INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-05 13:25 UTC

Law-Tech Connect 2026: Emerging Policy and Cyber Risk Landscape for Drone, AI, and Counter-UAS Operations

GOVERNANCE | MEDIUM

SCC Item ID	SCC-GOV-2026-0009
Type	Governance
Severity	MEDIUM
Affected Products	Drone and autonomy operators, AI systems, counter-UAS technologies, critical communications infrastructure
Published	2026-04-03
Discovery Source	Gemini

Executive Summary

The 2026 Law-Tech Connect Workshop signals growing institutional and regulatory momentum around cybersecurity requirements for drone operations, AI-integrated autonomous systems, and counter-UAS technologies. Organizations operating UAS fleets, managing airspace infrastructure, or deploying AI-driven autonomous systems face an evolving compliance landscape as BVLOS regulations and cyber resilience mandates advance. The business risk is lack of preparedness: organizations that have not inventoried UAS attack surfaces or assessed AI integration risks may find themselves behind regulatory expectations and exposed to operational disruption.

Technical Analysis

This is a governance and policy signal item with no associated CVE, active exploit, or confirmed threat actor. It indicates increasing regulatory and standards-body focus on UAS cyber risk. Known technical attack surfaces for UAS systems include: GPS spoofing (CWE-20: Improper Input Validation), RF jamming and command-and-control link hijacking (CWE-294: Authentication Bypass by Capture-replay, CWE-345: Insufficient Verification of Data Authenticity), and unencrypted telemetry interception (CWE-311: Missing Encryption of Sensitive Data). Mapped MITRE ATT&CK techniques include T1040 (Network Sniffing) for telemetry capture, T1498 (Network Denial of Service) as an analog for RF jamming effects, T1583.006 (Acquire Infrastructure: Web Services) for C2 infrastructure concerns, and T1205 (Traffic Signaling) for covert channel risks in drone comms. AI integration into autonomous drone perception systems introduces adversarial input attack risks (CWE-1025: Comparison Using Wrong Factors) and model integrity concerns; formal codification in NIST,

MITRE, or ISO frameworks is emerging but incomplete as of 2026. Counter-UAS systems present dual-use risk: they can be weaponized or misconfigured, requiring defense-in-depth architecture. Supply chain risks in drone firmware (e.g., unsigned firmware updates, vendor key compromise) align with NIST SP 800-161 supply chain risk management controls, requiring vendor vetting and cryptographic verification of firmware. Source quality for this item is moderate-high (score: 0.68); peer-reviewed and PMC-indexed research supports the attack surface taxonomy, while event-specific sourcing is Tier 3.

Action Checklist

1. Inventory: Identify all UAS assets, autonomous systems, and counter-UAS technologies in your environment. Document communication protocols, telemetry links, and any AI/ML components integrated into flight or decision systems.
2. Detection readiness: Assess current visibility into RF communications, GPS signal integrity, and drone C2 traffic. Determine whether existing SIEM or network monitoring covers UAS communication channels.
3. Control gap assessment: Evaluate whether command-and-control links use authenticated, encrypted protocols. Flag any systems transmitting unencrypted telemetry or relying on unauthenticated GPS input without integrity checks.
4. Regulatory alignment: Review current BVLOS operating authorizations and FAA cybersecurity guidance. Map existing controls to NIST CSF 2.0 and NIST SP 800-53 Rev 5 control families SC (System and Communications Protection) and SI (System and Information Integrity) for UAS-adjacent systems.
5. Post-assessment: Document findings and assign ownership. Monitor for Law-Tech Connect 2026 outputs and any forthcoming FAA or CISA guidance on UAS cyber requirements. Incorporate UAS threat scenarios into tabletop exercises.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if active evidence of GPS spoofing, C2 link anomalies, or unauthorized BVLOS boundary exceedance is detected during the assessment, or if CISA issues an emergency directive or FAA SAFO specifically mandating immediate UAS cybersecurity action with a defined compliance deadline.
Recovery Notes	Following remediation of control gaps, validate that all C2 links are confirmed operating on MAVLink v2 with message signing enabled and that GCS firewall rules are blocking unauthorized MAVLink port access before resuming BVLOS operations. Monitor GCS telemetry logs and RF spectrum for 30 days post-remediation for anomalies indicating residual interference, unauthorized signal presence, or GPS integrity degradation (HDOP spikes, unexpected satellite count drops). Resubmit or amend BVLOS authorizations to the FAA if cybersecurity control changes materially alter the safety case documented in the original waiver application.

Forensic Artifacts	GCS software flight logs (Mission Planner: %APPDATA%\Mission Planner\logs\ | QGroundControl: ~/Documents/QGroundControl/Logs/) — contain GPS fix quality, HDOP, satellite count, EKF status, and C2 RSSI time-series data that would show GPS spoofing signatures (sudden position jumps, HDOP drops coinciding with position shifts) or C2 jamming events (RSSI degradation followed by return-to-home trigger) | MAVLink parameter dump files (exported via Mission Planner Full Parameter List) — preserve pre-incident autopilot configuration including GPS_TYPE, EKF source settings, message signing status, and geofencing parameters; a spoofing or hijacking event may result in parameter changes that are only detectable against a pre-incident baseline | SDR spectrum captures (IQ recordings via rtl_433, GQRX, or GNU Radio) on operational C2 and GPS L1 (1575.42 MHz) / L2 (1227.60 MHz) frequencies — would preserve evidence of jamming waveforms, spoofing signal characteristics, or unauthorized transmitters operating on licensed C2 frequencies | GCS host network traffic pcaps (Wireshark/tcpdump on UDP/TCP port 14550 and 14556) — MAVLink session logs would show unauthorized GCS connections, unexpected COMMAND_LONG messages (e.g., forced mode changes, geofence disables), or connection source IPs inconsistent with the authorized GCS operator | Remote ID broadcast logs (if applicable under FAA 14 CFR Part 89) — Remote ID receiver logs or network Remote ID submissions would show whether the aircraft's broadcast ID was spoofed or whether a rogue UAS was operating in the vicinity during an incident, providing correlation evidence for counter-UAS detection events

Per-Action IR Details

Inventory: Identify all UAS assets, autonomous systems, and counter-UAS technologies in your environment. Document communication protocols, telemetry links, and any AI/ML components integrated into flight or decision systems.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability and asset visibility before incidents occur

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires knowing what assets require protection, NIST SI-7 (Software, Firmware, and Information Integrity) — inventory must capture firmware versions on flight controllers, GCS software, and AI/ML inference engines, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — extend asset inventory schema to include UAS tail numbers, GCS endpoints, RF frequencies, MAVLink/UAVCAN protocol versions, and C2 link encryption status, CIS 2.1 (Establish and Maintain a Software Inventory) — enumerate autopilot firmware (ArduPilot, PX4, DJI SDK versions), mission planning software, and any onboard AI/ML model versions

Compensating: For teams without CMDB or enterprise asset management: build a UAS-specific inventory spreadsheet capturing each airframe's tail/serial number, GCS IP/MAC, telemetry frequency (e.g., 900 MHz, 2.4 GHz, 5.8 GHz), protocol stack (MAVLink v1/v2, UAVCAN, proprietary DJI OcuSync), encryption status (AES-256 vs. none), and AI/ML component vendor. Use 'nmap -sn ' against GCS and companion computer subnets to discover networked UAS components. Cross-reference against FAA DroneZone registration records for BVLOS-authorized aircraft.

Evidence: Before inventorying, preserve a current snapshot of the RF environment using a software-defined radio (SDR) scan (e.g., rtl_433 or GQRX) to document baseline telemetry frequencies actively in use — this establishes a pre-change baseline and may reveal undocumented or shadow UAS assets transmitting on unexpected frequencies. Capture network traffic on GCS subnets via Wireshark/tcpdump to identify MAVLink heartbeat packets (UDP/TCP port 14550, 14556) that would reveal undocumented drone-to-GCS sessions.

Detection readiness: Assess current visibility into RF communications, GPS signal integrity, and drone C2 traffic. Determine whether existing SIEM or network monitoring covers UAS communication channels.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish monitoring infrastructure and detection capability before adverse events occur

Controls: NIST SI-4 (System Monitoring) — extend monitoring scope to include RF spectrum monitoring for drone C2 frequencies and GPS L1/L2 signal integrity checks, NIST AU-2 (Event Logging) — define loggable events specific to UAS operations: GPS spoofing anomalies, unexpected C2 frequency shifts, telemetry link drops, and unauthorized BVLOS boundary exceedances, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — establish review cadence for UAS telemetry logs and RF anomaly alerts, CIS 8.2 (Collect Audit Logs) — ensure GCS software audit logs, flight data recorder (FDR) logs, and RF monitoring sensor logs are collected and retained

Compensating: Without a SIEM: deploy an SDR-based RF monitor (RTL-SDR + DragonOS or OpenWebRX) on a Raspberry Pi positioned near flight operations to passively monitor C2 frequencies for anomalies (unexpected signal sources, frequency hopping, jamming signatures). For GPS integrity: configure GCS software (Mission Planner or QGroundControl) to log GPS HDOP values and flag HDOP > 2.0 as a potential spoofing/interference indicator. Forward GCS logs to a syslog server (rsyslog) and write a simple Python or bash script to alert on telemetry link loss events exceeding 3 seconds. Use Wireshark capture filters ('udp port 14550') on GCS interfaces to baseline normal MAVLink traffic volume.

Evidence: Capture current GCS software logs (Mission Planner: %APPDATA%\Mission Planner\logs\ or QGroundControl: ~/Documents/QGroundControl/Logs/) to establish a baseline of normal GPS fix quality, satellite count, HDOP, and C2 RSSI values. Record an SDR spectrum sweep of active operational frequencies before any changes — this documents the pre-assessment RF baseline and can later be compared against anomalous jamming or spoofing signatures. Preserve any existing IDS/firewall logs covering the GCS network segment for traffic to/from drone companion computer IPs.

Control gap assessment: Evaluate whether command-and-control links use authenticated, encrypted protocols. Flag any systems transmitting unencrypted telemetry or relying on unauthenticated GPS input without integrity checks.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Identify capability and control gaps that would impede detection or containment of UAS cyber incidents

Controls: NIST SC-8 (Transmission Confidentiality and Integrity) — C2 links transmitting MAVLink v1 without encryption fail this control; MAVLink v2 with AES-256 signing required, NIST SC-28 (Protection of Information at Rest) — flight logs and mission plans stored on GCS or onboard storage must be encrypted at rest, NIST SI-10 (Information Input Validation) — GPS input to autopilot systems must include integrity validation; unauthenticated GNSS input without cross-validation against IMU or secondary GNSS receiver represents a gap, NIST SI-7 (Software, Firmware, and Information Integrity) — autopilot firmware must be verified via cryptographic signature before deployment; unsigned firmware updates are a critical gap, CIS 4.4 (Implement and Manage a Firewall on Servers) — GCS systems must have host-based firewall rules restricting MAVLink port access to authorized drone IP ranges only, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — include UAS firmware CVEs and vendor security advisories in the vulnerability management scope

Compensating: For teams without enterprise vulnerability scanners: use MAVLink Inspector (built into Mission Planner) to confirm whether the active link uses MAVLink v2 message signing — look for HEARTBEAT messages and verify the 'signing' field is non-zero. For GPS integrity, check autopilot parameters via MAVLink: query GPS_TYPE parameter and verify EKF (Extended Kalman Filter) fusion includes IMU cross-validation (ArduPilot: EK3_SRC1_POSXY should not be set to GPS-only without a secondary source). Document gaps in a simple risk register with columns: system, gap description, NIST control failed, risk level, and owner.

Evidence: Before remediating gaps, capture a full MAVLink parameter dump from each autopilot (Mission Planner: Config > Full Parameter List > Save to file) — this creates a forensic baseline of the pre-remediation configuration that preserves evidence of insecure settings. Export GCS firewall rules (Windows: 'netsh advfirewall export' or Linux: 'iptables-save > iptables-backup.txt') to document the pre-assessment network posture. If any C2 links are found to be unencrypted, capture a 5-minute Wireshark pcap on the GCS interface to demonstrate the exposure scope before patching.

Regulatory alignment: Review current BVLOS operating authorizations and FAA cybersecurity guidance. Map existing controls to NIST CSF 2.0 and NIST SP 800-53 Rev 5 control families SC (System and Communications Protection) and SI (System and Information Integrity) for UAS-adjacent systems.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Align IR capability and controls to applicable regulatory requirements governing UAS operations

Controls: NIST IR-8 (Incident Response Plan) — IR plan must explicitly address UAS-specific incident scenarios including C2 link hijacking, GPS spoofing, and BVLOS boundary violations triggered by cyber manipulation, NIST SI-2 (Flaw Remediation) — apply FAA cybersecurity guidance and any CISA ICS advisories covering UAS/autopilot vulnerabilities as authoritative sources for flaw remediation prioritization, NIST SC-8 (Transmission Confidentiality and Integrity) — maps directly to FAA BVLOS authorization requirements for authenticated, encrypted C2 links, NIST SI-4 (System Monitoring) — maps to FAA Remote ID broadcast monitoring requirements and CISA guidance on detecting GPS interference, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate FAA Safety Alerts for Operators (SAFO) and CISA advisories for UAS platforms into the vulnerability intake process, CIS 7.2 (Establish and Maintain a Remediation Process) — establish SLAs for remediating UAS control gaps identified against FAA cybersecurity guidance, aligned to BVLOS re-authorization timelines

Compensating: For teams without GRC tools: build a CSF 2.0 mapping spreadsheet with columns for CSF Function (Govern/Identify/Protect/Detect/Respond/Recover), CSF Category, NIST 800-53 control ID, current UAS control implementation, FAA/CISA requirement reference, and gap status. Cross-reference against CISA's 'Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems' publication and FAA Advisory Circular AC 107-2B. Assign each gap a risk rating and an owner from the UAS operations team. Review FAA DroneZone for any conditions attached to existing BVLOS waivers that impose cybersecurity requirements.

Evidence: Before beginning regulatory mapping, preserve copies of all current FAA BVLOS authorizations (COA or Part 107 waiver documents), Remote ID broadcast logs if applicable, and any prior FAA safety inspection records — these establish the regulatory baseline and may be required if an incident later triggers FAA notification obligations. Document the current NIST CSF 2.0 profile in writing so that post-workshop changes can be diffed against a known baseline.

Post-assessment: Document findings and assign ownership. Track Law-Tech Connect 2026 outputs and any forthcoming FAA or CISA guidance on UAS cyber requirements. Incorporate UAS threat scenarios into tabletop exercises.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Document lessons learned, update policies, improve detection capability, and share intelligence to strengthen future IR posture

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to incorporate UAS-specific scenarios: C2 link takeover, GPS spoofing triggering autonomous behavior, remote ID spoofing, and counter-UAS system false positives, NIST IR-3 (Incident Response Testing) — conduct tabletop exercises simulating UAS cyber incidents including BVLOS boundary violation via GPS spoofing and GCS network intrusion leading to flight control manipulation, NIST IR-5 (Incident Monitoring) — establish ongoing tracking of FAA, CISA, and Law-Tech Connect 2026 regulatory outputs as authoritative sources for UAS cyber requirement updates, NIST SI-5 (Security Alerts, Advisories, and Directives) — formally subscribe to FAA SAFO notifications, CISA ICS-CERT advisories (UAS/avionics category), and relevant MITRE ATT&CK for ICS updates covering UAS attack techniques, CIS 7.2 (Establish and Maintain a Remediation Process) — assign remediation owners and due dates for each control gap identified in the assessment, with re-validation checkpoints tied to BVLOS reauthorization cycles

Compensating: For teams without formal GRC or ticketing platforms: use a shared markdown or spreadsheet-based findings register with columns for finding ID, description, affected UAS asset, NIST control gap, assigned owner, target remediation date, and status. For tabletop exercises: develop a 2-hour scenario based on a GPS spoofing attack causing a BVLOS aircraft to deviate from its authorized corridor, requiring the team to work through detection (RF anomaly alert), containment (return-to-home command or C2 override), and FAA notification decision. Use MITRE ATT&CK for ICS technique T0856 (Spoof Reporting Message) and T0816 (Device Restart/Shutdown) as scenario anchors. Subscribe to CISA's free alert service at cisa.gov/uscert/mailing-lists-and-feeds for ICS and UAS-relevant advisories.

Evidence: Preserve all assessment outputs as formal records before closing: gap analysis findings, CSF mapping spreadsheet, MAVLink parameter dumps, RF baseline captures, and GCS configuration exports. These constitute the pre-remediation evidence baseline and will serve as the comparison point for future assessments or regulatory audits.

Retain meeting notes or outputs from Law-Tech Connect 2026 sessions as contemporaneous records demonstrating the organization's awareness of emerging regulatory requirements — relevant if future FAA enforcement actions assess when organizations were on notice of cybersecurity obligations.

Detection Guidance

No specific IOCs are associated with this governance item. Detection focus should target known UAS attack surface behaviors: (1) GPS spoofing, monitor for sudden, implausible position shifts or satellite count anomalies in telemetry logs if your systems expose this data; (2) RF jamming, loss of C2 link or signal degradation patterns in RF monitoring tools; (3) Telemetry interception, baseline normal telemetry traffic volumes and flag unexpected external connections to telemetry endpoints; (4) Firmware integrity, verify cryptographic signatures on drone firmware updates against vendor-published hashes; (5) AI model integrity, if autonomous perception systems are in use, monitor for anomalous decision outputs that may indicate adversarial input injection. For network-connected ground control stations, apply standard network monitoring: log authentication events, flag unauthorized access attempts, and review egress traffic for unexpected destinations.

Framework Mappings

MITRE-ATTACK

- **T1040** — Network Sniffing
- **T1498** — Network Denial of Service
- **T1583.006** — Web Services
- **T1205** — Traffic Signaling

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A08:2021** — Software and Data Integrity Failures

NIST-800-53R5

- **SI-10** — Information Input Validation
- **SI-7** — Software, Firmware, and Information Integrity
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

- **A.8.24** — Use of cryptography

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1040	Network Sniffing	Credential-Access
T1498	Network Denial of Service	Impact
T1583.006	Web Services	Resource-Development
T1205	Traffic Signaling	Defense-Evasion

Sources

Source	URL	Tier
Drone Threats Rise: AiON Counter-UAS Solutions Evolve - LinkedIn	https://www.linkedin.com/posts/david-chen-3517681a2_as-drone-threat...	T3
Researchers expose critical security vulnerability in autonomous ...	https://techxplore.com/news/2026-02-expose-critical-vulnerability-a...	T3
CNA Tackling The Drone Industry's Toughest Security Problems	https://www.autonomyglobal.co/cna-tackling-the-drone-industrys-toug...	T3
Cybersecurity and Artificial Intelligence in Unmanned Aerial ...	https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ise2/2...	T2
Security analysis of drones systems: Attacks, limitations, and ... - PMC	https://pmc.ncbi.nlm.nih.gov/articles/PMC7206421/	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-05 13:25 UTC by TJS Security Command Center