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 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.

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 UASs. This product, a companion piece to CISA's Foreign Manufactured UASs Industry Alert, 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

An important part of managing risk when employing UASs is to understand the steps involved and potential vulnerabilities introduced during the installation and use of UAS software and firmware. UAS operators should strongly consider and evaluate the following cybersecurity best practices when dealing with software and firmware associated with UAS:

- 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. Take extra precaution to download software from properly authenticated and secured websites and ensure app store hosts verify mobile applications.
    - Access these websites or app stores from a computer not associated with, or at least not connected to, the enterprise network or architecture.
    - Ensure the management of security for mobile devices that will be directly or wirelessly connected to the UAS.[1] Review additional information for enhancing security on mobile devices.[2,3]

[1] For more information, see: National Institute of Standards and Technology (NIST). (2013). "Guidelines for Managing the Security of Mobile Devices in the Enterprise." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. Accessed May 16, 2019.
[2] For mobile security guidance from Apple, visit www.apple.com/privacy/manage-your-privacy.
[3] For mobile security guidance from Android, visit www.android.com/play-protect.

- Ensure file integrity monitoring processes are in place before downloading or installing files. Check to see if individual downloads or installation files have a hash value or checksum.[4] After downloading an installation file, compare the hash value or checksum of the installation file against the value listed on the vendor's download page to ensure they match.
- 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 caused by the recently installed software. External network communications could be part of the installation process and could potentially expose your system to unknown data privacy risks.
- During installation, do not follow "default" install options. Instead, go through each screen manually and consider installing software on a removable device (external HDD or USB drive).
    - Deselect any additional features or freeware bundled into the default install package.
    - Disable automatic software updates. Necessary updates should follow the same process outlined for download and installation.
    - Thoroughly review any license agreements prior to approval. Consider involving a legal team in the process to ensure organizations do not unknowingly agree to unsafe or hazardous practices on the part of the vendor.

SECURING UAS OPERATIONS

An important part of operating UASs is to ensure that communications are secure during all aspects of usage. There are multiple publicly accessible sites that indicate and detail how to intercept UAS communications and hijack UASs during flight operations. UAS operators should consider and evaluate the following cybersecurity best practices when conducting UAS operations:

- If a UAS data link is through Wi-Fi connections between the UAS and the controller.[5]
    - Ensure the data link supports an encryption algorithm for securing Wi-Fi communications.
        - Use WPA2-AES security standards or the most secure encryption standards available.
        - Use highly complicated encryption keys that are changed on a frequent basis. Ensure that encryption keys are not easily guessable, and do not identify the make or model of the UAS or the operating organization.
    - Use complicated Service Set Identifiers (SSIDs) that do not identify UAS operations on the network. Avoid using the specific make or model of the UAS or the operating organization in the SSID.
    - Set the UAS to not broadcast the SSID or network name of the connection.
    - Change encryption keys in a secure location to avoid eavesdropping either visually or from wireless monitoring.
- If the UAS supports the Transport Layer Security (TLS) protocol, ensure that it is enabled to the highest standard that the UAS supports.

[4] A checksum is a value derived from a segment of computer data calculated before and after transmission to assure data is free from tampering and errors. A hash value is a fixed-length numeric value that results from the calculation of a hashing algorithm. A hash value uniquely identifies data and is often used for verifying data integrity.
[5] For more information on securing a wireless network, see: DHS Cybersecurity Engineering. (2017). "A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)." www.us-cert.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf. Accessed March 18, 2019.

- Have the data links for UAS control, telemetry, payload transmission, video transmission, and audio transmission encrypted with different keys. Make sure the UAS is able to encrypt the data stored onboard.
- 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. Consider running wireless traffic analyzers during selected UAS operations to understand and monitor UAS communications traffic while in use.
- 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

Ensuring the security and privacy of UAS data, while at rest or in transit, is essential to managing UAS cybersecurity risks. UAS operators should consider and evaluate the following cybersecurity best practices for UAS data storage and transfer:

- When connecting the UAS or UAS-associated removable storage device to a computer:
  - 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.
- Data should be encrypted both at rest and in transit to ensure confidentiality and integrity.[6]
- Authentication mechanisms should be in place for UASs with access to private or confidential data. Use Multi-Factor Authentication (MFA) whenever possible for accounts associated with UAS operations.[7]
- 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.

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. These programs can also serve as a forum for UAS operators to share security vulnerabilities that could potentially impact the Nation's critical infrastructure or pose a threat to public health and safety. The following are three information sharing programs:

- Cyber Information Sharing and Collaboration Program (CISCP):
  - CISCP enables actionable, relevant, and timely information exchange through trusted, public-private partnerships across all critical infrastructure (CI) sectors by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused, operational context.

[6] For more information on encrypting stored data, see: National Institute of Standards and Technology (NIST). (2007). "Guide to Storage Encryption Technologies for End User Devices." NIST Special Publication 800-111. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf. Accessed March 15, 2019.
[7] For more information on security controls, see: National Institute of Standards and Technology (NIST). (2013). "Security and Privacy Controls for Federal Information Systems and Organizations." NIST Special Publication 800-53, Revision 4. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf. Accessed March 15, 2019.

  - For more information on the CISCP program, visit www.dhs.gov/ciscp or email CISCP_Coordination@hq.dhs.gov.

- Automated Indicator Sharing (AIS) Program:
  - The AIS program enables the quick exchange of cyber threat indicators between the Federal Government and the private sector through CISA. Companies that share indicators through AIS are granted liability protection and other protections through the Cybersecurity Information Sharing Act of 2015.
  - For more information on CISA services, call 1-888-282-0870 or email Central@cisa.gov. For more information on AIS and how to join, go to www.cisa.gov/automated-indicator-sharing-ais.
- Information Sharing and Analysis Centers (ISACs):
  - 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. CISA, through the NCCIC, works in close coordination with all of the ISACs.
  - For more information about ISACs, go to www.nationalisacs.org/.

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

- DHS CISA:
  - Email Central@cisa.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 us-cert.cisa.gov/report.
- CERT Coordination Center:
  - To report a vulnerability, go to www.kb.cert.org/vuls/report.

The UAS Cybersecurity Best Practices document is a collaborative product written by CISA's National Risk Management Center and Cybersecurity Division. This product was coordinated with the DHS/CISA/Infrastructure Security Division, DHS/Federal Protective Service, U.S. Army/Combat Capabilities Development Command, and Federal Bureau of Investigation/Cyber Division.

The National Risk Management Center (NRMC), Cybersecurity and Infrastructure Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit www.cisa.gov/national-risk-management.

June 11, 2019