OnDefend

DJI Security Assessment

OnDefend is trusted by national security stakeholders and enterprise leaders to independently test technologies and their supply chains, validating security, safety, and the protection of U.S. citizen data. Our experts include U.S. military and government professionals with deep operational experience.

In this assessment, OnDefend performed a thorough technical evaluation of two DJI drone systems, the Air 3S and Matrice 4E, along with their corresponding controllers and applications.

DJI TECHNOLOGY, INC. | MAY 14, 2026

OnDefend – Independent Security Inspector

Executive Summary: DJI Drone Security Evaluation | Air 3S & Matrice 4E | October 2025 – March 2026

Company Inspected

Engagement Overview

OnDefend conducted an independent, DJI-authorized security assessment of two drone platforms to evaluate national security concerns around data sovereignty, hardware vulnerabilities, and drone manipulation risks.

Devices Evaluated

DJI Air 3S with RC 2 Controller & DJI Fly App
DJI Matrice 4E with RC Plus 2 Enterprise & Pilot 2 App

Procurement Method

Consumer units were purchased independently without notification to DJI. Enterprise units were taken from existing dealer stock, ensuring tested units represented standard U.S. market distribution.

Engagement Period

October 21, 2025 – March 13, 2026

National Security Concerns Addressed

U.S. DATA SOVEREIGNTY	Drones collect sensitive imagery, telemetry, and geospatial data, with risks of unauthorized transmission to foreign or external systems.
DEVICE VULNERABILITIES	Firmware, software, and hardware components may introduce vulnerabilities through updates or supply chain tampering.
DRONE MANIPULATION	Software, communication channels, and circuit board components with antennas may enable hijacking, denial of service or operational disruption.

Components Tested

Drones	Controllers	Applications	Circuit Boards	RF Signals
Air 3S & Matrice 4E	RC 2 & RC Plus 2	DJI Fly & Pilot 2	PCB & Components	1 MHz- 6GHz Spectrum

Findings Summary

CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK	OBSERVATION
0	0	0	10	13

Type	Category	Tests Performed	Key Outcomes
STANDARD TESTING	**Application Security, Hardware, & Firmware**	✓ **Network Traffic Analysis:** Captured and analyzed controller traffic across modes, inspecting destinations, volume, and potential exfiltration. ✓ **Adversary Simulation:** Executed Meddler-in-the-Middle (MitM) attacks, certificate bypass, interception, decryption, and redirection testing. ✓ **Application & Device Security:** Analyzed DJI apps and attempted jailbreak, downgrade, privilege escalation, and WiFi/port exploitation.	✓ No data transmitted to China. All connections resolved to U.S.-based endpoints. ✓ Controllers resisted all jailbreak and firmware modification attempts. ✓ Default shared WiFi password identified and patched by DJI via firmware update. LOW RISK: 10 / OBSERVATION: 11
ADVANCED TESTING Powered by OnDefend Technology	**Hardware Teardown & RF Transmissions**	✓ **Hardware Analysis:** Disassembled drone platforms to perform component-level and PCB analysis. ✓ **RF Signal Analysis:** Conducted wide-spectrum scanning to baseline environments and identify anomalous emissions. ✓ **Signal Exploitation:** Isolated signals and executed replay, jamming, interference, and malformed injection attacks.	✓ All RF emissions were documented frequencies and protocols or were traced to Divider/PLL circuit artifacts of the documented O4 control signals- no unexplained transmission. ✓ O4 protocol fully resistant to replay, jamming, and injection attacks. ✓ No backdoor hardware transmissions identified. LOW RISK: 0 / OBSERVATION: 2
	Supply Chain Integrity & HBOM	✓ **Integrity Verification:** Cross-referenced PCB components against expected BOM. ✓ **Tampering Analysis:** Compared retail and enterprise units to identify inconsistencies, tampering, or undocumented modifications.	✓ No supply chain tampering detected. ✓ No unauthorized hardware modifications identified. LOW RISK: 0 / OBSERVATION: 0

Bottom Line

During the window of testing, OnDefend's assessment of the Air 3S and Matrice 4E identified no evidence of hidden backdoors, no data transmissions outside the United States, and no viable pathways for hijacking or weaponization. No critical or high-risk findings were identified.

Moving Forward

To maintain national security assurance, ongoing testing of firmware, software updates, and verification of hardware and chip integrity are recommended for continuous and ongoing validation.

The OnDefend Difference | OnDefend - America's Trusted Independent Security Inspector

OnDefend's Offensive Security Team

OnDefend is trusted by national security stakeholders and enterprise leaders to independently test technologies and their supply chains, validating security, safety, and the protection of U.S. citizen data. Our experts include U.S. military and government professionals with deep operational experience.

OnDefend's Proprietary Technology

OnDefend's proprietary hardware testing technology identifies unauthorized transmission and supply chain risks including hidden RF channels, covert data exfiltration paths, counterfeit components, undocumented modifications, and embedded hardware such as antennas through AI driven imaging and silicon level analysis.

Assessment Overview

Scope

OnDefend performed a thorough technical evaluation of two DJI drone systems, the Air 3S and Matrice 4E, along with their corresponding controllers and applications. The objective was to determine whether these devices transmit data outside the United States, contain backdoors that could enable unauthorized access or control, or present cybersecurity risks that would affect operational use. The evaluation covered both software and hardware across multiple testing disciplines.

Two units of each drone model were tested across controlled indoor and outdoor environments over a five-month engagement period from October 2025 through March 2026. All activity was conducted under rules of engagement explicitly authorized by DJI Technology, Inc.

Software: The team conducted static and dynamic application security testing of the DJI Fly and Pilot 2 applications, analyzed all network traffic during normal and Local Data Mode operation, and tested the controllers for jailbreak and privilege escalation vulnerabilities.

Hardware/Firmware: The team performed full spectrum radio frequency scanning, near field component analysis, and RF exploitation testing including jamming, replay, and injection attempts.

Assessment Methodology

The following methodology describes the structured, multi-discipline approach OnDefend applied to independently evaluate the security posture of DJI drone systems, directly addressing national security concerns related to unauthorized data transmission, software vulnerabilities, and the potential for drone manipulation. The engagement was conducted across two tiers:

STANDARD TESTING

Standard Testing encompasses application and network security, hardware and firmware analysis, and supply chain integrity, the foundational disciplines applied to assess documented behavior and known vulnerability classes.

ADVANCED TESTING
Powered by OnDefend Technology

Advanced Testing applies **OnDefend's proprietary and patented hardware analysis technologies** to surface hidden risks that standard testing cannot detect. Two purpose-built capabilities were central to this engagement:

- **Unauthorized Transmission Detection** identifies hidden or unauthorized RF communications within a device, including covert receivers, embedded sensors, and data exfiltration channels, exposing real-time malicious hardware behavior that software and network testing alone cannot reveal.
- **Board Imaging & Supply Chain Validation** digitally images and catalogs every chip and component to establish a trusted hardware baseline. AI continuously compares current images against past records, detecting tampering, counterfeits, or undocumented modifications across production runs and global supply chains

Together, these tiers allow OnDefend to validate not just what a device claims to do, but what it is physically doing at the hardware, firmware and component level.

Assessment Findings

During the window of testing, OnDefend's assessment of the Air 3S and Matrice 4E drone systems identified no clear evidence of hidden backdoors, no data transmissions outside the United States, and no viable pathways for hijacking or weaponization.

No critical or high-risk findings were observed. Ten low-risk findings and thirteen observations were identified, consistent with industry norms for complex mobile and embedded systems. They were primarily related to application security configurations, session handling, and wireless hardening. None presented a realistic risk to safe drone operation or to widespread exposure of confidential information.

CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK	OBSERVATION
0	0	0	10	13

Overall Summary		
Backdoors / Remote Access ✓ NONE FOUND	Data Exfiltration to Foreign Servers ✓ NONE FOUND	Unexplained RF Emissions ✓ NONE FOUND
Local Data Mode Effectiveness ✓ EFFECTIVE	Application Security Findings ⚠ LOW RISK	Controller Jailbreak Resistance ✓ RESILIENT

Risk Scoring Guide

CRITICAL RISK
A confirmed vulnerability with severe, wide reaching impact that is easily reproduced and exploited with minimal effort.

HIGH RISK
A confirmed vulnerability with potentially severe impact that requires moderate effort to reproduce and exploit.

MEDIUM RISK
A confirmed vulnerability with limited impact that requires specific conditions or moderate skill to exploit.

LOW RISK
A confirmed weakness with limited real-world impact under normal operating conditions.

OBSERVATION
A documented behavior that does not rise to the level of a vulnerability.

All Other Findings

Software Based Testing

→ Egress Traffic Detected with Local Data Mode - DJI RC 2 → Persistent Access Token - DJI Fly → Cryptographic Key Storage Not Aligned to Best Practice → Authentication Tokens Exposed in URLs - DJI Fly & Pilot 2 → Persistent PSK with WPA Wireless Authentication - DJI Air 3S Drones → Persistent Cross-Site Scripting (XSS) - DJI Fly → Egress Traffic Detected with Local Data Mode Functional Testing* - DJI RC Plus 2 → Weak TLS Protocols & Ciphers - DJI Fly & Pilot 2 → DoS of Open Port – DJI Fly & Pilot 2 → Local File Inclusion with Path Traversal in FlyShare - DJI RC 2	LOW RISK
→ Get Accounts Permission - DJI Fly → Use of WPA/WPA2 PSK for Quick Transfer Mode - DJI Air 3S & RC 2 → Runtime Application Self-Protection Bypass - DJI Fly → Runtime Application Self-Protection Bypasses - Pilot 2 → Cleartext Traffic Permitted for In-Scope Domains - DJI Fly & Pilot 2 → Disabled Compiler/Linker Hardening Flags - DJI Fly & Pilot 2 → Outdated Software - DJI Air 3S → Insecure Cryptographic Mode Support - DJI Fly & Pilot 2 → RPATH Set Without RUNPATH in Native Libraries - DJI Fly & Pilot 2 → Install on Android 7.x Permitted - DJI Fly → CORS Arbitrary Origin Trust - DJI Fly	OBSERVATIONS

Hardware Based Testing

→ Undocumented Radio Frequency Transmissions - DJI Air3S and RC2 → Undocumented Radio Frequency Transmissions - DJI Matrice 4E and RC2 Plus Enterprise	OBSERVATIONS

DJI collaborated with OnDefend on potential remediation during the engagement and is working to address remaining items in subsequent software releases. To maintain national security assurance, ongoing testing of firmware, software updates, and verification of hardware and chip integrity are recommended for continuous and ongoing validation.

*Local Data Mode prevents user data from being sent from the drone flight control application to any internet-based location. Even after resuming a normal data mode, no data related to past flights was sent via the internet.

Findings Highlighted Per National Security Concern

National Security Concern

Data Sovereignty

EXECUTIVE SUMMARY FINDING 1

VALIDATED

Local Data Mode Prevents User Data Egress

Security Concern

The assessment tested whether flight data, imagery, or telemetry could leave the operator's custody while Local Data Mode was enabled on DJI controllers and applications.

Test Performed

The team captured and reviewed traffic from the DJI RC 2 with DJI Fly (Air 3S) and the RC Plus 2 Enterprise with DJI Pilot 2 (Matrice 4E) in both standard data mode and Local Data Mode across pre-flight, flight, and post-flight states to determine whether user data reached internet-based destinations.

Outcome

Local Data Mode prevented user data from being sent from the drone flight-control application to internet-based locations. Even after returning to normal mode, no data related to past flights was sent via the internet. Local Data Mode did not fully isolate the controller itself because the controller operating system and other applications could still connect.

Recommendation

Align the DJI Trust Center privacy guidance with actual DJI Fly (RC 2) and DJI Pilot 2 (RC Plus 2 Enterprise) behavior regarding egress traffic while Local Data Mode is enabled, and evaluate an OS-level prompt on the controller that encourages disconnecting the controller from WiFi when LDM is engaged for a full network air-gap.

NEXT STEPS

For complete isolation, operators should disable the controller's network connection in addition to Local Data Mode. DJI should keep controller behavior and Trust Center privacy guidance aligned in future firmware and application releases.

National Security Concern

Data Sovereignty

EXECUTIVE SUMMARY FINDING 2

VALIDATED

No Evidence of Data Sent Outside the United States

Security Concern

A central objective of the engagement was to determine whether the controllers or flight-control applications transmitted data to non-U.S. systems.

Outcome

The engagement found no evidence of data being sent outside the United States from the controller devices or drone flight-control applications. Observed connections were to U.S.-based IP addresses, including content-delivery infrastructure associated with Alibaba and Tencent, along with expected services from Google, Facebook, Mozilla, Amazon, and others.

Test Performed

The team performed packet capture and destination analysis during normal operation and Local Data Mode, then reviewed observed traffic to determine whether any communications were sent to non-U.S. systems.

Recommendation

DJI should continue working with geographic IP database providers to reduce ambiguity around service location and, where needed, migrate services to infrastructure that is more consistently identified as U.S.-based.

NEXT STEPS

Future testing should continue validating destination geography and confirm that observed traffic remains limited to expected U.S.-hosted services throughout firmware and application changes.

National Security Concern
Hardware Vulnerabilities

EXECUTIVE SUMMARY FINDING 3

VALIDATED

No Unexplained Radio Emissions Identified

Security Concern
The hardware assessment examined whether the drones emitted undocumented radio frequencies that could indicate hidden communications capability or covert transmission outside documented behavior.

Test Performed
Two units of each drone model were operated repeatedly in multiple environments while RF emissions were monitored. The team identified all feasible spectrum areas, performed focused analysis on each emission, repeated tests to isolate spurious signals, and correlated undocumented emissions to known drone functions.

Outcome
No unexplained radio emissions were identified. All observed RF emissions were traced back to known functions on the drones. Some emissions were not included in FCC documentation at the start of the engagement, but they were confirmed to be artifacts of the documented signal-synthesis methods and changed in direct correlation with known protocols and operating states.

Recommendation
DJI should document spurious transmissions explicitly as artifacts of the primary control frequencies so later evaluations can distinguish expected RF byproducts from genuinely anomalous emissions, and remove 4G-dongle-associated antenna structures from drones sold in the U.S. market.

NEXT STEPS

Future hardware and firmware revisions should continue to be assessed so that any observed emissions remain attributable to known system behavior and documented engineering mechanisms.

National Security Concern
Drone Manipulation

EXECUTIVE SUMMARY FINDING 4

LOW RISK / OBSERVATION

Mobile Application Findings Were Limited and Operationally Manageable

Security Concern

The engagement evaluated whether weaknesses in the mobile applications used to control the drones could create realistic threats to flight safety or cause widespread leakage of confidential information.

Test Performed

The assessment included static and dynamic testing of DJI Fly and Pilot 2, controller and application traffic analysis, and evaluation of vulnerabilities associated with privacy, controller exposure, and adversarial effects on drone operation.

Outcome

A moderate number of low-risk and observation-level findings were identified in the mobile applications. None of these findings presented a realistic risk to safe drone operation or to widespread exposure of confidential information. DJI collaborated on potential fixes and is working toward resolving many of the issues in later software versions.

Recommendation

DJI should continue remediating identified low-risk issues, particularly around session handling, FlyShare input validation, exposed controller ports, signing credentials, and wireless hardening, while operators track residual risk through standard risk-management processes.

NEXT STEPS

Operators may continue operating the drones with compensating controls while DJI resolves the remaining low-risk findings in subsequent software releases. This residual-risk approach is well established in information-security practice and aligns with guidance referenced by NIST RMF, CISA, ISC2, and related cybersecurity standards bodies.

Additional Details and Recommendations

Specific findings and recommendations for each area of testing are detailed within the Assessment Technical Details section of this report. Future recommendations include the following testing cadence to ensure continued assurance of United States national security interests:

Continuous Testing Recommendation Moving Forward

This individual assessment is bound by its scope and time and therefore cannot accurately measure security and data privacy into the future. Continuous validation testing is a recommended future activity that would provide ongoing assurance regarding national security concerns.

Continuous validation testing is the practice of repeatedly testing live services with statistically significant sample sizes across the full range of hardware devices, firmware, applications, and supporting services to ensure substantial, ongoing coverage rather than relying on one-time validation. Full tests should be performed for every hardware and firmware version, and for any software release that introduces or substantially refactors capabilities. Sample based testing should be performed on an ongoing basis to identify any variances in how firmware and software interact with supporting services and to test against new cyber-adversary methodologies. This approach maintains continuous confidence in end-to-end system behavior as any changes in the technology stack over time are pro-actively identified.

While the specific cadence for continuous testing is context dependent, OnDefend generally recommends a continuous validation testing cadence like the example shown below.

STANDARD	**Software**	Every major release at minimum. Once per month to once per quarter depending on company's software release cycle.
	Firmware	Every major release at minimum, normally a few times per year, depending on the release cycle.
ADVANCED Powered by OnDefend Technology	**Hardware Teardown & RF Transmissions**	Every component or supply chain revision. At least once per year is a general expectation for a full test, with periodic samples to validate prior test results are applied to future units between full tests.
	Supply Chain Integrity & HBOM	

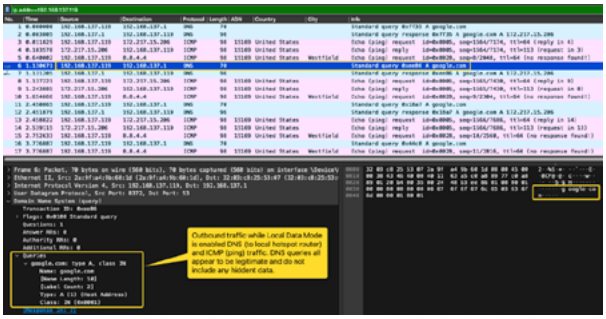
Application Security, Hardware & Firmware Analysis

STANDARD TESTING

Egress Network Activity Analysis

Full packet capture is performed at a controlled WiFi access point to inspect all traffic between the controllers and the drones in scope. Both indoor and outdoor test environments leverage this method to capture and analyze traffic during every phase of testing, including preflight, in flight, and post flight states. Capture is sustained across power cycles and across changes to data mode settings to confirm that observed behavior is consistent with documented controls.

Captured traffic is inspected for contents, protocol, total connection size, and the location and nature of external services, and is correlated with specific user actions on the controller. This characterizes traffic patterns and validates whether flight, video, or image data is transmitted, without requiring decryption of encrypted streams. Comparative baselines are produced against unmodified mobile operating systems (for example, an Android virtual device of the same major version) to determine whether observed network connections originate from the application under test or from the underlying operating system.



HTTP and HTTPS traffic between the application and its backend services is intercepted using an interception proxy after bypassing certificate pinning. Authentication tokens, session lifetimes, signing schemes, and replay characteristics are evaluated against industry guidance, including the OWASP Mobile Application Security Testing Guide and the OWASP Session Management and OAuth 2.0 cheat sheets. TLS configuration on accessible endpoints is reviewed for deprecated protocols, weak cipher suites, and missing forward secrecy.

Network Service and Exposed Port Testing

Network analysis is performed against both drones and controllers while they are connected and operating. Listening services and open ports are enumerated and fingerprinted, and any proprietary services are exercised by sending crafted, randomized, or malformed input to characterize the protocol and identify failure modes. Exposed services are tested for vulnerable configurations, authentication weaknesses, and resource exhaustion (denial of service) conditions. Where impact is observed against the application without affecting flight controls, the boundary between application functionality and safety critical control paths is documented.

Controller and Device Access

All standard techniques are attempted to root the controllers and to gain a privileged shell on associated devices. Where conventional rooting paths are unsuccessful, custom controller applications are developed that provide direct operating system access to the device, along with monitoring of all available drone telemetry across every phase of flight as well as controller state. This access is then used to validate the source and nature of every packet identified during traffic capture, to retrieve installed application binaries, and to read configuration and runtime data that is not otherwise exposed.

Application Binary and Runtime Analysis

Mobile and on device applications are analyzed using both static and dynamic techniques. Static analysis is performed against extracted application packages and native shared libraries using disassemblers and decompilers such as Ghidra. Static review focuses on embedded keys, request signing logic, hardcoded endpoints, authentication mechanisms, exported native symbols, and use of insecure cryptographic primitives. Dynamic analysis is conducted on rooted devices using runtime instrumentation frameworks such as LSPosed and Xposed (or equivalent hooking frameworks) to intercept calls at the Java to native boundary and to observe parameters passed into security relevant functions, including signing keys, nonces, timestamps, and request paths.

Hardware Teardown & RF Transmissions

ADVANCED TESTING
Powered by OnDefend Technology

RF Spectrum Baseline and Anomaly Detection

The radio frequency methodology begins with repeated scans of the electromagnetic spectrum from 1 MHz to 6 GHz in a controlled laboratory environment with all target devices powered off. These scans aggregate ambient transmissions in the room into an environmental baseline. Devices are then powered on and exercised across operational states aligned to real world usage, including paired and idle, paired with active video feed, and active flight, while transmissions are continuously recaptured.

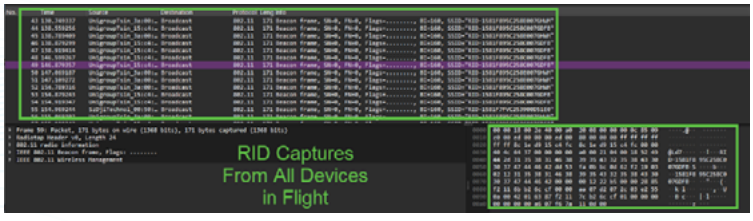
Captured transmissions are compared against the environmental baseline using subtractive analysis to isolate emissions that exceed ambient levels. Statistical analysis across repeated measurements, including kurtosis evaluation to detect bursty or non-Gaussian behavior, filters out anomalous signals that are not consistently attributable to the device under test. Drones are also operated in a clear sky outdoor setting so that any functionality contingent on satellite reception, such as GNSS, is active and observable. Spectrograms validate signal characteristics (constant frequency, bursty, or frequency hopping spread spectrum), and IQ analysis differentiates modulated signals from electronic noise.

Initial Signal Characterization

Initial RF analysis characterizes detected signals and identifies plausible activity by cross referencing FCC filings, manufacturer documentation, drone operating manuals, and common uses of the identified frequency bands. Candidates are flagged for additional testing to rule out harmonic artifacts, intermodulation products, and electromagnetic interference originating from onboard electronics such as high-speed buses, camera transmission lines, and time of flight sensors.

ADS-B Reception and Remote ID Transmission

Expected Remote ID (RID) transmissions are validated, including WiFi beacon-based broadcasts, and the exploitation surface of the RID service is examined. ADS-B reception is tested for resilience, with malformed packets injected on 978 MHz and 1090 MHz to evaluate the device's handling of out of specification traffic. Where a feature is reported as receive only, additional testing is planned to confirm that no transmission is observed on the corresponding frequencies during operation.

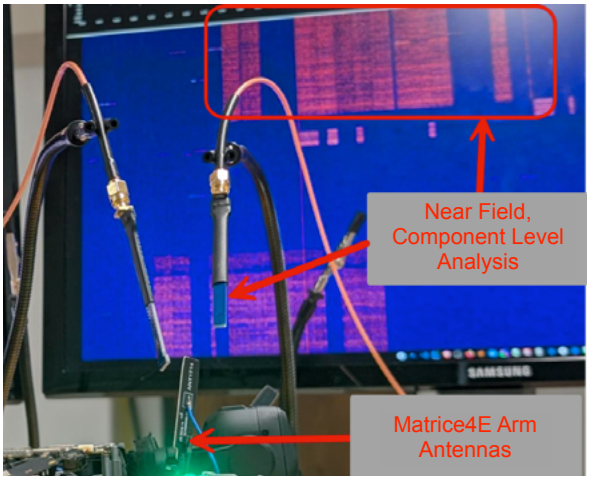


Hardware Teardown & RF Transmissions

ADVANCED TESTING
Powered by OnDefend Technology

Hardware Breakdown and Near Field Component Analysis

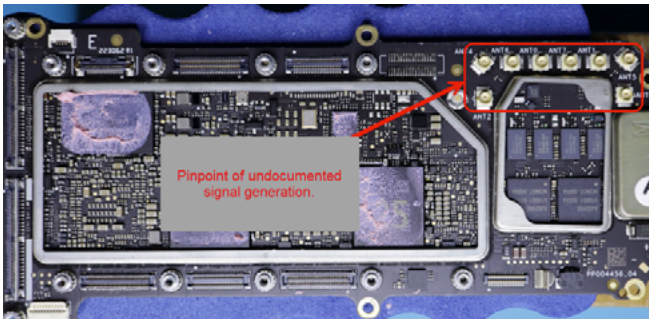
All identified frequencies are tracked to a specific operating mode and to a specific generating component using 1mm near field antennas in conjunction with full spectrum analysis. Hardware breakdown proceeds through cycles of component elimination while preserving the ability to power on and operate the device. Suspected emitters such as time-of-flight sensors, camera modules, and antenna assemblies are progressively removed and the device is re-tested after each modification. Where spurious transmissions persist after removal of suspected sources, near field probing of the remaining boards isolates the originating component down to the level of an individual integrated circuit or trace.



Where the controller exposes manual selection of operating band, channel, or bandwidth, these settings are manipulated during operation to test for one to one shifts in spurious emissions. Confirmed correlation between control settings and spurious frequencies supports hypotheses such as PLL or divider leakage in the signal pre processing circuit, and helps distinguish leakage artifacts from intentional secondary transmissions.

RF Exploitation

Identified frequencies are evaluated for exploitability through replay attempts, amplified disruption (jamming), and multi-source interference, as well as through malformed protocol injection against ADS-B and Remote ID. All RF exploitation activity is conducted within legal and authorized limits in the testing environment. Observed effects are documented along the dimensions of telemetry impact, video link impact, and flight control impact, so that the safety boundary between disruption of application features and loss of flight control is clearly recorded.



Supply Chain Integrity & HBOM

ADVANCED TESTING
Powered by OnDefend Technology

Device Procurement

Test devices are procured autonomously through public retail or authorized distribution channels that are representative of inventory available to end users in the target market. The vendor is selected by the engagement team without prior coordination with the manufacturer, and the manufacturer is notified only after the units have shipped. Units are shipped to an address of the engagement team's choosing. This procurement model ensures that devices under test are representative of those received by typical customers, and that the supply chain has not been pre staged or modified for the purposes of the assessment. The procurement record, including vendor, purchase date, and serial numbers, is preserved with the engagement evidence.

Component Cataloging (HBOM Development)

During teardown, every major board, module, and integrated circuit of interest is photographed and recorded. Chip markings, manufacturer identifiers, package types, and (where determinable) country of origin are captured for each component. Components are mapped to their functional role within the device, including radio front end, baseband and transceivers, application processor, sensors, memory, and power management. The resulting Hardware Bill of Materials (HBOM) provides a structured inventory of the device's physical composition that supports downstream analysis of supply chain risk and undocumented capability.

Firmware, Operating System, and Application Inventory

A firmware and software inventory is produced for each device under test. Firmware images, operating system build identifiers, kernel and bootloader versions, and installed application versions are enumerated for both the drone and its associated controller. Where firmware is upgradeable, each version observed during the engagement is recorded along with the procedure used to obtain or apply it. Mobile applications associated with the device are inventoried by package name and version, and significant native libraries packaged within those applications are listed. This inventory establishes a known, reproducible baseline against which subsequent versions, configurations, and behaviors can be compared.

Public Documentation Cross-Reference

Observed hardware components and radio behavior are cross referenced against the manufacturer's FCC filings, datasheets, user and operator manuals, and other publicly available documentation. The cross reference identifies components or radios that are present in the device but not described in the manufacturer's published material, capabilities that exceed the stated operating envelope (for example, transmissions outside FCC documented bands), and discrepancies between marketing material and observed behavior. Findings from this cross reference inform both the supply chain risk picture and the targeting of follow-on RF, hardware, and firmware testing.

Secure Your Environments . Outpace the Adversary.

OnDefend.com

OnDefend

Headquarters
10151 Deerwood Park Blvd. Building 200 – Suite 110 Jacksonville, FL 32256

General Inquiries
Contact@OnDefend.com

Telephone
1-800-214-2107