

Findings from the 2024 Surveillance Technology Equipment Reporting

*Sherri Johnson, Research Analyst
Virginia Department of Criminal Justice Services*



DCJS

Virginia Department of Criminal Justice Services

Background

HB 1496

(Jan 2024) **Surveillance Technology Registry**

(Enacted) **Surveillance technology reporting by state and local law-enforcement agencies and sheriff's departments**

Data collection process

Introduction of the legislation and process (summer 2024)

Collection of data (October 2024)

Reminder emails (Mid and late Oct)

Data collection process

Data collected:

- Agency contact (name, agency, email, phone)
- List of surveillance tech equipment listed in Code
- Other surveillance tech equipment not on the list

Primary Checklist

3.1

Instructions: Please indicate which of the listed surveillance technologies your agency/department has procured/acquired.
Answer "Yes" if it has been acquired; answer "No" if it has not been acquired.

	Yes	No
International mobile subscribed identity (IMSI) catchers and other cell site simulators	<input type="radio"/>	<input type="radio"/>
Automatic license plate readers	<input type="radio"/>	<input type="radio"/>
Electronic toll readers	<input type="radio"/>	<input type="radio"/>
Closed-circuit television cameras	<input type="radio"/>	<input type="radio"/>
Facial recognition technology, including any electronic system or service for conducting an algorithmic comparison of images of a person's facial features for the purpose of identification	<input type="radio"/>	<input type="radio"/>
Other biometric surveillance technology, including voice, iris, and gait-recognition software and databases	<input type="radio"/>	<input type="radio"/>
Mobile DNA capture technology	<input type="radio"/>	<input type="radio"/>
Gunshot detection and location hardware and services	<input type="radio"/>	<input type="radio"/>
X-ray vans	<input type="radio"/>	<input type="radio"/>
Video and audio monitoring or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras	<input type="radio"/>	<input type="radio"/>
Surveillance enabled or capable lightbulbs or light fixtures	<input type="radio"/>	<input type="radio"/>
Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network	<input type="radio"/>	<input type="radio"/>
Social media monitoring software	<input type="radio"/>	<input type="radio"/>
Through-the-wall radar or similar imaging technology	<input type="radio"/>	<input type="radio"/>
Passive scanners of radio networks	<input type="radio"/>	<input type="radio"/>
Long-range Bluetooth and other wireless-scanning devices	<input type="radio"/>	<input type="radio"/>
Radio-frequency I.D. (RFID) scanners	<input type="radio"/>	<input type="radio"/>
Software designed to integrate or analyze data from surveillance technology, including surveillance target tracking and predictive policing software	<input type="radio"/>	<input type="radio"/>

Data collection process

By November 2024

275 responses from the 335 LEAs contacted

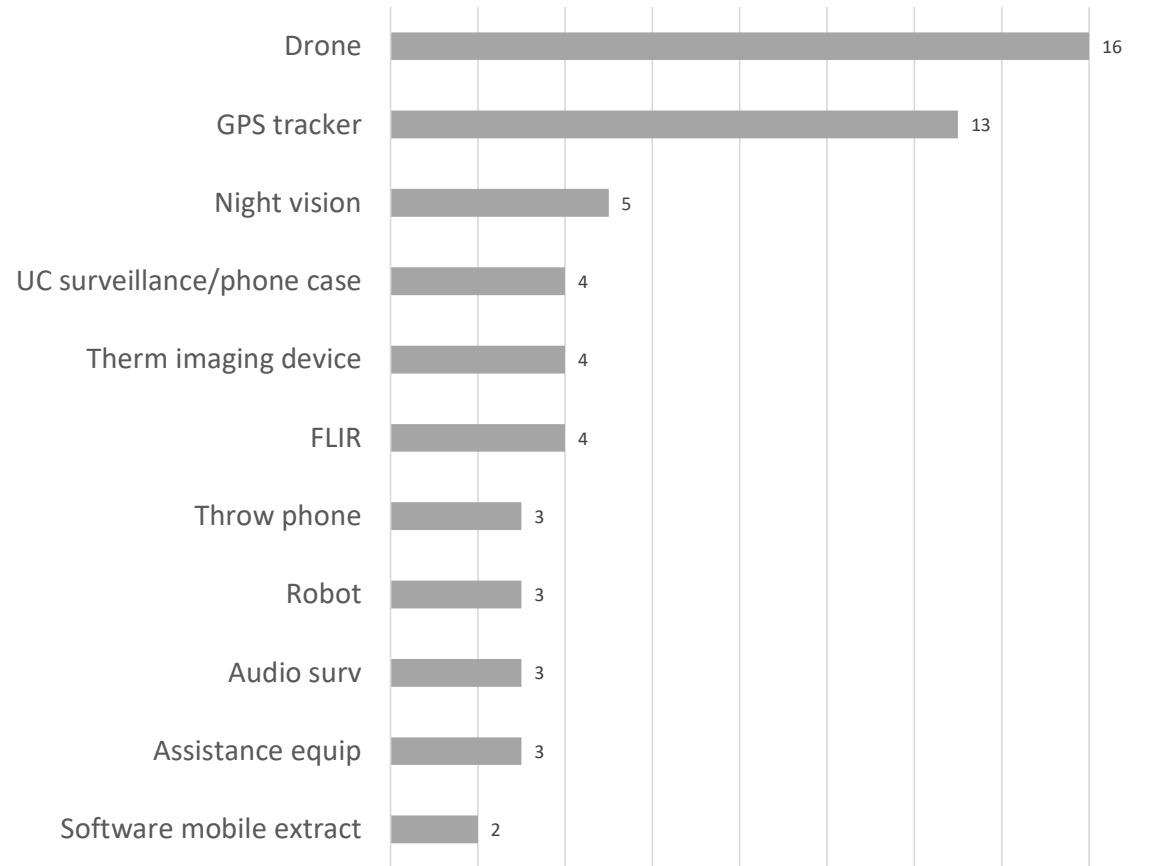
Response rate = 82%

Findings

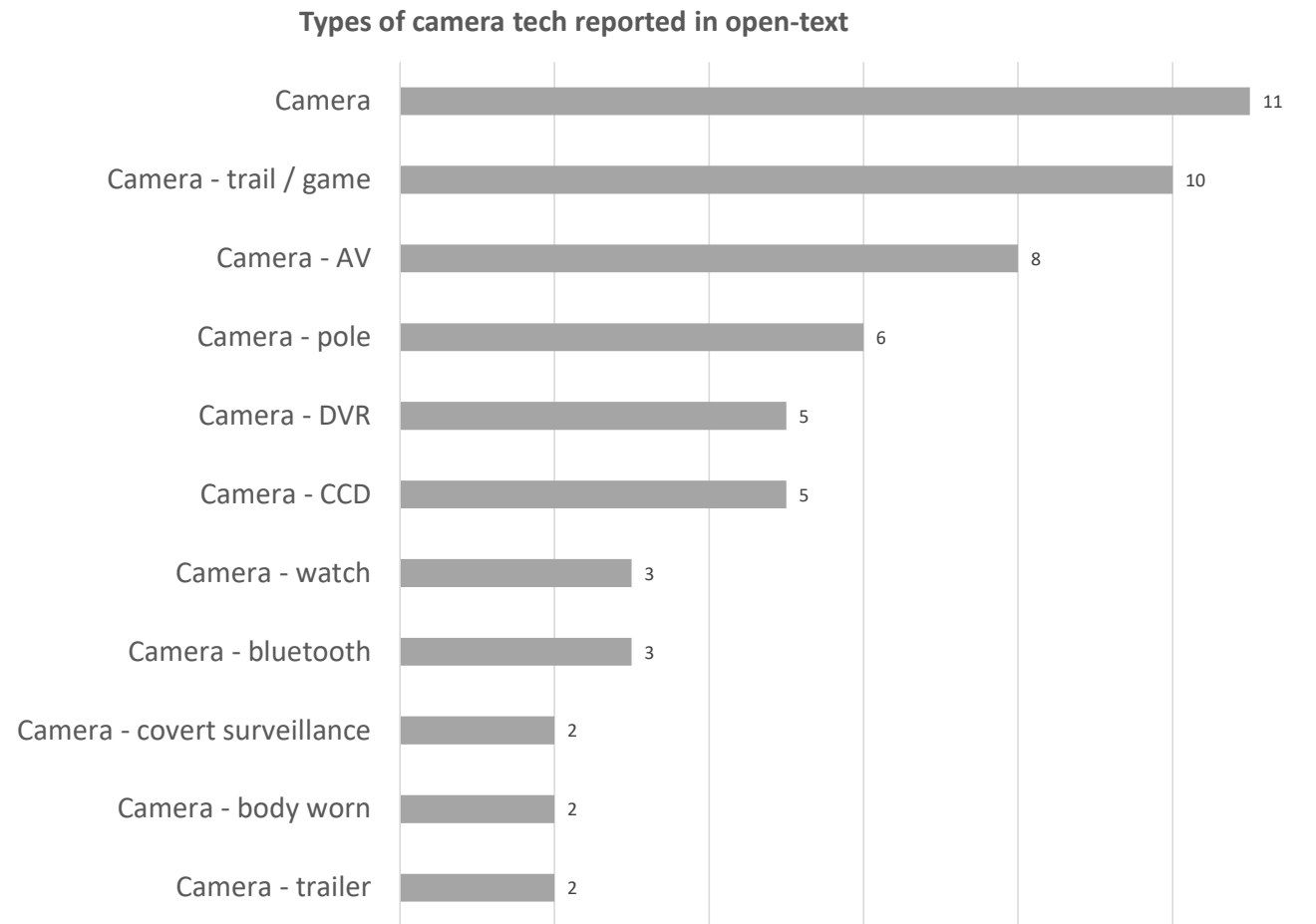
Surveillance Items	#	%
Video and audio monitoring or recording technology	240	87%
Closed-circuit television cameras (CCTV)	141	51%
Automatic license plate readers (LPR)	140	51%
Tools used to gain unauthorized access to a computer, computer service, or network	43	16%
Software designed to integrate or analyze data from surveillance technology	28	10%
Radio-frequency I.D. (RFID) scanners	14	5%
Gunshot detection and location hardware and services	14	5%
Social media monitoring software	10	4%
Through-the-wall radar or similar imaging technology	7	3%
Surveillance enabled or capable lightbulbs or light fixtures	7	3%
Facial recognition technology	7	3%
Passive scanners of radio networks	6	2%
International mobile subscriber identity (IMSI) catchers and other cell site simulators	5	2%
Long-range Bluetooth and other wireless-scanning devices	3	1%
X-ray vans	3	1%
Mobile DNA capture technology	2	1%
Other biometric surveillance technologies, including voice, iris, and gait-recognition	2	1%
Electronic toll readers	2	1%

Findings

Tech reported in open-text (not in list)



Findings



Findings

Department size analysis (based on number of sworn LEOs)

Large department	200 sworn or >	17 departments
Med department	199 – 30 sworn	96 departments
Small department	29 sworn or <	160 departments

Findings

	# depts reported	% of same size depts reported
Video and audio monitoring or recording technology		
Large dept	16	94%
Med dept	88	92%
Small dept	135	84%
Automatic license plate readers (LPR)		
Large dept	14	82%
Med dept	71	74%
Small dept	56	35%
Closed-circuit television cameras (CCTV)		
Large dept	12	71%
Med dept	57	59%
Small dept	71	44%
Tools used to gain unauthorized access to a computer, service, or network		
Large dept	9	53%
Med dept	26	27%
Small dept	8	5%

Findings

Data integration software designed to integrate or analyze data from STE		
Large dept	7	41%
Med dept	17	18%
Small dept	3	2%
Radio-frequency I.D. (RFID) scanners		
Large dept	4	24%
Med dept	6	6%
Small dept	3	2%
Social media monitoring software		
Large dept	4	24%
Med dept	5	5%
Small dept	1	1%
Gunshot detection and location hardware and services		
Large dept	4	24%
Med dept	4	4%
Small dept	6	4%
International mobile subscriber identity (IMSI) catchers and other cell site simulators		
Large dept	4	24%
Med dept	1	1%
Small dept	0	0%

Findings

Long-range Bluetooth and other wireless-scanning devices		
Large dept	2	12%
Med dept	1	6%
Small dept	0	0%

Surveillance enabled or capable lightbulbs or light fixtures		
Large dept	2	12%
Med dept	4	4%
Small dept	1	1%

Drone/unmanned aircraft		
Large dept	1	6%
Med dept	7	7%
Small dept	4	3%

Through-the-wall radar or similar imaging technology		
Large dept	1	6%
Med dept	3	3%
Small dept	3	2%

Facial recognition technology		
Large dept	1	6%
Med dept	3	3%
Small dept	3	2%

Findings

Passive scanners of radio networks			
Large dept	1		6%
Med dept	2		2%
Small dept	2		1%
Electronic toll readers			
Large dept	1		6%
Med dept	1		1%
Small dept	0		0%
Mobile DNA capture technology			
Large dept	1		6%
Med dept	1		1%
Small dept	0		0%
Other biometric surveillance technologies, including voice, iris, and gait-recognition			
Large dept	0		0%
Med dept	2		2%
Small dept	0		0%
X-ray vans			
Large dept	0		0%
Med dept	1		1%
Small dept	2		1%

Items that may require legislative changes

- Explain use of the term “unauthorized”
- Clarify time frame instructions (*annually report tech or report tech procured annually?*)
- Advise whether access to tech via third-party subscription services or other entities should be reported, add language

Items that may require legislative changes

*(xi) tools, including software and hardware,
used to gain unauthorized access to a computer, computer
service, or computer network*

Items that may require legislative changes

Lack of clarity in guidance language (time frame)

*B. All state and local law-enforcement agencies and sheriff's departments shall **provide** to the Department (DCJS) a list of all surveillance **technologies procured** by such agencies and departments **on an annual basis** by November 1 of each year. The Department (DCJS) shall also provide such information to the Virginia State Crime Commission and the Joint Commission on Technology and Science.*

Items that may require legislative changes

Language in HB 1496 requires LEAs report only what they've procured (possess), not what they may access (use)

*B. All state and local law-enforcement agencies and sheriff's departments shall provide to the Department (DCJS) a list of all surveillance technologies **procured** by such agencies and departments on an annual basis by November 1 of each year. The Department (DCJS) shall also provide such information to the Virginia State Crime Commission and the Joint Commission on Technology and Science.*

Items that may require legislative changes

Do we want LEAs to report on STE they have access to when needed but do not own?

- Third-party subscription services
- VSP or other LE
- Non-LEA sources (businesses, airport, trail/Ring cameras)

Non-statutory changes

- Provide guidance document in 2025
- Add items to list often reported in open-text (drones, GPS trackers)
- Adjust data collection tool if intent is to know about use and access, not just procurement of, STE

Non-statutory changes

Other items in list that prompted questions

- (i) international mobile subscriber identity (IMSI) catchers
and other cell site simulators*
- (ii) automatic license plate readers*
- (iii) electronic toll readers*

Non-statutory changes

Items to add to primary checklist

Drones (16)

GPS trackers (13)

Specify often-named types of cameras

Non-statutory changes

Can add skip-logic questions to the checklist of STE to collect information on ownership, access, and use of equipment

Does your agency own automatic license plate readers? (yes, no)

- If yes – did your agency use this equipment in 2025?
- If no – did your agency access this equipment via a subscription service, another LEA, or other source in 2025?

In summary, to improve Surveillance Technology Equipment reporting

- Explain language used (unauthorized) and provide guidance for listed equipment items
- Clarify time frame instruction (annually report tech or report tech procured within the year)
- Advise whether access to STE via third-party subscription services or other entities should be reported – Is intent to know who owns what, or is the intent to know who uses what?
- If intent includes knowing what STE is used/accessed, adjust data collection tool to capture
- Add STE often described in open-text section to primary checklist (drones, GPS trackers)

Sherri Johnson

Research Analyst

Virginia Department of Criminal Justice Services (DCJS)

sherri.johnson@dcjs.virginia.gov