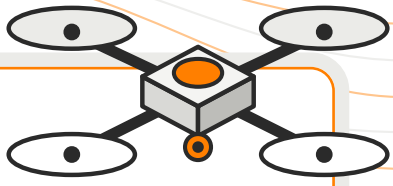
Security Built Into the Foundation of a Drone Program

Drone operations, cybersecurity, and operational resilience

For public safety, private security, and critical infrastructure leaders

white paper



Executive summary

A drone program connects drones, docking stations, remote pilots, cloud services, live video feeds, and incident command. Security works best when it protects that entire operating chain. A compromised account can expose an active incident, and an altered mission or interrupted command link can create a flight safety event. Hosting location and hardware eligibility are important parts of the assessment, and a complete review also covers access, flight execution, and recovery.

October 2026 was Cybersecurity Awareness Month, and the practical next step is to turn awareness into recurring controls: strong authentication, deliberate sharing, verified updates, rehearsed flight contingencies, and accountable recovery. The National Cybersecurity Alliance chose the 2026 theme “Don’t Make It Easy for Them.” [1] For drone operators, this theme encourages reducing opportunities for misuse while maintaining the safeguards that keep each drone safe.

Inside this paper

1 The VOTIX vision 3
2 Safeguards and responsibility 4 to 5
3 Regulations and eligibility 6 to 7
4 Six areas for a secure program 8
5 Governance and system map 9
6 Flight safety 10 to 11
7 Collaboration, data, and AI 12 to 13
8 Respond and recover 14
9 Exercise and improvement cycle 15
10 Procurement questions 16
11 Conclusion and references 17

Turn awareness into recurring controls.

“Don’t Make It Easy for Them.”
National Cybersecurity Alliance, 2026 theme

© 2026 VOTIX. All Rights Reserved.

Executive summary

Four Evaluation Areas, **Two Essential Disciplines**

VOTIX's vision of hardware-agnostic automation, coordination, and remote operation offers a useful foundation and best-practice reference for this work. Its management, streaming, and flight capabilities connect operational workflows and extend coordination across incident participants. The security opportunity is to apply consistent governance across those connections and to validate the protections of each drone, integration, and deployment. [2 to 4]

This paper expands four evaluation areas: infrastructure, hardware eligibility, access control, and documentation. It adds two essential disciplines: secure flight execution and incident resilience. The paper focuses on United States programs and separates legal obligations from recommended practices. Regulatory references reflect sources reviewed on November 4, 2026, and every purchasing or operating decision benefits from a fresh review of applicability.

Six areas at a glance

EVALUATION AREAS

- Infrastructure
- Hardware eligibility
- Access control
- Documentation

ESSENTIAL DISCIPLINES

- Flight execution
- Resilience

The leadership decision

Approve drone operations as a joint aviation, cybersecurity, privacy, and procurement responsibility. Require evidence for the deployed configuration, assign owners for residual risk, and test the response to failure before scaling automated or remote missions.





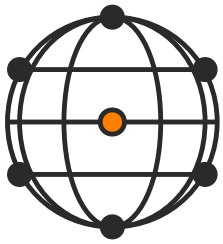


© 2026 VOTIX. All Rights Reserved.

The VOTIX Vision and the Security Boundary

An Operating Layer for **Drone Operations**

VOTIX is a Drone Operating platform that connects the moving parts of drone operations. This approach supports an enterprise objective: coordinating missions and resources across supported hardware, so workflows stay independent of any single drone vendor. Hardware flexibility can reduce switching effort, and migration benefits from compatibility checks, training, flight validation, and approval review. [2]



Three capabilities, three places to apply program controls

VOTIX MANAGE



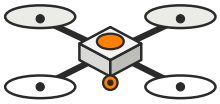
VOTIX MANAGE provides planning, checklists, scheduling, fleet records, analytics, and flight logbooks.

STREAM



STREAM supports live video and telemetry collaboration.

FLY



FLY supports internet-based remote command and control, automation, payload operation, and drone-in-a-box integration.

These capabilities offer clear places to apply program controls, and their availability and behavior depend on the specific drone, firmware, subscription, and integration. [3]

Situation Rooms



VOTIX's newest technology, SITUATION ROOMS, brings drone and other video feeds, voice, chat, and shared tactical mapping into a collaborative command environment. This can improve shared awareness and highlights the value of participant identity, access duration, and clear control authority. [4]

Programs benefit from evaluating permission to observe an incident separately from permission to command a drone or change a mission.

© 2026 VOTIX. All Rights Reserved.

The VOTIX Vision and the Security Boundary

Documented Safeguards and **Deployment Assurance**

VOTIX is built for public safety, where trust is part of the mission. Our security program follows the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and our published privacy policy documents the safeguards that support it. [5]



Hosted in the United States

The cloud infrastructure supporting VOTIX maintains independent third-party attestations, including SOC 2, ISO/IEC 27001, and FedRAMP authorizations at the provider level.

Protected end to end

Data is encrypted in transit between the drone, the cloud, and every operator screen, and encrypted at rest across the cloud infrastructure.

Access by role, by design

Role-based access control follows least privilege, so each person receives the access their role requires, and each agency operates in its own isolated workspace.

Decisions enforced on the server

Authorization, licensing, and flight-gating rules are evaluated and enforced on our servers, so the browser carries the interface and the server holds the authority. This protects the integrity of every pre-flight check and every launch decision.

Visibility at all times

Centralized logging and monitoring track platform health and security events, which supports a fast response and a clear audit trail.

People and process

Security is part of how our team works every day. Access is granted by role and removed promptly when a team member leaves, and changes to the platform follow a reviewed release process.

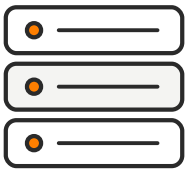
We work with agencies that operate under criminal justice information requirements to support their assessment.

© 2026 VOTIX. All Rights Reserved.

The VOTIX Vision and the Security Boundary

Deployment Review and **Shared Responsibility**

A deployment review benefits from establishing the exact hosting regions, backup and recovery locations, support access, subprocessors, encryption boundaries, and contractual commitments. Hosting in the United States is one part of a complete assessment, which also confirms tenant isolation, service continuity, suitability for criminal justice information, and protection of each drone's radio link. Cloud provider attestations complement a review of the Drone Operating platform application and the customer configuration.



A shared responsibility model

Drone Operating platform

The Drone Operating platform should provide system architecture, security evidence, supported configurations, and service commitments.

Drone and dock suppliers

Drone and dock suppliers document device security and failure behavior.

The operator

The operator owns mission authorization, personnel permissions, endpoint management, legal collection limits, and operating procedures.

Integrators and partners

Integrators and partner agencies define explicit responsibilities for their connections and access.

Recording these boundaries before launch keeps every participant aligned during an incident.

© 2026 VOTIX. All Rights Reserved.

Regulations and Eligibility Call for Separate Decisions

FCC Authorization and **Fleet Planning**

The Federal Communications Commission (FCC) added foreign-produced drones (UAS) and critical components to its Covered List on December 22, 2025. Its announcement explains that the action blocks new equipment authorizations for covered devices and preserves the use of lawfully acquired drones, along with the treatment of previously authorized models. Fleet planning benefits from confirming eligibility for each drone, agency, and funding source individually. [6]

FCC exceptions have included Blue UAS Cleared List equipment, qualifying domestic end products, and device-specific Conditional Approvals. Published notices attach conditions and, for certain exceptions, dates. The FCC's August 2026 notice explains that UAS Conditional Approvals continue subject to onshoring commitments and updated vetting. Matching the exact model and components to the operative notice gives programs a reliable eligibility picture. [7, 8]

The regulatory picture continues to develop. A July 2026 FCC proceeding sought comment on restricting the importation and marketing of certain previously authorized foreign-produced military-grade UAS and components. A proposal becomes a prohibition when the FCC adopts it. Procurement teams can check subsequent orders and effective dates before committing to replacement drones, thermal or light detection and ranging (LiDAR) systems, docks, and spares. [9]

Timeline of the actions described

Dec 22, 2025

Foreign-produced drones (UAS) and critical components added to the FCC Covered List. [6]

July 2026

FCC proceeding seeks comment on restricting importation and marketing of certain previously authorized foreign-produced military-grade UAS and components. [9]

August 2026

FCC notice explains that UAS Conditional Approvals continue, subject to onshoring commitments and updated vetting. [8]

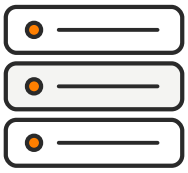
Matching the exact model and components to the operative notice gives programs a reliable eligibility picture.

© 2026 VOTIX. All Rights Reserved.

Regulations and Eligibility Call for Separate Decisions

Federal Procurement and **Funding Restrictions**

The American Security Drone Act restrictions implemented in Federal Acquisition Regulation (FAR) 40.202 operate separately from FCC equipment authorization. The FAR addresses procurement, operating services, and the use of federal funds involving drones manufactured or assembled by American Security Drone Act-covered foreign entities, subject to applicable exemptions, exceptions, and waivers. The Federal Acquisition Security Council (FASC) maintains the list of those entities, and the regulation refers to their drones as FASC-prohibited UAS. For a grant-funded program, the responsible grants or contracting official can help review the statute, award conditions, agency guidance, and state restrictions. A dedicated review of these restrictions complements FCC authorization and any general compliance statement from a supplier. [10]



Aviation Authority and **Information Obligations**

Aviation authority

Programs use the applicable Federal Aviation Administration (FAA) operating framework and specific authorizations, including any Part 107 waiver or public-agency certificate of waiver or authorization (COA). Remote operation capability works together with the required authorization for beyond visual line of sight (BVLOS) flight. FAA sources reviewed describe Part 108 as a proposed framework, so programs confirm any final rule and effective date before changing operations. Remote ID under Part 89 is a separate identification requirement that serves a distinct purpose from command authentication and cybersecurity practices. [11, 12]

Information obligations

For criminal justice information, determine whether the actual data and workflows trigger federal security policy requirements, and then involve the agency's information security authority. Drone video is classified according to the data and workflows involved, so each program confirms the classification of its own recordings. Applicable privacy law, evidentiary duties, public records rules, retention schedules, and legal holds guide collection and disclosure. Programs operating outside the United States repeat the review under local aviation and data protection requirements. [13]

Remote operation capability works together with the required authorization for beyond visual line of sight (BVLOS) flight.

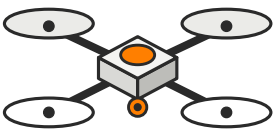
© 2026 VOTIX. All Rights Reserved.

Six areas

Six Areas for a **Secure Drone Program**

The original four areas work best when assessed alongside flight execution and resilience. The recommendations below are evaluation criteria that help program owners confirm which controls come from VOTIX, from suppliers, or from the operating agency.

Area	Required decision	**Evidence to examine**
Infrastructure	Which systems may handle each data class	Data flow and trust boundaries; hosting and backup regions; key and support access; tenant isolation testing
Hardware eligibility	Which exact configurations may be bought and flown	Model and component inventory; firmware baseline; funding restrictions; dated eligibility review
Access control	Who may observe, command, administer, and export	Role demonstration; authentication settings; guest revocation; service account scope; access reviews
Documentation	How claims become documented evidence	Control matrix; assessment scope and dates; vulnerability process; contracts; retained configuration records
Flight execution	How unauthorized actions and failures are contained	Command authority and handover tests; link and navigation contingencies; signed update evidence where supported
Resilience	How safe operation and trusted service are restored	Incident playbook; recovery objectives; restore test; alternate coordination procedure; return to service approval



The original four areas work best when assessed alongside flight execution and resilience.

© 2026 VOTIX. All Rights Reserved.

Six Areas for a Secure Drone Program

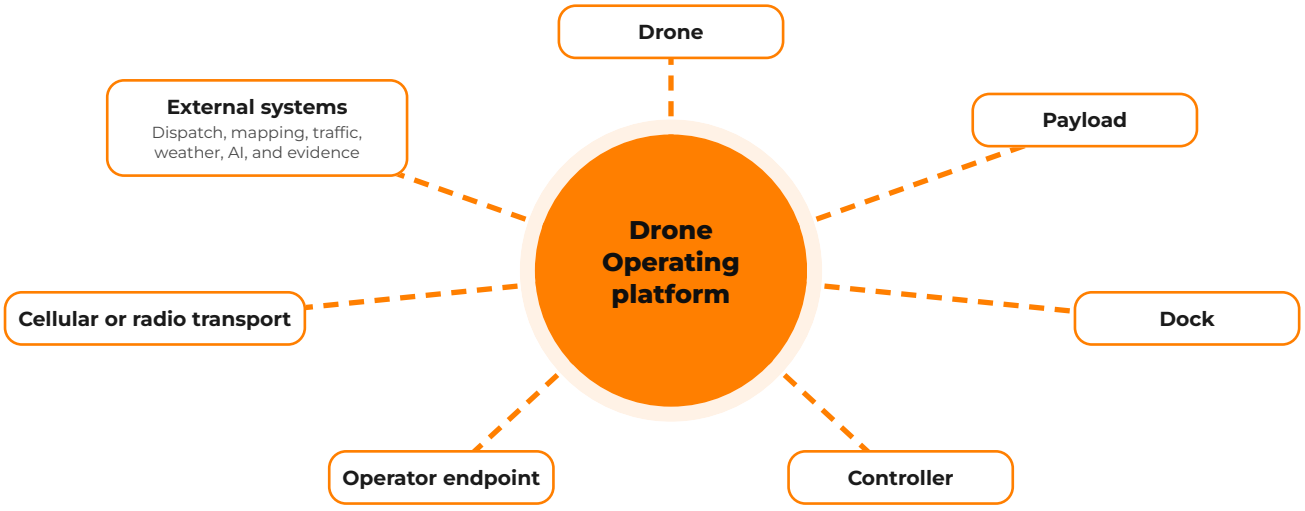
Use a Recognized **Governance Framework**

NIST CSF 2.0 provides six continuous functions: Govern, Identify, Protect, Detect, Respond, and Recover. Programs assign an accountable owner, inventory the complete system, select controls for mission risk, monitor exceptions, rehearse response, and prove recovery. CSF alignment is a way to organize outcomes, and each control gains confidence through its own testing and evidence. [14]

1	2	3	4	5	6
Govern	Identify	Protect	Detect	Respond	Recover

Six continuous functions, applied repeatedly across the life of the program

Apply Security **Where Systems Meet**



Map the drone, payload, dock, controller, operator endpoint, cellular or radio transport, Drone Operating platform, and external dispatch, mapping, traffic, weather, artificial intelligence (AI), and evidence systems. Identify each credential, data transfer, command path, and failure dependency. Treat every integration as a separate trust relationship with a documented owner and a removal process.

© 2026 VOTIX. All Rights Reserved.

Flight safety

Protect Command Authority and **Flight Safety**

Control the command path

Require authenticated command sessions and integrity protection on supported communication paths. Identify where encryption begins and ends, including video protection at the cloud boundary and protection of every drone link. Validate device identity, session expiration, command authorization, and the rejection of stale or replayed commands.



Protect application programming interfaces (APIs) with scoped credentials, rotation, rate limits, and monitoring. Keep drone control permissions separate from incident viewing and routine administration.

Keep drone control permissions separate from incident viewing and routine administration.

Command authority and handover

1
Who holds command authority

2
Who may transfer it

3
How the receiving pilot confirms the handover

Before a remote mission, establish who holds command authority, who may transfer it, and how the receiving pilot confirms the handover. Testing confirms that command authority stays with the active pilot until a confirmed handover.

Emergency support access is approved, time-limited, and logged. Reauthentication and session expiration policies reflect flight safety, so identity controls support continuous, managed control of the drone.



Reauthentication and session expiration policies reflect flight safety, so identity controls support continuous, managed control of the drone.

© 2026 VOTIX. All Rights Reserved.

Protect Command Authority and Flight Safety

Prepare for Degraded **Communications and Navigation**

Test the loss of internet, cloud access, drone command link, telemetry, video, and dock connectivity as six distinct events. A video outage can occur while command remains active, and a frozen map can show a stale position instead of a current one. Measurable freshness and latency limits, defined launch inhibition criteria, and documented pilot actions give crews clear guidance when a display becomes unreliable.

SIX DISTINCT EVENTS TO TEST

Internet | Cloud access | Drone command link | Telemetry | Video | Dock connectivity

Global navigation satellite system (GNSS) jamming or spoofing can send false signals that lead a drone off course, and electromagnetic interference can disrupt drone communication signals. [15] Validate model-specific navigation checks and approved alternatives, safe landing locations, reserve battery margins, and flight termination or diversion criteria. Returning home, hovering, and landing immediately each carry location-dependent risks, so the drone manufacturer's guidance and the operating authorization shape the right choice. Test the chosen behavior before it is needed.

Secure Drone Docks and **Operator Endpoints**

Inventory firmware, operating systems, mobile apps, radios, payloads, and dock network equipment. Remove default credentials and unnecessary services, and use managed operator devices and segmented networks. Restrict dock maintenance and network access, inspect for physical tampering, and protect removable media. Limit connections to approved destinations where feasible, including any direct original equipment manufacturer (OEM) cloud or diagnostic pathways that bypass the Drone Operating platform.

Evaluate supplier update authenticity, signing and secure boot support, vulnerability disclosure, component inventories or software bills of materials (SBOMs), and end-of-support dates. Stage updates in a controlled environment and flight test the approved configuration before deployment. Use emergency update procedures for urgent vulnerabilities, with a safe fallback when an update affects airworthiness or compatibility. NIST's Secure Software Development Framework offers a useful basis for supplier questions. [16]

© 2026 VOTIX. All Rights Reserved.

Protect Incident Collaboration and Mission Data

Make Access **Intentional**

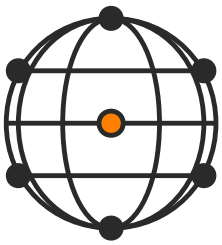
Use named accounts and least privilege for every participant. Multifactor authentication is available as a voluntary feature that each person activates in their own profile, and programs can encourage every user to turn it on. Document any additional identity safeguards the program relies on, together with the residual risk.

Restrict administrator accounts, separate daily work from privileged activity, and promptly revoke the credentials of departed staff, contractors, guests, and service accounts. Test active session termination alongside account removal.

For shared streams, approve participants and the purpose of access before sharing sensitive feeds. Ask whether invitations can expire, be limited to authenticated recipients, be revoked immediately, and be recorded in logs. Test forwarding and reconnection behavior. Where redistribution remains possible, treat it as a disclosure risk and adjust sharing procedures accordingly. Keep viewing privileges separate from control of drones and payloads.

Keep viewing privileges separate from control of drones and payloads.

Protect the Data **Throughout Its Life**



Classify live video, recordings, audio, chat, annotations, telemetry, credentials, and mission plans. Limit collection to the mission's purpose, record the locations the mission requires, and keep sensitive information in shared views to a minimum. Define which records become evidence and which are routine operational data. Establish approved export destinations and accountable recipients.

Create retention rules by record type, with legal holds taking precedence over normal deletion where required. Account for drone storage, controllers, docks, cloud copies, exports, backups, and third-party integrations. Confirm how deletion propagates and how long backup copies persist. Reconcile privacy policy statements, the service agreement, and the data processing terms so that secondary use, AI processing, support access, and post-termination handling are explicit.

CLASSIFY EACH DATA TYPE

Live video | Recordings | **Audio** | Chat | **Annotations** | Telemetry | **Credentials** | **Mission plans**

© 2026 VOTIX. All Rights Reserved.

Protect Incident Collaboration and Mission Data

Preserve Evidence and **Accountability**

For evidentiary material, preserve originals and relevant metadata, use integrity hashes at collection or transfer, keep a record of who handles the material at each step, and document authorized redactions. Hashes help detect changes, and authenticity is established through the combination of these measures. Keep time synchronized across systems and retain the context needed to interpret a flight or incident timeline.

Require logs sufficient to investigate logins, failed access, permission changes, stream sharing, exports, configuration edits, and control transfers. Confirm which of these events the deployed system records, who can change or delete logs, and how logs reach agency monitoring. Describe logging coverage in terms of the events that the deployment has demonstrated.

EVENTS LOGS SHOULD COVER

- Logins
- Failed access
- Permission changes
- Stream sharing
- Exports
- Configuration edits
- Control transfers

Keep AI Subject to **Mission Controls**

For AI-supported visual analysis or automation, document model and service providers, input destinations, retention, and training permissions. Validate outputs under expected weather, lighting, and sensor conditions. Treat classifications as decision support until the specific automated behavior has been safety assessed and authorized. Ensure that external inputs reach flight authority and mission boundaries only through approved, trusted paths.



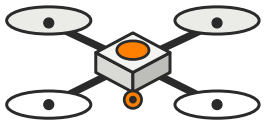
Treat classifications as decision support until the specific automated behavior has been safety assessed and authorized.

© 2026 VOTIX. All Rights Reserved.

Respond, Recover, and Demonstrate Readiness

Coordinate Cyber Response **with the Pilot**

A drone cyber incident calls for an aviation-aware response. The remote pilot in command assesses the airborne situation before a responder disables an account, disconnects a network, or isolates a dock. The approved contingency lands, diverts, or maintains safe control, and then the team contains affected access and systems. Targeted instructions, written for each scenario, keep the response from creating a larger flight hazard.



The playbook should name the pilot, incident commander, security lead, Drone Operating platform and equipment support contacts, records custodian, and legal or privacy lead. Preserve relevant logs, telemetry, configurations, and data before remediation changes them, wherever safety permits. Define contractual notification routes and assess the legal, contractual, aviation, and law enforcement reporting requirements for the actual event.

ROLES THE PLAYBOOK NAMES

- Pilot
- Incident commander
- Security lead
- Drone Operating platform and equipment support
- Records custodian
- Legal or privacy lead

Restore and demonstrate

Restore from a trusted configuration, rotate affected credentials, validate device and integration integrity, and test control authority before returning to service. Agree on recovery objectives for each critical service. Demonstrate restore capability and define how the program coordinates if the software, a carrier, or the cloud service becomes unavailable. Testing turns recovery objectives into dependable commitments.

1 Restore from a trusted configuration

2 Rotate affected credentials

3 Validate device and integration integrity

4 Test control authority before returning to service

Testing turns recovery objectives into dependable commitments.

© 2026 VOTIX. All Rights Reserved.

Respond, Recover, and Demonstrate Readiness

Illustrative Exercise for a **VOTIX-Enabled Program**

During a multi-agency Drone as First Responder (DFR) incident, an unexpected participant appears in a shared room while one drone's video freezes. The commander verifies participant identity through an established channel. The pilot independently checks the command link and telemetry, evaluates data freshness, and follows the approved contingency plan if minimum operating conditions are lost. The security lead restricts the suspect participant using tested access procedures while the pilot's control session continues.

After a safe recovery, the team correlates room membership, identity, sharing, command, and network records, preserves evidence, and determines whether the frozen feed reflected a communications fault or malicious activity. The exercise succeeds when guest removal works, command authority stays clear, and the team can reconstruct events.

This hypothetical test scenario supports exercise planning and is separate from any actual VOTIX incident or automatic system response.

A Continuous **Improvement Cycle**

Programs can organize improvement work into three repeating stages, and each stage produces evidence that the program owner can review.

Stage	Program action	**Acceptance evidence**
Map and Review	Map systems and data; review permissions and eligibility; approve flight contingencies	Owned inventory; data map; access review; dated restrictions register
Test and Verify	Test sharing, revocation, control handover, degraded links, and updates	Recorded results for each supported drone and dock configuration
Exercise and Improve	Run an incident and recovery exercise; close priority gaps	Restore evidence; safe return to service record; accepted residual risks

© 2026 VOTIX. All Rights Reserved.

Procurement and renewal

Questions for Procurement **and Renewal**

Use these eight questions with every connected supplier. Request a demonstration or dated artifact, identify its scope, and record any exception with an accountable owner.

1

Where Does Each Class of Data Go?

Request a data flow map covering live traffic, storage, backups, support access, subprocessors, OEM services, and exports. Confirm regions and the contractual handling of transfers and termination.

2

Which Exact Drones and Docks Are Supported and Eligible?

Match the model, components, firmware, funding source, and operating authority. Ask for the migration effort and validation needed if hardware changes.

3

Who May View, Command, Administer, and Export?

Demonstrate role boundaries, authentication, privileged access, guest controls, revocation, and service account limits in the proposed configuration.

4

How Is the Complete Command Path Protected?

Identify encryption and authentication boundaries, device identity, command handover, and the separation between shared incident awareness and flight authority.

5

What Happens When Links, Navigation, or Services Fail?

Test stale data warnings, launch restrictions, lost link behavior, GNSS anomalies, alternate coordination, and the pilot's contingency actions.

6

How Are Software and Integrations Kept Trustworthy?

Review update verification, how security fixes are delivered, supported versions, vulnerability intake, dependency risk, and safe testing before deployment.

7

Can Records Support Investigation and Lawful Disclosure?

Inspect actual event coverage, retention, time synchronization, log protection, evidence export, legal holds, and deletion behavior.

8

What Independent Evidence and Recovery Commitments Apply?

Ask for available assessment scope and dates, remediation status, incident communication practices, recovery objectives, restore results, and the shared responsibility matrix.

© 2026 VOTIX. All Rights Reserved.

Conclusion and references

Conclusion

A Drone Operating platform delivers the most value when operational coordination is paired with verified trust boundaries. Programs can use that architecture to govern access and workflows consistently while keeping responsibility for drone safety, lawful collection, supplier eligibility, and tested recovery. The outcome is a program that explains its safeguards, demonstrates them under pressure, and improves them as technology and regulations change.



References

Numbered citations identify supporting publications. Recommended program controls are guidance developed from those sources and the operational analysis in this paper.

[1] National Cybersecurity Alliance. Cybersecurity Awareness Month 2026. Open source

[2] VOTIX. About VOTIX. Open source

[3] VOTIX. Features. Open source

[4] VOTIX. VOTIX Launches Situation Rooms. Open source

[5] VOTIX. Privacy Policy, effective July 16, 2026. Open source

[6] Federal Communications Commission. Fact Sheet: FCC Updates Covered List to Include Foreign UAS and UAS Critical Components on Going Forward Basis, December 22, 2025. Open source

[7] Federal Communications Commission. Erratum to the Covered List entry for UAS and UAS critical components, released April 3, 2026. Open source

[8] Federal Communications Commission. DA 26-850, Public Notice on Conditional Approvals and exemptions from the Covered List, with the UAS Conditional Approvals list in Appendix B, released August 14, 2026. Open source

[9] Federal Communications Commission. DA 26-758, FCC Seeks Comment on Prohibiting the Importation and Marketing of Certain Foreign-Produced Military-Grade UAS and UAS Critical Components, PS Docket No. 26-189, released July 21, 2026. Open source

[10] Federal Acquisition Regulation. Section 40.202, Prohibition on the procurement and operation of FASC-prohibited UAS, FAC 2026-01, effective March 13, 2026. Open source

[11] Federal Aviation Administration. Announcement of the proposed beyond visual line of sight rule, August 6, 2025. Open source

[12] Federal Aviation Administration. Remote Identification of Drones. Open source

[13] Federal Bureau of Investigation. Security policy for criminal justice information, version 6.1, June 25, 2026. Open source

[14] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, February 26, 2024. Open source

[15] Canadian Centre for Cyber Security. Cyber security considerations for drone use (ITSAP.00.143), January 2026. Open source

[16] National Institute of Standards and Technology. SP 800-218, Secure Software Development Framework (SSDF) Version 1.1, February 2022. Open source

© 2026 VOTIX. All Rights Reserved.