IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security CIO-IT Security-20-104

Revision 1

February 14, 2023

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – December 26, 2019		
N/A	ISE	Initial Release	New guide providing guidance regarding the security and use of drones.	N/A
		Revision 1 – February 14, 2023		
1	ISI	Updated references and removed ability for GSA to purchase UAS.	Updates to GSA policies and procedures	Throughout
2	McCormick	• Updated language to reflect current drone/UAS policies and procedures. • Edited and formatted to current guide formatting. • Updated hyperlinks.	Align to current formatting and style.	Throughout

Approval

IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security, CIO-IT Security 20-104, Revision 1, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

1 Introduction

This procedural guide provides an overview of the process by which small Unmanned Aircraft Systems (UAS), also known as drones, are registered and authorized for use by contractors on behalf of the General Services Administration (GSA). GSA Order OAS 5615.1, "GSA Unmanned Systems (UAS) Policy," prohibits the agency from purchasing Federal aircraft, including UAS.

Part 107, Small Unmanned Aircraft Systems Regulations, provides operating requirements for UAS or drones weighing less than 55 pounds. At GSA this includes any unmanned aircraft used on behalf of GSA for any business purpose, including surveillance of buildings or aerial photography/video capture. Operators of drones on the GSA must conform to requirements and operating rules as specified in Part 107; drones that exceed 55 pounds are not allowed at GSA.

GSA recognizes that UAS may have functionality that poses risks to GSA's Information Technology (IT) security posture. These risks originate from:

1. **Operators**: Both transmitted and stored data are vulnerable when a UAS device, its components, or its transmission feed are not properly secured by the operator.
2. **Manufacturers and Vendors:** Supply chain risks exist if the UAS contains malware or contains automatic data transmission back to a third party.
3. **Data Theft**: Organizations are susceptible to theft of information if the UAS device operates on improperly secured communications feeds.
4. **Network Intrusions:** UAS can expose organizations to network breaches.

In addition, UAS that do not have sufficient cybersecurity protections may be at risk of being hijacked. A hijacked UAS device could pose a safety threat to personnel or a threat to physical assets.

To achieve the GSA's mission and meet GSA's customer's needs, the GSA Office of the Chief Information Security Officer (OCISO) has established the following process for evaluating the IT Security risk posture of UAS proposed for GSA purchase and subsequent use. This process includes both approvals at the model level in support of maintaining a UAS device on the GSA IT Standards profile, as well as a user registration/re-certification process to track individual device approvals.

1.1 Purpose

The purpose of this procedural guide is to identify a process for GSA Federal employees and contractors to request security approval to use a UAS. In addition, this document defines the OCISO process and procedures to facilitate security assessment of UAS in support of GSA Order CIO 2160.1F CHGE 2, "GSA Information Technology (IT) Standards Profile." This guide supplements the software security testing procedures identified in GSA CIO-IT Security-16-72: Software Security Testing.

2 Pre-Purchase UAS Security Considerations

GSA customers that are interested in selecting UAS for business use should possess the following prior to purchase:

- Knowledge of reputable vendors for purchase of UAS devices and components.
- Understanding of how and where UAS data is being stored.
- Determination of how the UAS device will interact with infrastructure and networks.

2.1 Using Reputable Vendors

Conduct research and ensure any vendors from whom a purchase of UAS devices and components is planned are trustworthy. Considerations should include the country where the manufacturer originates.

Note that GSA will not approve use of any drone produced by or containing substantial or critical components from a prohibited source, as maintained on the C-SCRM Policies, Regulations, and Laws Prohibited Sources and Supply Chain Risk Management (SCRM) InSite page that includes the following as of November 2022:

- Dahua Technology Company
- Hangzhou Hikvision Digital Technology
- Huawei
- HyTera
- ZTE (URL is not secure)
- Kaspersky Lab
- Any subsidiaries or affiliates of the listed vendors
- Hardware, software, telecommunications, or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

In addition, GSA may restrict purchase and/or use of UAS if the cybersecurity, privacy, or supply chain risk is assessed to be unacceptable.

2.2 Understanding Data Storage

Determine if UAS data is being stored by the vendor or other third parties. If the data is being stored, determine how, where, and for how long the data is being stored. UAS device approvals will be limited to local storage or already authorized platforms (e.g., GSA’s Google Drive instance).

2.3 Determining Infrastructure and Network Interaction

To avoid compromising sensitive or controlled information, understand how to properly operate and limit the UAS device's access to networks to avoid unnecessary exposure of data to external threats. There are proactive steps that can be taken to deactivate vulnerable features of UAS detailed in Section 3.

3 General UAS Security

Although UAS offer benefits to an organization, they can also pose cybersecurity risks, and caution should be exercised when using them. To help protect networks and information, the following cybersecurity best practices should be used to assist in reducing the risk associated with the use of UAS within an organization. The following sections describe general processes and requirements that should be applied to UAS devices in use at GSA and are based on general UAS/drone security best practices and consideration for securing like devices.

3.1 Installing and Using UAS Software and Firmware

When employing UAS within an organization, operators should use the following best practices related to the installation and use of UAS software and firmware.

- Ensure 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 vendors and third party websites. Extra precaution should be taken 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 UAS devices.
  - Review all additional information for enhancing security on mobile devices.
- 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. After downloading the 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 that 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 the system to unknown data privacy risks.

- During installation, operators should not follow "default" install options. They should go through each screen manually to understand what options are being selected. Operators should:
  - 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.

3.2 Securing UAS Operations

An important part of operating UAS is to ensure secure communications during all aspects of usage. There are multiple publicly accessible sites that indicate and detail how to intercept UAS communications and hijack UAS during flight operations. UAS operators should 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:
  - Ensure the data link supports an encryption algorithm for securing Wi-Fi communications.
    - Use WPA2-AES security per GSA Policy standards.
    - Use highly complicated encryption keys that are changed on a frequent basis. Ensure 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.
- Have the data links for UAS control, telemetry, payload transmission, video transmission, and audio transmission encrypted with different keys. Make sure the UAS can 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.

3.3 Storing and Transferring Data

Ensuring the security and privacy of UAS data, while at rest or in transit, is essential to managing UAS cybersecurity risks. Consistent with applicable laws and requirements, including the E-Government Act of 2002, and to ensure the protection of privacy, GSA will only collect information from UAS sensors, and will only use, retain, or disseminate information obtained from such UAS sensors, for a properly authorized purpose, as documented in a Privacy Threshold Assessment (PTA) and in accordance with GSA Order CIO 1878.3, "Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices," in GSA. In general, existing security requirements still apply to UAS, including requiring that storage of data on third party servers be limited to platforms with an Authorization to Operate (ATO). UAS operators should 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:
  - A standalone computer should be used to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network.
  - Verification that a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused by 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.
- Authentication mechanisms should be in place for UAS with access to private or confidential data. Multi-Factor Authentication (MFA) should be used whenever possible for accounts associated with UAS operations.
- Data management policies for data at rest, data in transit, and any sensitive data should be followed.
- All data from the UAS and any removable storage devices should be erased after each use.

4 UAS Testing and Approval Process

Before conducting operations which involve the use of a UAS for GSA related projects, UAS operator must use an already approved device (as identified in the GSA Enterprise Architecture [EA] Analytics and Reporting (GEAR) IT Standards List) or submit a request to the IT Standards Team to have the device evaluated prior to it being used for GSA purposes. Further, the UAS operator must register the device and must annually recertify for continued use. Any request for the use of UAS must be submitted through the normal IT Standards processes.

4.1 Requesting Unapproved UAS

For new devices not already approved in GEAR, the following information must be included in the IT Standards request:

- UAS Manufacturer Name
- UAS Manufacturer Location (Country)
- Model Number

The OCISO is responsible for conducting the security portion of the review as part of the IT Standards process. This review will use a risk-based approach, as identified in CIO-IT Security-16-72, and will include additional testing for devices identified as high-risk that are detailed in an internal Standard Operating Procedures.

4.2 Approving and Recertifying UAS Operators

In addition to using an approved device, UAS operators must be approved and annually recertified with GSA using the Drone – UAS Operator Approval/Recertification Form which requires the following information:

- Name of Operator.
- UAS Operating Organization.
- Manufacturer, Model, and Serial number of the UAS device.
- Confirmation that the drone is registered with the FAA in accordance with regulations, including FAA registration number (as applicable).
- Assertion that the operator has obtained from the FAA a Remote Drone Pilot Certification.
- Assertion that operators will securely operate their UAS device in accordance with Section 2 of this guide, including ensuring that mobile applications and firmware are up to date.
- Privacy Threshold assessment as described in Section 3.3.