners of buildings, these cameras provide the perspectives of four cameras in a single package due to multiple lenses housed in a single dome. Because of their limited distance resolution and lack of mechanical zoom, these cameras should be installed at places where obstacles or difficult angles can allow their wide field of view features to shine instead of in large, open spaces or in long, narrow corridors.
	+ Fixed cameras provide the advantage of precise, focused imagery and crisp, high-resolution feeds. These cameras excel in locations where long-distance monitoring is necessary or where vital entrances or chokepoints necessitate motionless monitoring with maximum pixels-on-target. For optimal monitoring, fixed cameras are paired with PTZ cameras or 360° cameras in such a way that the fixed camera can focus on important areas while the other camera is able to capture the other angles. When events of interest occur, fixed cameras and PTZ cameras can be configured together to coordinate multiple angles of view on a subject, such as having one camera zoom in for detail while the other tracks the subject’s movements with the wider context in view. At locations where special safety threats exist, thermal imaging features can be used to maximize nighttime visibility.
	1. ***What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology and the measures that will be taken to
	minimize the inadvertent collection of the data; and***
* After careful consideration, the SOC cannot determine any instance or situation where legally protected information may be collected from the proposed technology.
* Although not the intent of the technology, images of the vehicle’s driver, passenger, or personal property may be inadvertently connected.
	1. ***How inadvertently collected surveillance data will be expeditiously identified
	and deleted;***
* After careful consideration, the SOC cannot determine any instance or situation where legally protected information may be collected from the proposed technology.
* The proposed contract provides that the SOC and the Detroit Police Department owns all the data collected. In the event protected information is collected through the misuse of the technology, the SOC will cause for its deletion as soon as feasible.
1. ***Data protection. The safeguards will be used to protect surveillance data
from unauthorized access, including encryption and access control mechanisms;***
* The SOC and Detroit Police Department will comply with FBI/State of Michigan rules pertaining to Criminal Justice Information Systems (CJIS) regulations and other applicable standards and policies to protect data.
* All Contactor representatives working on CoD Security and Network systems must be fingerprinted and have a background check performed by the Detroit Police Department and have Michigan State Police CJIS security awareness training on file.
1. Data retention. Insofar as the privacy of the public can be severely compromised by the long-term storage of mass surveillance data, the regulations and procedures that govern the retention of surveillance data, including those governing:

	1. ***The 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 or
	purposes enumerated in the Surveillance Technology Specification Report;***
* The SOC will adhere to the Detroit Police Department’s Data Retention Policy, which matches the requirements set forth in the corresponding state statute.

	1. ***The specific conditions that must be met to retain surveillance data beyond the
	retention period identified pursuant to Subsection (b)(9)a of this section; and***
* Data will not be retained beyond the retention period except where such information constitutes evidence of a crime related to an open case or a closed case where the prosecution/ or appeals remain pending.
.
	1. ***The process utilized to regularly delete surveillance data after the retention period stated in Subsection (b)(9)a of this section has elapsed and the auditing procedures that will be implemented to ensure data is not improperly retained;***
* The SOC will follow the Detroit Police Department’s policies and procedures which allow for the retention of surveillance data for up to one year. However, any hits or reads that were not used in a criminal investigation will be automatically deleted by the system after 15 days for cameras. If the Detroit Police Department preserves the surveillance data for use in an investigation, it will fall under the retention and destruction requirements for case files and not under the retention requirements for surveillance information. This is a Detroit Police Department only policy and is in compliance with Michigan law.
1. **Surveillance data sharing:** If a City department is seeking authorization to
share access to surveillance technology or surveillance data with any other govern-
mental agencies, departments, bureaus, divisions or units, or non-governmental
persons or entities in the absence of a judicial warrant or other legal mandate, the
City department shall detail:
	1. ***Which governmental agencies, departments, bureaus, divisions or units,
	or non-governmental persons or entities will be approved:***
		1. ***For surveillance technology sharing to the governmental agency, department,
		bureau, division or unit, or non-governmental person or entity, and***
		2. ***For surveillance technology sharing from the governmental agency, department, bureau, division or unit, or nongovernmental person or entity; and***
		3. ***For surveillance data sharing to the governmental agency, department, bureau, division or unit, or non-governmental person or entity;***
	2. ***Where applicable, the type of information of surveillance data that may be
	disclosed to the governmental agency, department, bureau, division or unit, or
	non-governmental person or entity; and***
	3. ***Where applicable, any safeguards or restrictions that will be imposed on the surveillance technology or data receiving governmental agency, department, bureau, division or unit, or non-governmental person or entity regarding the use or dissemination of the provided surveillance technology or data;***
* As of May 17, 2023, The Detroit Police Department has entered into a Data Sharing Agreements with 31 law enforcement agencies. Under no circumstances are members of the department authorized to share information for the purpose of assessing immigration status or enforcing immigration laws. The Detroit Police Department provides a monthly report to the Board of Police Commissioners reflecting the number of law enforcement agencies with home the Department has data sharing agreement.
1. **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;
* The SOC will only share information with the Detroit Police Department or other emergency services (e.g. EMS, Fire). The Detroit Police Department will only share information with government entities or third parties in accordance with duly authorized data sharing agreements. Under no circumstances is a member of the SOC or the Detroit Police Department authorized to share information for the purpose of assessing immigration status or enforcing immigration laws.
1. **Auditing and oversight.** What mechanisms will be implemented to ensure
the Surveillance Technology Specification Report is followed, including what independent persons or entities will be given oversight authority, if and how regular audits will be conducted, and, in the case of the Detroit Police Department, how the Board of Police Commissioners will be involved in the auditing and oversight process;
* The primary responsibility of ensuring the Surveillance Technology Specification Report is followed will fall primarily on the General Services Department Security Administration.
* Upon identifying that protected information has been collected through the misuse of technology, General Services Department Security Administration will report the following to the Police Department
	+ Type of information collected;
	+ Date range of the collection;
	+ Extent of the impact (i.e., how many persons’ information was collected);
	+ Staff members who had access to the information; and
	+ Date and method of destruction, once it has been destroyed.
* On a monthly basis, the Detroit Police Department will provide the Board of Police Commissioners with a list of members who have access to the surveillance technology.
* The Detroit Police Department will provide the Board a monthly report of the total number of license plate reads for the prior month.
1. **Training.** Would specialized training be required in connection with the use
of the surveillance technology; and
* Every member of theGeneral Services Department Security Administration and SOC will receive some degree of training with respect to the technology.
1. **Complaints.** What procedures will allow members of the public to register
complaints or concerns, or submit questions about the deployment or use of a
specific surveillance technology, and how the City department will ensure each
question and complaint is responded to in a timely manner.
* The policies and procedures of the Police Department require that upon receiving notice of the desire to file a complaint, a member of the Department must involve a supervisor as soon as possible to receive the complaint. Questions regarding the technology may be directed to the Office of the Chief of Police.