CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY BEST PRACTICES FOR OPERATING COMMERCIAL UNMANNED AIRCRAFT SYSTEMS (UASs)

UASs provide innovative solutions for tasks that are dangerous, time consuming, and costly. Critical infrastructure operators, law enforcement, and all levels of government are increasingly incorporating commercial UASs into their operational functions and will likely continue to do so. Although UASs offer benefits to their operators, they can also pose cybersecurity risks, and operators should exercise caution when using them.[1]

To help UAS users protect their networks, information, and personnel, the Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) identified cybersecurity best practices for operating commercial UASs. This document can assist in standing up a new UAS program or securing an existing UAS program, and is intended for information technology managers and personnel involved in UAS operations. Similar to other cybersecurity guidelines and best practices, the identified best practices can aid critical infrastructure operators to lower the cybersecurity risks associated with the use of UAS, but do not eliminate all risk.

Installation and Use of UAS Software and Firmware

- Ensure that the devices used for the download and installation of UAS software and firmware do not access the enterprise network.
- Properly verify and securely conduct all interactions with UAS vendor and third party websites. Ensure file integrity monitoring processes are in place before downloading or installing files.
- Run all downloaded files through an up-to-date antivirus platform before installation and ensure the platform remains enabled throughout installation. Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic.
- Thoroughly review any license agreements prior to approval. During installation, do not follow "default" install options. Disable automatic software updates. Necessary updates should follow the same process outlined for download and installation.

Securing UAS Operations

- If using Wi-Fi, ensure the data link supports an encryption algorithm for securing Wi-Fi communications. Use the most secure encryption standards available and complicated encryption keys that are changed regularly.
- Use complicated Service Set Identifiers (SSIDs) that do not identify UAS operations on the network. Set the UAS to not broadcast the SSID or network name of the connection.
- Use standalone UAS-associated mobile devices with no external connections, or disable all connections between the Internet and the UAS and UAS-associated mobile devices during operations.
- Run mobile device applications in a secure virtual sand-box configuration that allows operation while securely protecting the device and the operating system.

Data Storage and Transfer

- Use a standalone computer to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network.
- Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused from the connection of the UAS or removable storage device. Verify and ensure that the computer has up-to-date antivirus installed.
- Follow data management policies for data at rest, data in transit, and any sensitive data.
- Erase all data from the UAS and any removable storage devices after each use.

(Continued on Back)

[1]For more information on UAS cybersecurity risks, see: DHS Office of Cyber and Infrastructure Analysis. (2018). "Cybersecurity Risks Posed by Unmanned Aircraft Systems." PDM17252. Additional information can be found in: DHS Cybersecurity and Infrastructure Security Agency. (2019). "Unmanned Aircraft Systems Industry Alert."

Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs)

Information Sharing and Vulnerability Reporting

By participating in information-sharing programs and reporting non-public, newly-identified vulnerabilities, users will have access to timely information to mitigate cybersecurity threats.

- The Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely information exchange through trusted, public-private partnerships across all critical infrastructure (CI) sectors. For more information on the CISCP program, visit **cisa.gov/CISCP** or email **CISCP_Coordination@hq.dhs.gov.**
- The Automated Indicator Sharing (AIS) Program enables the quick exchange of cyber threat indicators between the Federal Government and the private sector through CISA. For more information on NCCIC 24/7 services, call 1-888-282-0870 or email **NCCICCustomerService@hq.dhs.gov**. For more information on AIS and how to join, go to **https://www.us-cert.gov/ais/**.
- The Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry. For more information about ISACs, go to **https://www.nationalisacs.org/**.

If a UAS software or hardware vulnerability is discovered, or a suspicious or confirmed UAS cybersecurity incident occurs, CISA recommends reporting the vulnerability or incident through the following channels:

- Email CISA at NCCICCustomerService@hq.dhs.gov or call 1-888-282-0870. When sending sensitive information to DHS CISA via email, we recommend encryption of messages. For more information, visit **https://ics-cert.us-cert.gov/Report-Incident**.
- To report a vulnerability to the CERT Coordination Center, go to **https://www.kb.cert.org/vuls/report/**.

CONTACTS

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

For More Information, contact NRMC@hq.dhs.gov
or visit our website:
www.cisa.gov/national-risk-management