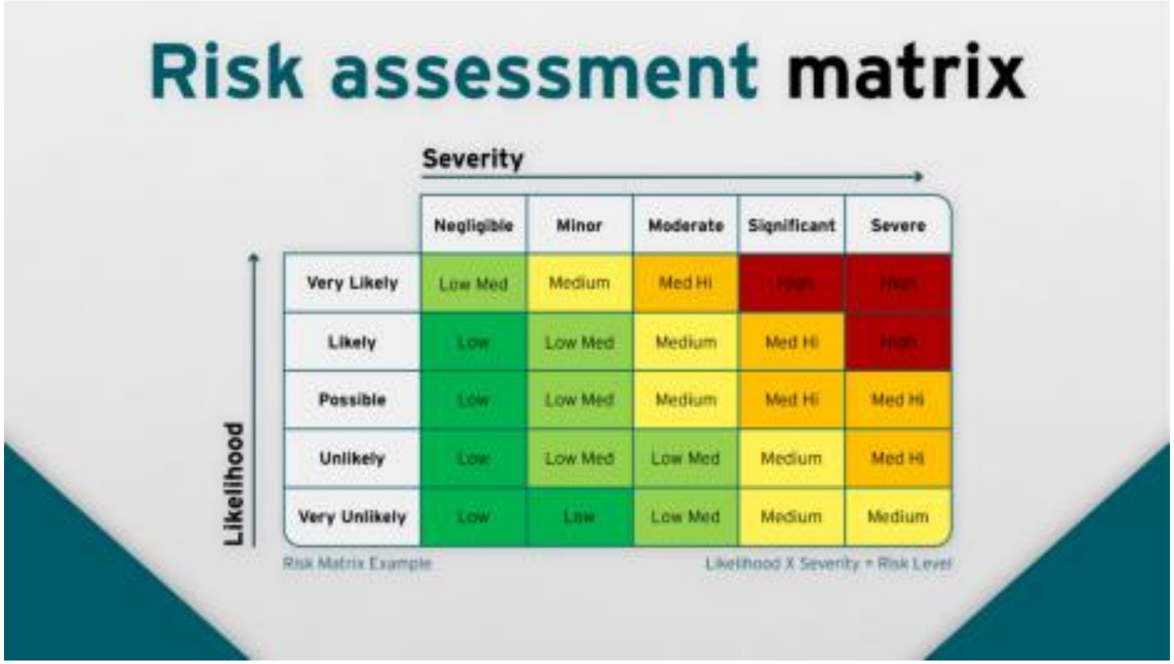
Numina Deployment on Michigan Avenue: Safety Plan and Risk Assessment

High-level Assessment:
The Numina system includes its proprietary sensors, which are designed to mount easily to light poles or building faces, wire to power (with very low consumption, <10 kWH per month), and transmit data over cellular networks. The sensors transmit only anonymous data to our cloud, which makes insights available via API and web dashboard. Numina sensors have been deployed in the public realm for 7 years in over 35 cities globally. Given Numina’s track record of success and the design of its hardware and software — which relies on common mounting materials, is entirely standalone from other entities’ information systems, and does not collect any Personally Identifiable Information —, the risk level of this project is estimated to be **Low**.



Risk assessment matrix

Severity

Likelihood	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Matrix Example

Likelihood X Severity = Risk Level

Source: https://riskpal.com/risk-assessment-matrices/

Specific potential risks are outlined below.

Potential Risks & Mitigation:

Potential Risk	Potential Impact	Likelihood	Severity	Mitigation
The sensor falls down from its mounted position on a light pole.	Sensor is damaged and no longer usable; potential street-level damages or injury, and hazard of debris.	Very unlikely	Significant	Numina's sensors are typically mounted to street light poles using the same steel straps any street sign uses. Numina's sensors are designed to be lightweight and compact, which allows for easy installation and minimizes the impact on streetlight infrastructure. Since Numina’s inception and over hundreds of deployments, this type of incident has never happened.
The sensor is mounted incorrectly.	Sensor data is unusable as the sensor view shifts.	Unlikely	Moderate	In a typical project, the customer is responsible for installation, either using their own engineering staff or hiring a third-party electrician. If the steel straps are mounted incorrectly because the steel straps are not significantly tightened, we would be able to tell from the sensor view that the sensor view has shifted, even incrementally, and alert the installation team. This would also be covered by the installers’ liability or insurance. **This incident would interfere with the project success but would not endanger any external person or system.**

The sensor is subject to vandalism.	The sensor is no longer able to collect data.	Very unlikely	Moderate	Numina sensors are mounted 15-20 feet high, making them out of reach for spontaneous acts of vandalism. Since Numina's inception and over hundreds of deployments, this type of incident has never happened. **This incident would interfere with the project success but would not endanger any external person or system.**
Citizens are worried about personally identifiable information (PII), such as their faces or license plate numbers, being recorded by the sensor.	There is community concern, which delays or shuts down the project.	Possible	Minor	Numina's community engagement plan aims to address any privacy concerns. Numina's Privacy-by-Design approach means that every aspect of data collection, transmission, validation, analysis, delivery, and visualization is intentionally designed to minimize data collection and to strip away potentially Personally Identifiable Information (PII). Numina provides *Intelligence without Surveillance*. Our data collection practices are outlined in detail in Numina's privacy policy, viewable at https://numina.co/privacy. Numina's privacy philosophy is explained at https://numina.co/our-privacy-principles. Numina has also successfully piloted community engagement tools that can be co-deployed with our sensor technology. We participated in community outreach activities during the Newlab Accessible Streets Studio. We are also aware that other camera-based technologies, which are *not* privacy-conscious and have not conducted community engagement of any kind, are deployed and have not

				encountered prohibitive pushback from the local community.
There is a security breach.	Unauthorized users have access to data.	Very unlikely	Moderate	We implement best-in-class practices related to data transmission security. Numina’s sensors encrypt all communication with TLS1.2 using industry-standard AES-256 encryption. Only authorized devices can communicate with sensors. This requirement removes pathways for data interception or sensor access by unauthorized third parties. All of our data is stored in Amazon Web Services (AWS), is encrypted at rest, and access is restricted to current Numina employees and contractors using AWS best practices for limited identity and access management. Further, because we only transmit anonymized data, there is no risk of Personally Identifiable Information (PII) being exposed. Since Numina’s inception and over hundreds of deployments, this type of incident has never happened. In the worst-case scenario, any data “leak” **would interfere with the project success but would not endanger any external person or system.**

The sensor loses power.	Sensor is unable to collect data.	Possible	Moderate	Because Numina transmits only critical, anonymous data over cellular networks, we are able to achieve low power usage (less than 10 kWH per month) and a low data rate (less than 200 kbps) for each sensor. Further, each sensor is equipped with a back-up battery in the case that there is a temporary power outage. Sensors can lose power if there is an issue with power at the light pole (i.e. a certain site is not energized or loses power). This issue would be out of Numina’s control but only requires an on-the-ground resource to revisit the location to re-establish a power connection or coordination with the local utility. **This incident would interfere with the project success but would not endanger any external person or system.**
Something obstructs the view of the sensor once it is mounted, such as foliage.	Sensor data is unusable as it is obstructed.	Possible	Moderate	Sensor locations are identified to minimize any risk of obstruction. In the event that a sensor’s view is obstructed, we would be able to remotely detect unusual activity in the sensor's view (such as a drop in detections) and follow up with an in-person investigation to resolve the issue. **This incident would interfere with the project success but would not endanger any external person or system.**

The cell network is down, and the sensor is unable to transmit data.	No data is transmitted, and data is not collected.	Very unlikely	Significant	Because all sensors come with 4G LTE SIM cards installed, we typically have strong connectivity in developed areas and don’t run into network issues. We aren’t able to reach the sensors if the network is down, but this is a rare event out of our control. Once the network is back up, the sensor will come back online and if additional troubleshooting is needed, our engineers can provide remote support. **This incident would interfere with the project success but would not endanger any external person or system.**