City of Dunwoody Georgia

4800 Ashford Dunwoody Road
Dunwoody, Georgia 30338
dunwoodyga.gov | 678.382.6700

To: Members
Dunwoody City Council

From: Ginger LePage
Technology Director

Re: Dunwoody IT Security Assessment of Flock Safety
Date: 3/23/2026

Summary

As requested by Council, Dunwoody IT Department completed a Flock Safety security assessment focused on operational security, data protection, access controls, auditing, and overall risk considerations for continued use within police department operations. The assessment results are summarized in a color-coded risk matrix, identifying strengths and any items requiring ongoing monitoring or procedural reinforcement.

Based on the assessment findings, existing operational use, and proven value to public safety operations, staff recommends the City continue the contract with Flock Safety, with the noted governance and administrative controls maintained (and enhanced where applicable).

Details

1) Assessment Scope Highlights
The review considered the City's practical usage and core security/control areas commonly expected for a public-sector technology service, including:
- Governance & policy alignment (CJIS-adjacent considerations, retention expectations, internal policy fit)
- Data protection (encryption expectations, separation of duties, handling of sensitive data)
- User access & authentication (role-based access, least privilege, MFA/SSO capability as applicable)
- Audit logging & oversight (ability to review access and searches, administrative reporting)
- Operational resilience (availability, vendor support model, incident response expectations)
- Privacy & compliance administration (appropriate-use controls, documented procedures, transparency considerations)

2) Color-Coded Security Matrix (Assessment Results) Legend:
- Green = Meets expectation / Minimal risk
- Yellow = Meets with conditions / Low to Moderate risk (requires monitoring or compensating controls)
- Amber = Meets with conditions / High Risk (requires enhanced controls, auditing, and/or monitoring
- Red = Does not meet expectation / Higher risk (requires remediation)

The assessment results are separate from the agenda in a table named "FlockSafetyAssessmentMatrix.xlsx". The presentation will be added after completion.

Final Considerations

The Technology Department has determined this risk is acceptable due to several contributing considerations, such as, the users accessing the data are law enforcement meeting CJIS standards, the need for the application has been proven to be high, and there is regular auditing being conducted. Additionally, the Technology Department has found that Flock has obtained numerous security certifications including: SOC2 Type 2, CJIS, FedRamp, NDAA, VPAT, ISO 27001/27017/27018/27701/42001:2023 which do show Flock's efforts to be compliant with security standards.

#2.

Dunwoody_Council_Matrix_PD

System Inventory - GREEN

Q#	Topic (short)	Score	Risk Mitigation
Q1.1	Networks/tenants list	Green	Acceptable
Q1.2	Device inventory	Green	Acceptable
Q1.3	Use cases (pilot/operational/planned)	Yellow	Inherent
Q1.4	Integrations	Yellow	Inherent

Retention and Deletion - YELLOW

Q#	Topic (short)	Score	Risk Mitigation
Q2.1	Retention settings + exceptions	Yellow	no evidence
Q2.2	Who can change retention + approvals	Yellow	no evidence
Q2.3	Preservation / legal hold	Yellow	no evidence

Access Control, Users, MFA, roles, and lifecycle controls - GREEN

Q#	Topic (short)	Score	Risk Mitigation
Q3.1	Current user list export	Green	Acceptable
Q3.2	Non-PD direct logins	Yellow	Policy Requested - PD Agreed
Q3.3	MFA posture	Yellow	Risk - Flock
Q3.4	Account lifecycle + access reviews	Yellow	Policy Requested - PD Agreed

Sharing governance and external agency access - GREEN

Q#	Topic (short)	Score	Risk Mitigation
Q4.1	External agencies with access	Yellow	Inherent
Q4.2	Standing/self-service access	Yellow	Inherent
Q4.3	Nationwide/broad lookup enabled	Yellow	Risk - Flock
Q4.4	Review cadence + removals	Yellow	Policy Requested - PD Agreed
Q4.5	External agency searches visible to Dunwoody	Yellow	Policy Requested - PD Agreed

Audit Logs, reason codes, and supervisory oversight -YELLOW

Q#	Topic (short)	Score	Risk Mitigation
Q5.1	Audit log sample (minimum fields)	Amber	Training, Policy, Audits
Q5.2	What PD reviews + cadence + escalation	Amber	Policy Requested - PD Agreed
Q5.3	Misuse detection/investigation documentation	Yellow	Risk - Flock
Q5.4	Case number / reason code requirement	Amber	Training, Policy, Audits

Operational continuity/resilience - GREEN

Q#	Topic (short)	Score	Risk Mitigation
Q6.1	Local storage vs cloud-only + outage procedure	Yellow	Acceptable
Q6.2	Escalation path / runbook	Green	Acceptable
Q6.3	Vendor security incident notification	Green	Acceptable
Q6.3	Contract/SLA breach notification timeframe	Amber	Updated in Contract Proposal

Policy, Council transparency artifacts, and public FAQs - GREEN

Q#	Topic (short)	Score	Risk Mitigation
Q7.1	PD policies/SOPs	Yellow	Policy Requested - PD Agreed
Q7.2	Governance requirements (PD input)	Yellow	Policy Requested - PD Agreed
Q7.3	Top 10 public/Council questions (FAQ)	Green	Acceptable

Dunwoody_Council_Matrix_Flock

SOC2 scope, coverage, and AWS carve-out - YELLOW

#2.

Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q1.1	Current SOC 2 Type II + scope	Yellow	Updated/inclusive SOC2
Q1.2	Cloud services/regions + carve-out vs inclusive	Yellow	no evidence
Q1.3	Shared responsibility matrix	Green	Acceptable
Data lifecycle, transmission, encryption, and ownership - GREEN			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q2.1	Data storage/processing + data flow	Yellow	Risk - Flock
Q2.2	Encryption at rest + key mgmt	Green	Acceptable
Q2.3	Encryption in transit	Yellow	Acceptable
Q2.4	Device-to-cloud/cloud-to-client protections	Yellow	Acceptable
Q2.5	Contract language: City ownership + secondary use limits	Green	Updated in Contract Proposal
Access Control, remote access, MFA, PAM, sessions, credentials, and admin access - GREEN			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q3.1	Vendor remote access controls	Green	no evidence
Q3.2	MFA enforcement	Green	no evidence
Q3.3	PAM (JIT, vaulting, break-glass, recording)	Green	no evidence
Q3.4	Provisioning/deprovisioning + RBAC + SoD	Green	no evidence
Q3.5	Credential storage/password policy/session security	Green	no evidence
Q3.6	No backdoor accounts	Green	no evidence
Sharing model, oversight controls, and auditablility - YELLOW			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q4.1	Sharing model (standing access vs approvals)	Yellow	Acceptable
Q4.2	Granular sharing restrictions	Green	Acceptable
Q4.3	Audit log schema + exportability + external agency activity	Green	Acceptable
Q4.4	Reason-for-search/case number enforceable	Yellow	Risk - Flock
Q4.5	Controls against credential sharing	Green	no evidence
Q4.6	Audit log field reductions since 10/1/2025	Green	no evidence
Data deletion, termination/exit, backups, and recovery - YELLOW			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q5.1	Offboarding/termination export/deletion confirmation	Green	Acceptable
Q5.2	Deletion permanence + backup retention	Red	Update requested
Q5.3	DR/BCP (RPO/RTO + test frequency)	Green	Risk - Flock
Q5.4	Restore authorization + logging	Green	Acceptable
Q5.5	Resilience if cloud access is down (device buffering)	Green	Acceptable
Third Parties, subprocessors, tenancy, and disclosures to government - GREEN			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q6.1	Subprocessor list (purpose/access/monitoring)	Yellow	no evidence
Q6.2	Data residency (US-only)	Green	Acceptable
Q6.3	Tenancy/isolation controls	Green	no evidence
Q6.4	Government/legal requests + customer notice	Green	Updated in Contract Proposal
Security operations, vulnerability management, patching, DDoS, and physical security - YELLOW			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q7.1	Preventive security controls	Green	no evidence
Q7.2	Vulnerability scanning + remediation SLAs	Green	no evidence
Q7.3	Pen test exec summary + remediation status	Green	no evidence

Q7.4	Patch/update cadence + firmware authenticity	Green	no evidence
Q7.5	DDoS mitigation + SLA	Green	no evidence
Q7.6	Physical security	Green	Acceptable
Incident response, breach history, monitoring, and customer communications - AMBER			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q8.1	Breach/security incident history	Red	Risk - Flock
Q8.2	Monitoring stack + anomalous search detection	Green	no evidence
Q8.3	Customer notification commitments	Amber	Updated in Contract Proposal
CJIS alignment & Georgia law-enforcement governance - YELLOW			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q9.1	CJIS mapping/boundary	Yellow	no evidence
Q9.2	Feature gating/misuse controls	Yellow	no evidence
Business continuity, insurance, and accountability - YELLOW			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q10.1	DR/BCP existence + last test	Yellow	no evidence
Q10.2	Cyber liability insurance + COI	Green	Acceptable
Q10.3	Security accountability/org	Green	Acceptable
Q10.4	Security training program	Green	no evidence
Q10.5	Threat intelligence process	Green	no evidence
City operational integrations (notifications/email) - YELLOW			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q11.1	SMTP integration security	Green	no evidence
Q11.2	Role accounts for notifications	Amber	not enough info
Contractual governance requirements (Councilmember items) + validation of risk signals- GREEN			
Q#	**Topic (short)**	**Score**	**Risk Mitigation**
Q12.1	Freeze online T&Cs / order of precedence clause	Amber	Updated in Contract Proposal
Q12.2	No secondary use / AI training without approval (clause)	Green	Updated in Contract Proposal
Q12.3	Sharing governance/audit commitments	Green	Acceptable
Q12.4	Mandatory enforceable controls (MFA/logs/breach)	Yellow	no evidence
Q12.5	Liability expectations	Green	Updated in Contract Proposal

City of Dunwoody Georgia

Technology

Technology Department's Security Assessment of Flock Safety with Council Matrix

Background

- Flock Safety was founded in 2017 to address neighborhood crime utilizing license plate reading cameras.
- Flock Safety has become the "go-to" product for Law Enforcement Agencies across the Nation due, in part, to it's data sharing model.
- Flock Safety is the umbrella company that includes numerous modules and applications (a few examples):

  -License Plate Reader Cameras
  -Drones
  -Flock OS
  -Flock (OS) 911
  -Nova
- Dunwoody PD (DPD) utilizes many of Flock Safety's products and the DPD is looking to renew the contract for Flock (OS) 911.
- Due to some recent security concerns, Council requested the Technology Department complete a Security Assessment of Flock Safety.

Flock (OS) 911

- Flock (OS) 911 allows responding officers to hear 911 calls, real time.

- Call Taking process without Flock (OS) 911:
  1. Call Taker (CT) asks the questions
  2. CT inputs data into CAD
  3. Dispatcher reads CAD and announces data via radio
  4. Officer asks followup question
  5. Dispatcher enters followup question into CAD
  6. CT reads CAD and starts back at 1.

- Call Taking process with Flock (OS) 911:
  1. Call Taker (CT) asks the questions
  2. Officer hears response real time and can ask Dispatcher real time followup questions
  3. Dispatcher relays to CT and starts back at 1.

Flock (OS) 911 Security Assessment

Based our review, as it relates to Flock (OS) 911 specifically, the Technology Department found there to be no abnormal risks identified with this product beyond that which would be identified with using any similar product. We would rank this product as a Green Level (Meets Expectations / Minimal Risk) in the Council Matrix.

Flock Safety Security Assessment

The Technology Department acknowledges Council’s request for a comprehensive security assessment of Flock Safety. Over the past month, we have reviewed available information, completed many interviews, and developed a **Council Matrix** to clearly summarize and simplify our findings.

Color-Coded Council Matrix (Assessment Results) Legend:

- Green = Meets expectation / Minimal risk
- Yellow = Meets with conditions / Low to Moderate risk (requires monitoring or compensating controls)
- Amber = Meets with conditions / High Risk (requires enhanced controls, auditing, and/or monitoring
- Red = Does not meet expectation / Higher risk (requires remediation)

* Note: To meet the condition of any color grade, both criteria must be met.

Flock Safety Security Assessment

For simplicity reasons, the Council Matrix is broken down into six (6) main categories:

1. Governance & Policy Alignment (CJIS-adjacent, retention expectations, internal policy)
2. Data Protection (encryption, handling sensitive data)
3. User Access & Authentication (Role-Based Access Control, Multi-Factor Authentication, Single Sign On)
4. Audit Logging & Oversight (review of access/searches, admin reporting)
5. Operational Resilience (availability, support model, incident response)
6. Privacy & Compliance Administration (appropriate-use controls, documented procedures, transparency)

Governance & Policy Alignment

(CJIS-adjacent, retention expectations, internal policy fit)

1. CJIS alignment – Flock has CJIS Security Certification
2. Retention/legal hold governance - DPD operations have established workarounds but not automated in the platform
3. Formal review cadence for sharing relationships – DPD policy updates

#2.

Data Protection

(encryption, handling sensitive data)

1. Encryption at rest/in transit is clearly described
2. Tenancy isolation controls are described
3. Labelled yellow due to no supportive evidence provided for several categories.

User Access & Authentication

(Role-Based Access Control, Multi-Factor Authentication, Single Sign On)

1. Flock asserts MFA enforced and RBAC exists for Admins
2. Agencies manage their own users MFA
3. DPD utilizes MFA

Audit Logging & Oversight

(review of access/searches, admin reporting)

1. This is dominated by the standing/self-service sharing model which is intrinsically higher oversight risk
2. DPD has agreed to address multiple audit/oversight items via training, auditing, and policy
3. Flock has agreed to consider adding “Real Time Alerting” on potential misuse

Operational Resilience

(availability, support model, incident response)

1. DR targets are stated (RPO 1 hr / RTO 24 hrs)
2. Single-provider dependency concern
3. Flock states “no breaches in last 3 years,” but there has been publicized camera breaches
4. Adding definitions and documentation to the contract for “Breach”

Privacy & Compliance Administration

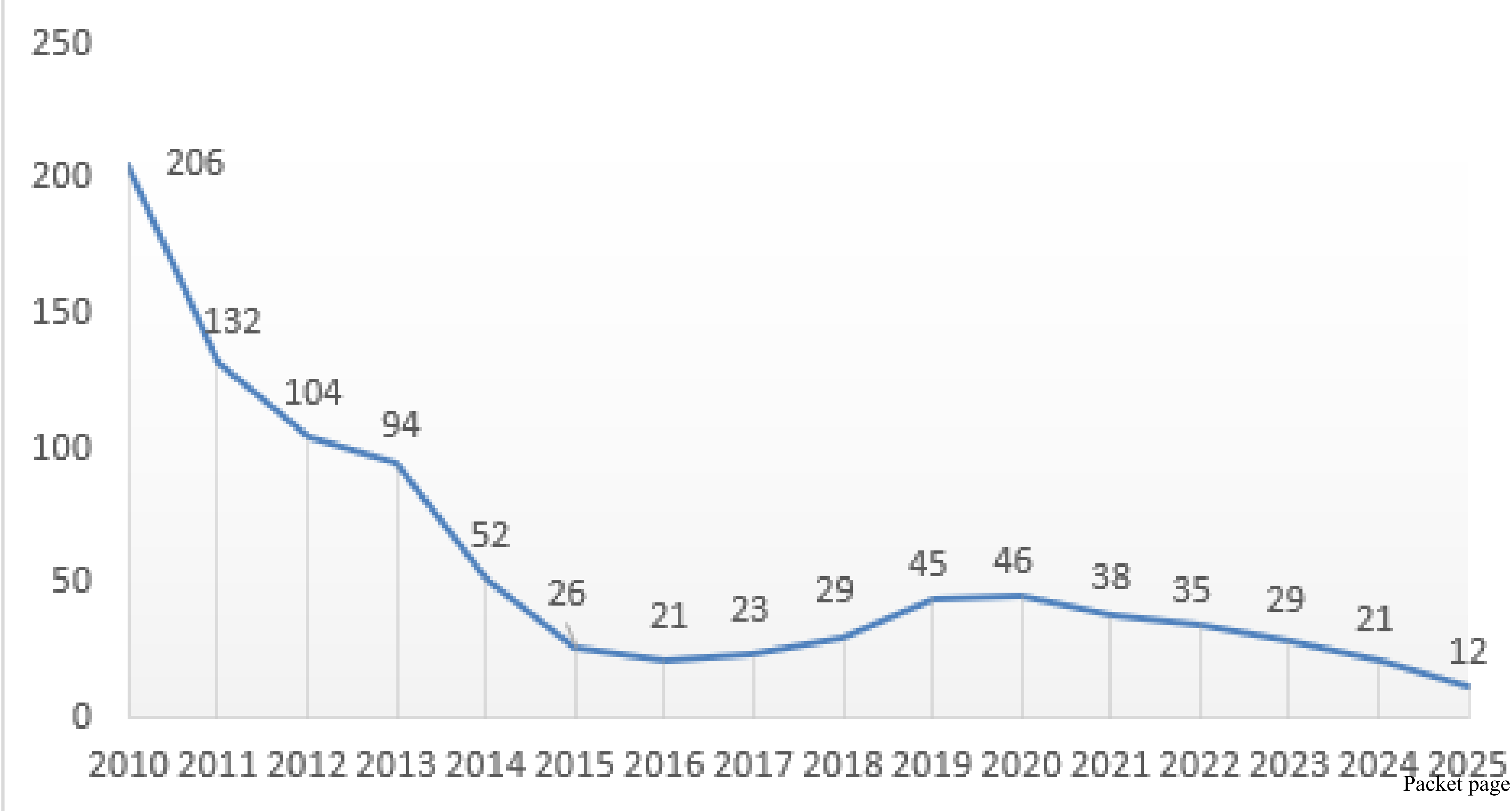
(appropriate-use controls, documented procedures, transparency)

1. Master Service Agreement is being formalized and will not be changeable without completing a new review
2. DPD is making updates to Policy for External auditing

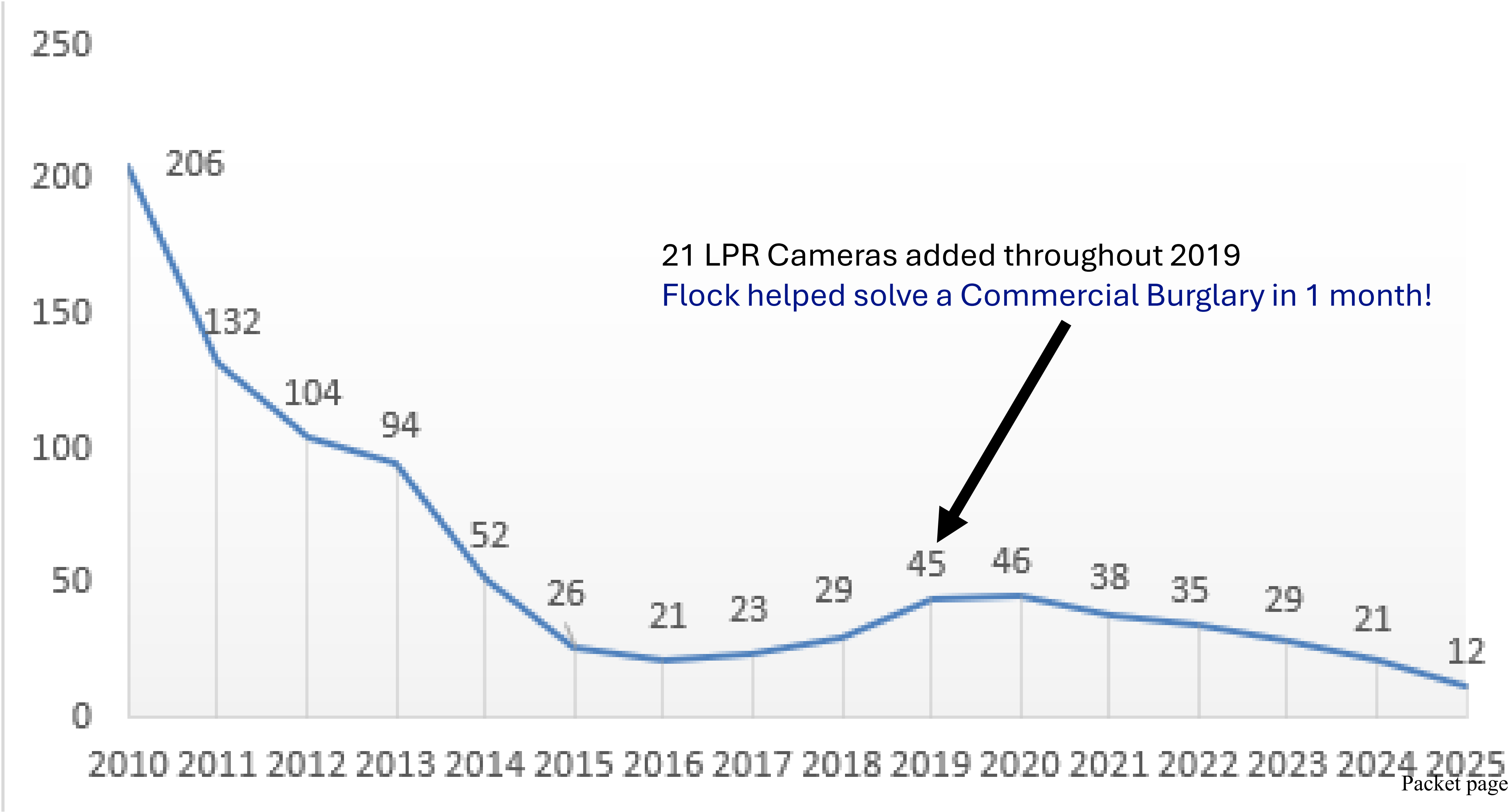
Risk vs. Reward

When completing a Security/Risk Assessment, a huge portion of the analysis is the “Risk Vs. Reward”.   The technology department worked with DPD to answer questions about “Reward”.

Average Days to Close



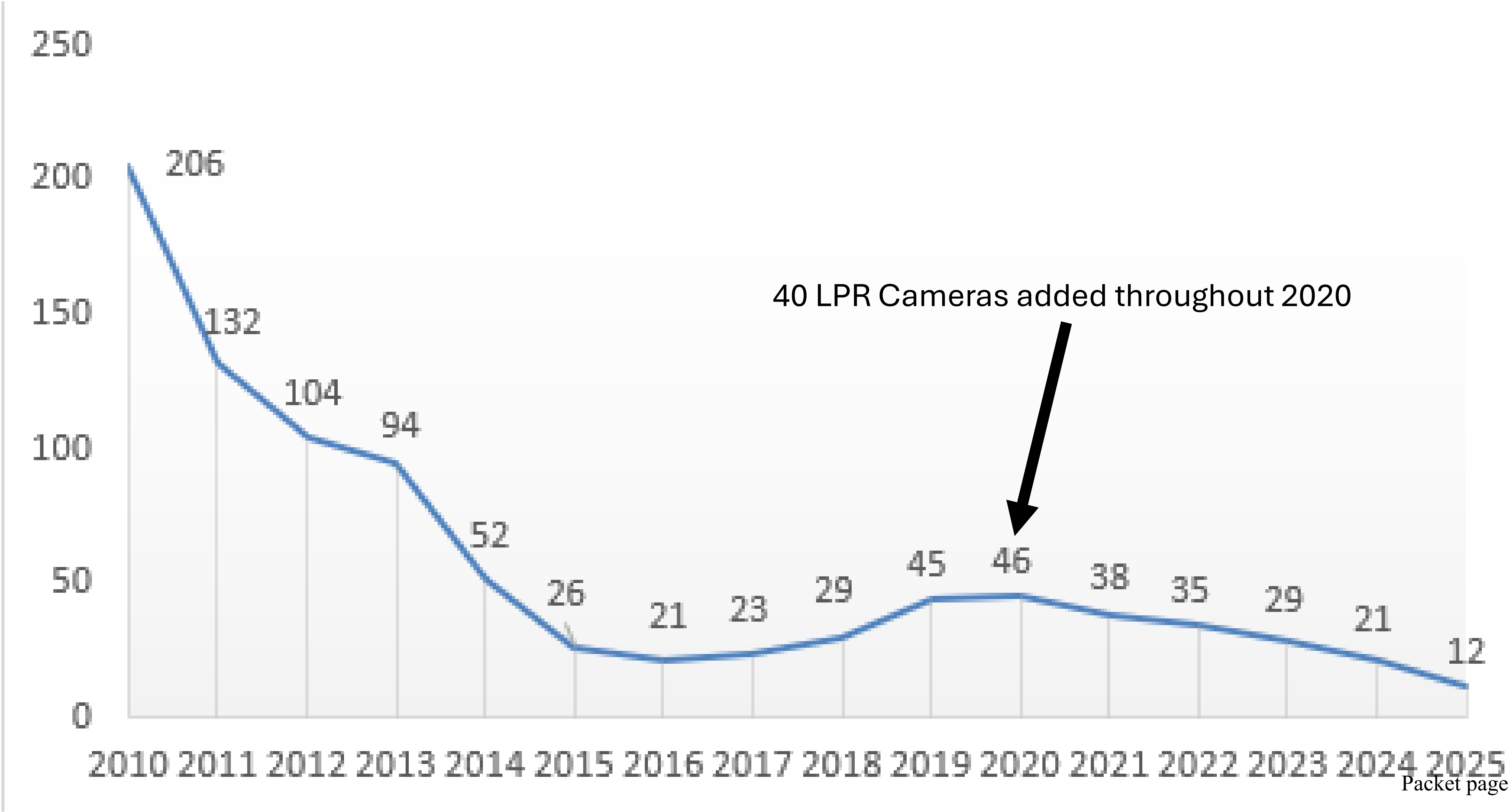
Average Days to Close



21 LPR Cameras added throughout 2019

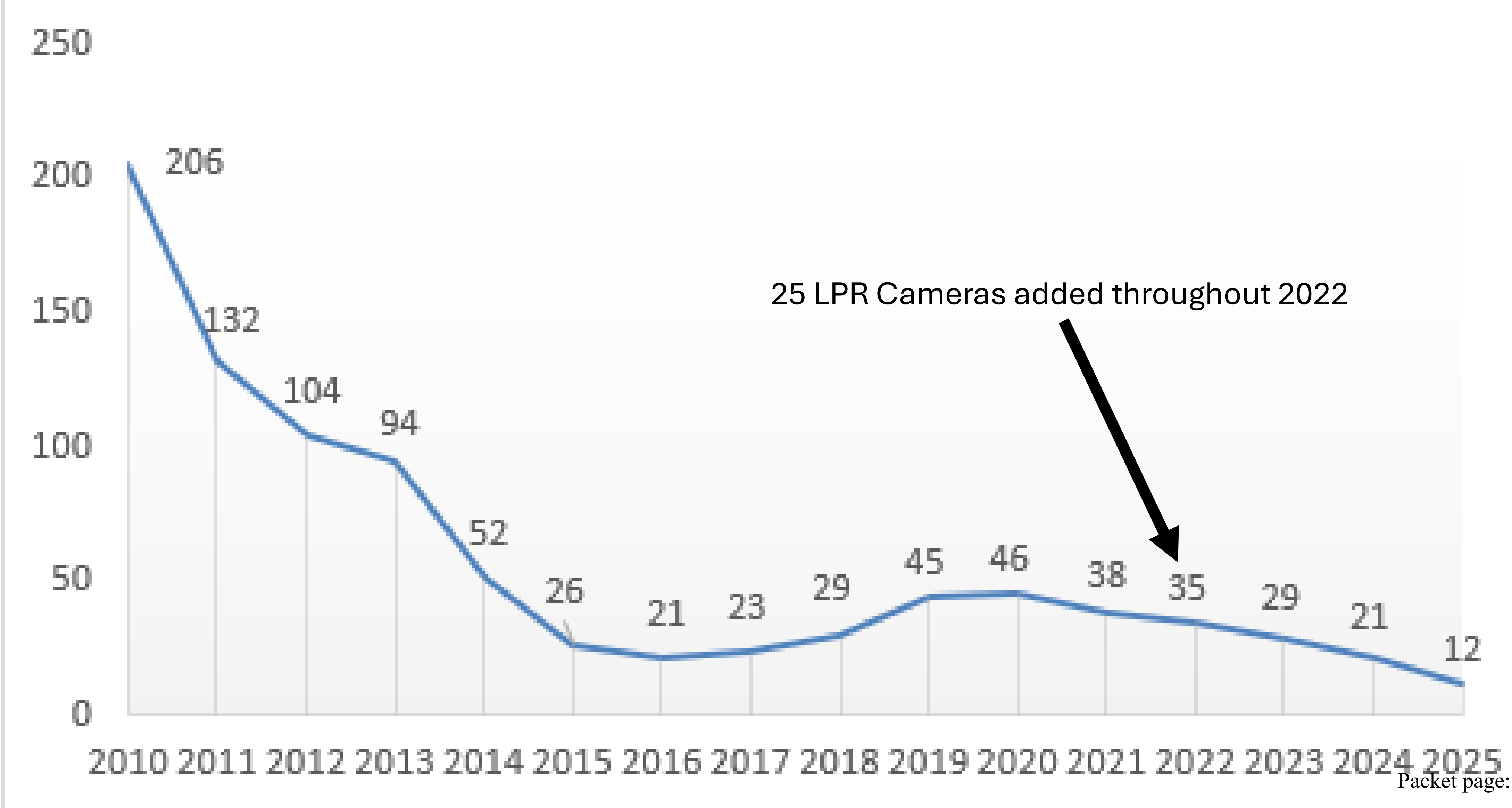
Flock helped solve a Commercial Burglary in 1 month!

Average Days to Close



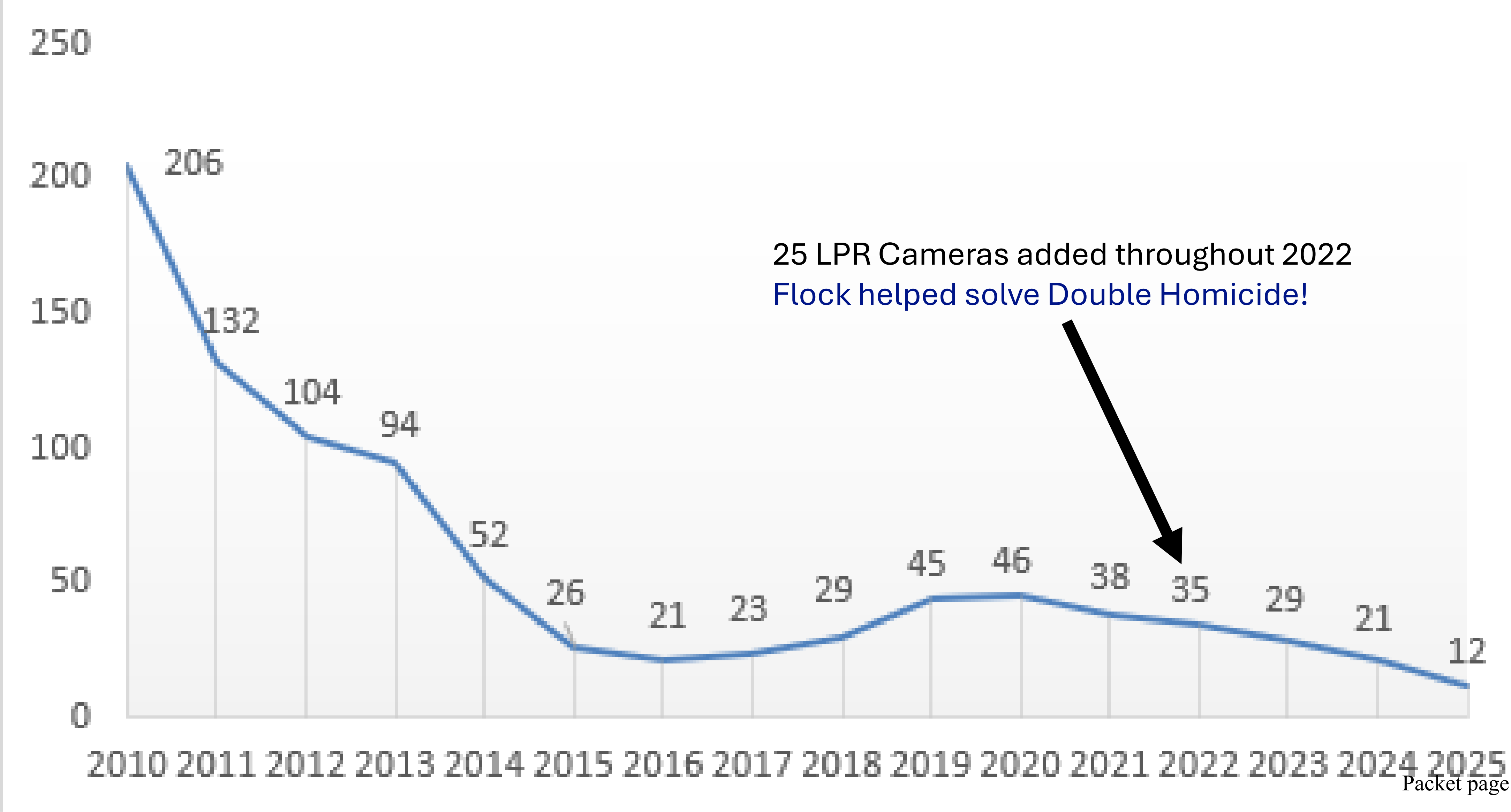
40 LPR Cameras added throughout 2020

Average Days to Close



25 LPR Cameras added throughout 2022

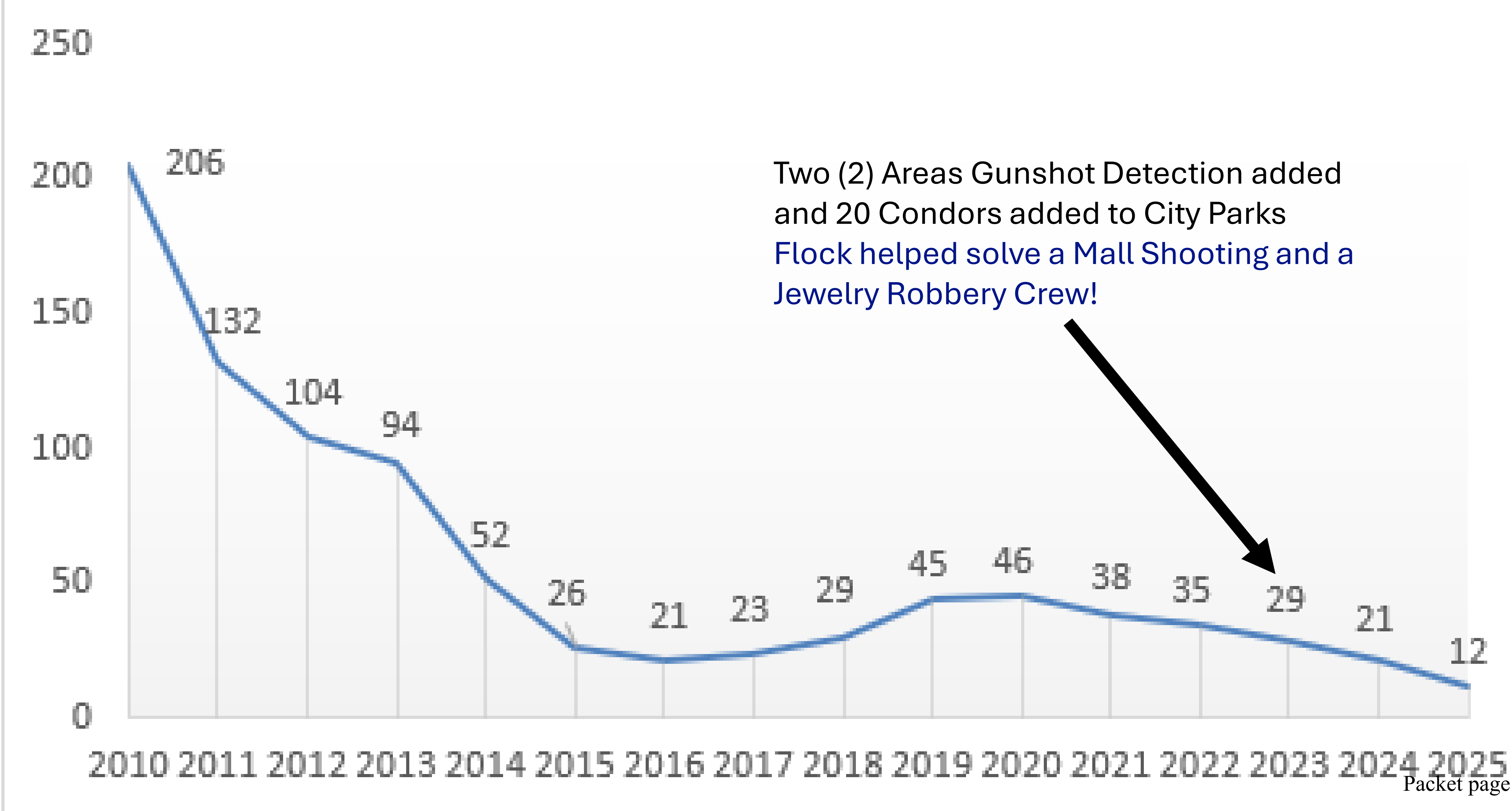
Average Days to Close



25 LPR Cameras added throughout 2022

Flock helped solve Double Homicide!

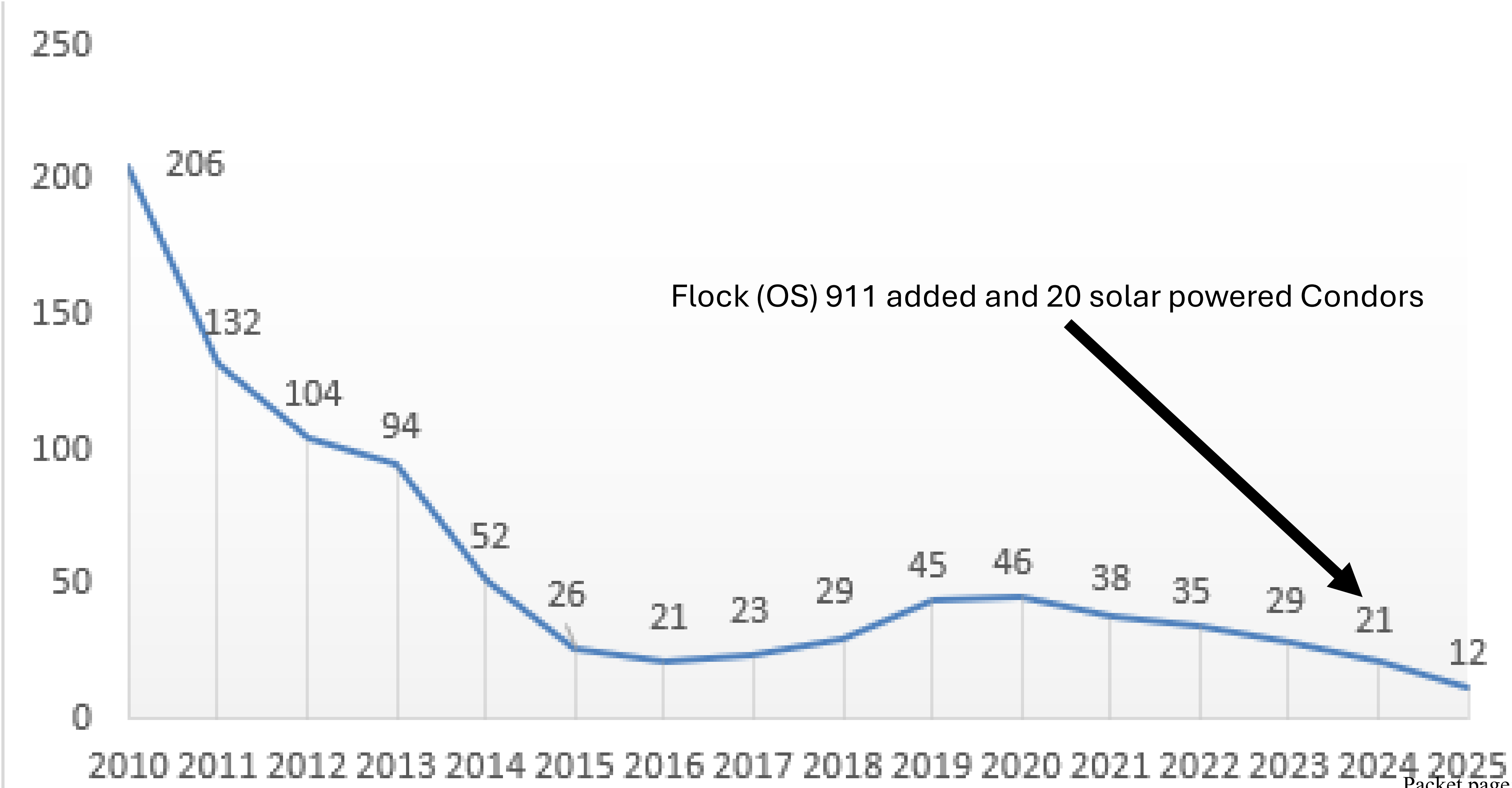
Average Days to Close



Two (2) Areas Gunshot Detection added and 20 Condors added to City Parks

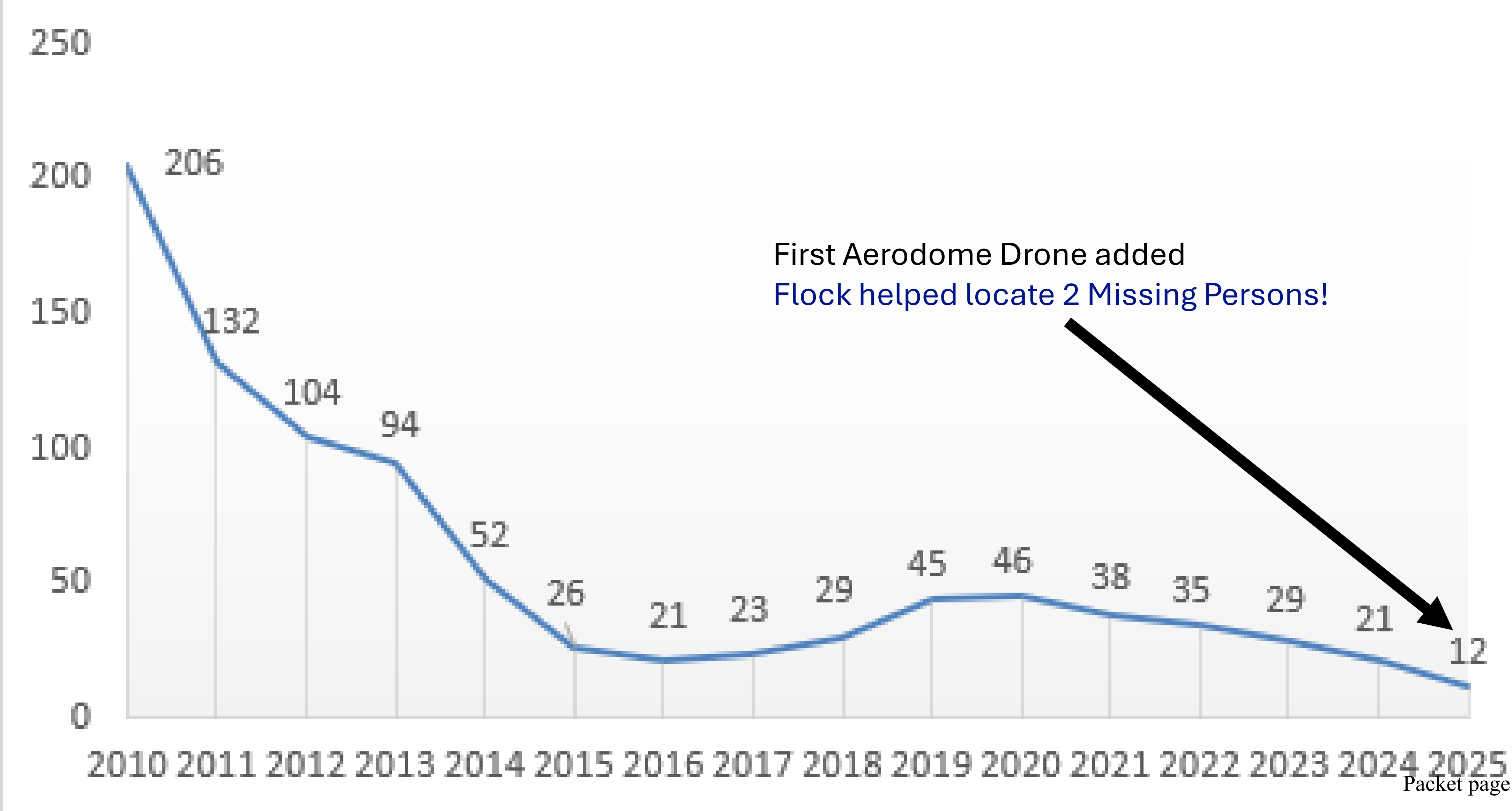
Flock helped solve a Mall Shooting and a Jewelry Robbery Crew!

Average Days to Close



Flock (OS) 911 added and 20 solar powered Condors

Average Days to Close



First Aerodome Drone added

Flock helped locate 2 Missing Persons!

FAQs

1.) “Is this system tracking me or building a database of everywhere I go?”

No. Flock is not GPS, and it does not track vehicles in real time like a phone app would; it records a “detection” only when a vehicle passes a camera location. Those detections can be searched later (within the 180-day retention period) when there is a legitimate law-enforcement purpose. We do not use the system to monitor residents’ day-to-day routines, and all searches are logged and can be audited.

FAQs

2.) “What exactly is being captured—license plates only, or photos of drivers/passengers too?”

Flock captures an image of the vehicle area (typically the rear/side) and reads the license plate when it can. The image is mainly used to identify the vehicle and plate, and it may also note general vehicle descriptors like color, type, and make/model characteristics. The system is not designed for facial recognition, and we do not use it to identify drivers or passengers by their faces.

#2.

FAQs

3.) “Who can access the data, and how do you prevent misuse?”

Access is limited to authorized, trained personnel who need it to perform official duties. Each search is logged (including who searched, when, and what they searched), and those logs can be reviewed to confirm the system is being used appropriately. If someone were to use the system for personal reasons, it would be treated as a serious policy violation and could result in disciplinary action—up to and including termination—and potentially a criminal investigation, depending on the circumstances.

FAQs

4.) “How long do you keep the data, and can it be used for ‘minor’ issues?”

Detections are retained for 30 days and then automatically deleted, unless specific records are saved as evidence in an individual case consistent with law and policy. Our intent is to focus use on legitimate public-safety needs—for example, stolen vehicles, vehicles connected to crimes, missing persons cases, or suspect vehicles.

FAQs

5.) “Is this legal, and what privacy protections are in place—especially in Georgia?”

Yes. License plates are displayed in public, and courts have generally treated plate and vehicle observations in public view as information law enforcement may lawfully observe and document. Even so, we take privacy seriously. We follow written policies that define permitted uses, limit who can access the system, set retention timeframes, and require audit logs to deter and detect misuse. We also comply with applicable Georgia law and public records requirements, including protecting information that is exempt from release (for example, details that could compromise an active investigation or sensitive victim-related information).