TLP:GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

CISA
CYBER+INFRASTRUCTURE

20 November 2019

PIN Number
20191120-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Interior (DOI) Office of Aviation Services (OAS) with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released TLP:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

Risks of Using Unmanned Aircraft Systems

Summary

Organizations are leveraging versatile Unmanned Aircraft Systems (UAS) for identifying physical security gaps and vulnerabilities at facilities, searching and surveying large areas in reduced time, monitoring and securing areas with rapid response, and site inspection. UAS incorporate technologies which generate or collect sensitive data or otherwise are accessing critical systems. Organizations should be aware of the potential exposure of private data through operating UAS. Sensitive data may be at greater risk of exposure when operating UAS designed, manufactured, or supplied abroad where the data is stored, transferred to, or accessible by servers in a foreign country.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

Organizations need to be aware of the various cyber risks the use of UAS present to their and their customers' information. As with all connected devices, the protection of sensitive information or intellectual property remains a significant challenge and should be a top priority. Organizations conducting operations associated with national security or the Nation's critical functions must remain especially vigilant as they may be at risk for espionage and theft of sensitive information. Additionally, the US government has strong concerns when UAS data is stored, transferred, or accessible in the territory of a foreign country with limited or no data privacy protections, or subject to a foreign government which does not share the US's Constitutional norms and values, including meaningful and independent judicial review.

UAS have the potential to expose information through the following vectors (see also the May 2019 DHS CISA Industry Alert, *Chinese Manufactured Unmanned Aircraft Systems*):

- **Operators:** Inexperienced operators can place an organization's UAS device and its data at risk if they do not follow established procedures for securing the UAS before, during, and after flight. Both transmitted and stored data are vulnerable when the device, its components, or its transmission feed are not properly secured by the operator.
- **Manufacturers & Vendors:** An organization's information is at risk if it employs technology corrupted by malware or performs automatic data transmission back to a third party. Manufacturers and vendors of UAS, its firmware, and software applications potentially can build in malware or collect data from UAS devices without an organization's knowledge.
- **Data Theft:** Organizations are susceptible to theft of information if the UAS device and an organization's network are not properly secured, and if the communication feed on which the UAS is operating is unencrypted. The potential data at risk to exposure from using a UAS includes: location data; personally identifiable information (PII); phone/tablet data; video/pictures; biometric data; and flight logs and telemetry data.
- **Network Intrusion:** UAS—as with other connected, Internet of Things devices—can expose organizations to network breaches, which could lead to unauthorized access to company internal data sets and other information. Malware incorporated into software, firmware, or hardware modules within the UAS supply chain may potentially spread to a corporate network depending on its design and how data is retrieved from the UAS.

- **Wireless Communications:** UAS and their controllers may be susceptible to various local wireless attacks because they communicate using a number of protocols, and are impacted by whether or how the communications are encrypted. Some potential attacks include: GPS spoofing, command injection, tracking, WPA2 defeat, and forced disconnection. The outcomes of local wireless attacks range from denial-of-service and destruction to hijacking and remote command execution.[a]
- **Foreign Law Enforcement and Foreign Government Cooperation:** While companies operating within any country are typically expected to comply with applicable law and government regulations, foreign governments may require companies to disclose far more information without significant legal protection for customers. UAS data is often sent to servers controlled by or accessible to the UAS manufacturing company or third-party application vendor. For UAS designed, manufactured, or supplied abroad, company Internet servers may be located in the US and/or in foreign countries. Data servers run by or accessible to foreign companies, especially those located in foreign countries, may be susceptible to foreign law enforcement and government seizure without the benefit of the types of legal protections under US law.

Mitigation Strategies

Commercial UAS operators should refer to the DHS CISA *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems* (11 June 2019), and the DOI OAS *Unmanned Aircraft Systems (UAS) Best Practices for Responsible Operations*[b] (22 February 2019).[c] For further information, please see the section, "How Organizations May Reduce Risk" in the May 2019 DHS CISA Industry Alert, *Chinese Manufactured Unmanned Aircraft Systems*.

[a] Research Article; Watkins, Lanier, et al.; 26 June 2018; "Exploiting Multi-Vendor Vulnerabilities as Back-Doors to Counter the Threat of Rogue Small Unmanned Aerial Systems"; https://dl.acm.org/citation.cfm?id=3215467; Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy.

[b] U.S. Department of the Interior (DOI) Office of Aviation Services, 22 February 2019, "Unmanned Aircraft Systems (UAS) Best Practices for Responsible Operations"; https://www.doi.gov/sites/doi.gov/files/uploads/doi_uas_best_practices_for_responsible_operations_v1.0_2-22-19.pdf.

[c] Further information on security requirements can be found under Command and Control and Miscellaneous Specifications tables of U.S. Department of the Interior (DOI Office of Aviation Services, 15 March 2019, "Master UAS Requirements for the DOI"; https://www.doi.gov/sites/doi.gov/files/uploads/doi_master_uas_requirements_document_-_v1.3_3-15-19.pdf

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

The following are additional and complementary mitigation suggestions for UAS initial setup, offline use, and use with mobile devices:

- During initial UAS activation, use of a designated generic name, email address, and password unassociated to a specific company may reduce a UAS manufacturer's ability to track the owner/user through association with this identifier. *Note*: It should be assumed that the current GPS location will be transmitted during UAS activation, which could reveal the true owner.
- Care should be taken when setting up any mobile device to be used with a UAS designed, manufactured, or supplied by a foreign country to minimize any exposure or collection of PII. New mobile devices without a SIM card installed or set up previously and never used for other activities will contain limited to no PII collectable by a foreign UAS company. For previously-used devices, performing a wipe and factory reset of the mobile device prior to using it as a controller is advisable.

Additional Information

Although the DOI OAS has tested UAS technology[d] with its industry and federal partners, this PIN should not be considered an endorsement for or warning against any particular UAS manufacturer, model, or software solution.

Administrative Note

This product is marked TLP:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

[d] DOI OAS signed a limited authorization applicable to tested UAS technology (https://www.doi.gov/sites/doi.gov/files/uploads/limited_dji_uas_ authorization_-_final_signed_-_july_3_2019.pdf). See, e.g., DOI OAS Frequently Asked Questions (https://www.doi.gov/ sites/doi.gov/ files/uploads/ key_messages_and_faqs_-_oas_uas_data_management_assurance_flight_test_and_technical_ evaluation_report.pdf) and the DOI OAS report (https://www.doi.gov/sites/doi.gov/files/uploads/oas_flight_test_and_technical_evaluation_ report_-_dji_uas_data_managment_assurance_evaluation_-_7-2-19_v2.0.pdf).

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

For comments or questions related to the content or dissemination of this product, contact FBI CyWatch. For more information please visit the DHS CISA UAS site, at https://www.dhs.gov/cisa/uas-critical-infrastructure, and the DOI OAS UAS site, at https://www.doi.gov/aviation/uas/news.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey