



Seattle Office of
Inspector General

Hostage Negotiation Throw Phone Report 2024

As Required by Seattle Municipal Code 14.18.060

June 6, 2025

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064

206.684.3663
oig@seattle.gov

Technology Description

The Hostage Negotiation Throw Phone refers to the Critical Incident Negotiations Team (CINT) System and tactical phone made by 836 Technologies, which facilitates two-way communication between law enforcement and a subject. By facilitating this communication, officers can develop negotiation tactics, conduct a situational assessment, and monitor situational safety. This surveillance technology belongs to Seattle Police Department's (SPD) Hostage Negotiation Team (HNT).

This surveillance technology consists of three parts: (1) the CINT Commander Box, which is a physical hub that can serve as a phone for officers, (2) a tactical throw phone that the subject interacts with and (3) a CINT software application that is installed on an SPD laptop when the device is physically connected to the CINT Commander Box. This software automatically logs and records each time the CINT System is used.

To operate the tactical Throw Phone, it must be manually connected through cables to the CINT Commander Box. The CINT Commander Box is also connected to a laptop and DVR. After all the components are connected, officers can monitor a scene through the tactical throw phone's cameras and microphones by connecting headphones in the range of the CINT System. The CINT System can be used without the tactical Throw Phone, but in these cases the CINT system does not have video recording capabilities.

Despite its name, the Hostage Negotiation Throw Phone is not designed to be thrown. The Throw Phone is inside of a large kit that must be physically delivered to a subject. To use the Throw Phone, it must be connected to the CINT System with multiple cables, which makes it difficult to deploy. Deploying the tactical Throw Phone presents logistical challenges, which has led officers to use a technology called a Brinc Ball more frequently than the traditional Throw Phone. The Brinc Ball has no cameras or recording capabilities. Since the Brinc Ball does not have a camera or recording capabilities, it does not meet the criteria of a surveillance technology and is not included in this review.

SECTION A

Frequency and Patterns of Use

SMC 14.18.060, § A: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.



Figure 1. HNT Officers Delivering the Throw Phone



Figure 2. CINT Commander Box Connected to SPD Laptop

The Throw Phone is only used when the HNT is called to a scene. HNT responds to calls that involve a barricaded person,¹ a person in crisis, or in service of a warrant or high-risk operation² with another unit. In addition to these conditions, the Throw Phone is only used whenever there is no other means of communication. The Throw Phone is not deployed if there are other ways to communicate with a subject. For example, an officer will not deploy the Throw Phone if it is possible to contact a subject by calling their cellphone. Since there are often other means of communication and the Throw Phone is difficult to deploy, it is rarely used. In 2024, there were no recorded deployments of the technology. The last time the technology was deployed was in 2022. While the HNT does not deploy the Throw Phone often, Section 2.2 of the Surveillance Impact Report (SIR) for this technology states that Throw Phones are standard equipment for hostage negotiation.

Case Example

Officers responded to a domestic violence scene where a woman and her infant fled their apartment. The suspect refused to leave the apartment and threatened to jump from the fourth-floor window. Officers were able to establish dialogue with the suspect, but it was difficult to hear the suspect because of the distance and passing traffic. The HNT was able to negotiate the delivery of the Throw Phone and deployed it by lowering it from the roof of the building. After a four-hour negotiation, the suspect agreed to exit the building, and no force was used.

1 The Hostage Negotiation Team defines a barricaded incident as an incident where there is a need for police intervention and the involved suspect(s) or subject(s) have a position of advantage that would impede immediate access or intervention due to the physical environment or threat of a weapon and the suspect or subject is or appears to be refusing to comply with police directions over a period of time.

2 The HNT defines a high-risk incident as a barricaded incident where there is a reasonable belief that the involved subject/suspect has used, possessed, or threatened to use a weapon as part of the incident that they still have access to; has access to persons who could reasonably be harmed by their actions or are being prevented from leaving; has made threats to create a fire or other dangerous situation that would endanger others or has taken actions demonstrating so; has indicated a plan to goad police into using lethal force; or involves a known suspect/subject with a substantial history of violent acts and/or resistance to police.

SECTION B

Data Sharing with External Partners and Other Entities

SMC 14.18.060, § B: How often surveillance technology or its data are being shared with other entities, including other governments in particular.

Office of Inspector General (OIG) found no evidence that the Throw Phone was used in 2024; therefore, no data are expected to have been shared with external entities or members of the public. The HNT occasionally uses recordings as a part of their trainings with both internal and external entities, but the team does not provide copies of the evidence to participants. In the event that the Throw Phone is used, any evidence collected is uploaded to Evidence.com where sharing may occur as part of the criminal justice process.

SECTION C

Data Management and Safeguarding of Individual Information

SMC 14.18.060, § C: How well data management protocols are safeguarding individual information.

In the rare case that the Throw Phone is used, data are stored locally on an SPD laptop and/or DVR if video recordings are captured. These files are then uploaded to Evidence.com. If a copy of the recording is requested by the investigative officer, it is stored on a thumb drive.

Data is stored locally on the SPD laptop used during deployment. When the CINT System is used, the system automatically logs and records all calls. The software uses a file type that does not allow users to alter logs, ensuring transparency in the incidents recorded by the system. All data are stored indefinitely and used for training purposes by the HNT.

SECTION D

Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

SMC 14.18.060, § D: How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations (...).

Unauthorized deployment of the Throw Phone constitutes one of the greatest risks to civil liberties associated with this technology. The Throw Phone can only be used in the case where a person is barricaded, in crisis, or in the event of a hostage situation. Deployment into a constitutionally protected area requires warrant or warrant exception such as consent, exigent circumstances, or community caretaking/emergency.

In the only documented deployment of the Throw Phone in the past 2 years, OIG found that the technology was deployed in compliance with state law and SPD policy documented in the SIR. The HNT's log reports that the 2022 Throw Phone deployment was in response to a barricaded incident or person in crisis where officers received authorization for the deployment through consent.

Given that this technology is so rarely used, it is unlikely that the technology itself causes disproportionate impacts on certain disadvantage populations.

SECTION E

Complaints, Concerns and Other Assessments

SMC 14.18.060, § E: A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance.

Customer Service Board Comments

In 2024, there were no relevant Customer Service Board (CSB) complaints filed pertaining to this surveillance technology.

Office of Police Accountability Complaints

In 2024, there were no relevant Office of Police Accountability (OPA) complaints filed pertaining to this surveillance technology.

Internal Audits/Assessments

No internal audits or assessments of this surveillance technology were conducted in 2024.

SECTION F

Total Annual Costs

SMC 14.18.060, § F: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

SPD reported that there were no costs associated with the technology in 2024.

Non-Audit Statement This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.

Appendix A SPD Management Response

The Seattle Police Department appreciates the Surveillance Ordinance audits conducted by the Office of Inspector General. We appreciate the collaboration and support to ensure our department is appropriately using surveillance technology.