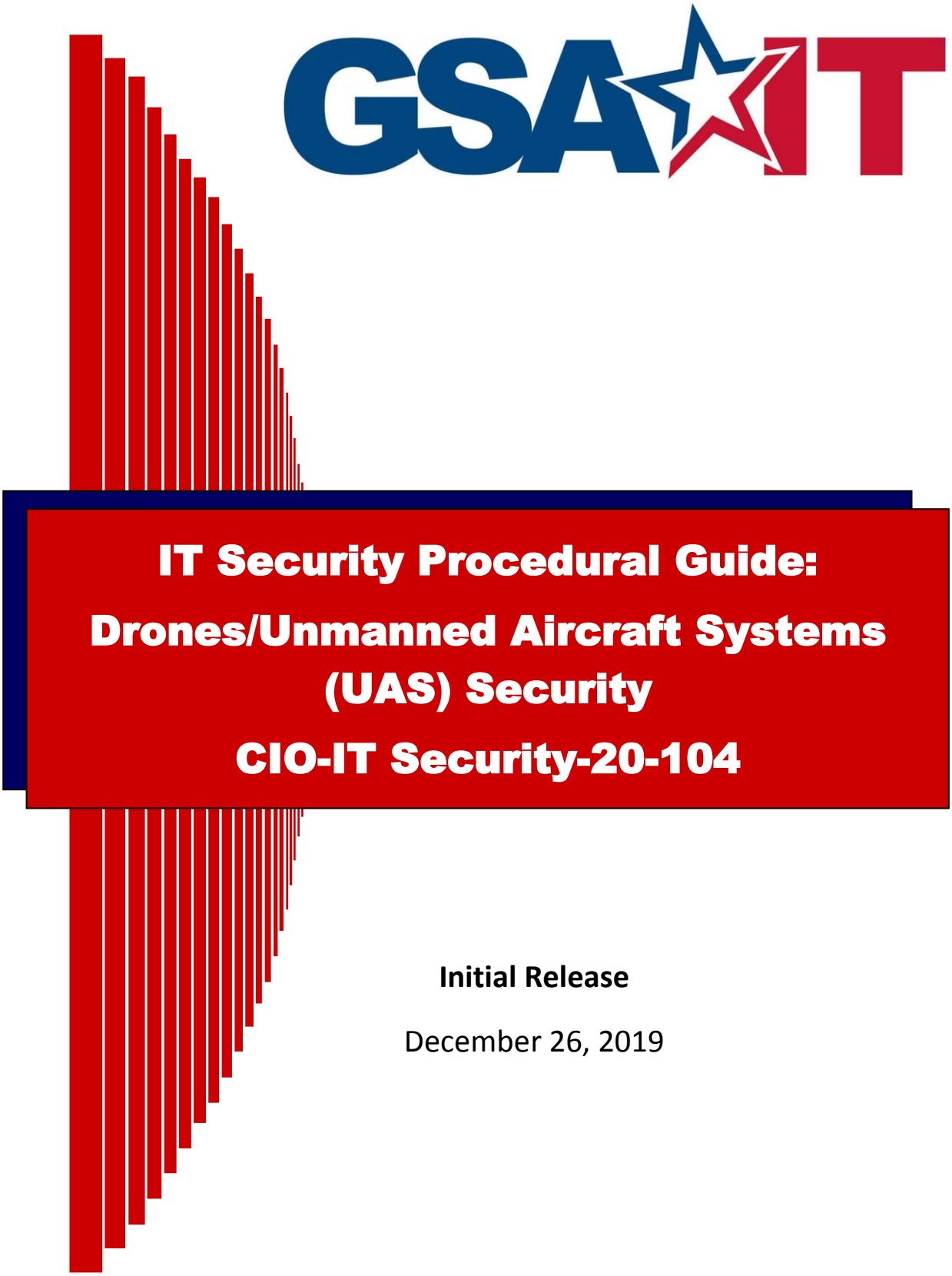

IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security CIO-IT Security-20-104

Initial Release

December 26, 2019

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

Approval

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

X DocuSigned by:
Bo Berlas
FD71792616 1344F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE) at SecEng@gsa.gov.

Table of Contents

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

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 General Services Administration (GSA) users or contractors on behalf of GSA. As determined by the Federal Aviation Administration (FAA), a UAS meets the definition of an aircraft - "any contrivance invented, used, or designed to navigate or fly in the air." At GSA this would include any unmanned aircraft purchased by GSA or on behalf of GSA for any business purpose. This includes those used for surveillance of buildings or aerial photography/video capture. GSA users or contractors on behalf of GSA are to conform to requirements and operating rules as specified in the FAA's UAS rule (known as "part 107"). Drones that are larger than the weight limit are not allowed at GSA.

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

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

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

In order to achieve the GSA's mission, and to meet the GSA's customer 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 purchase and subsequent use by GSA. 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 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 a UAS for business use should consider the following prior to purchase:

- Purchase UAS devices and components from reputable vendors.
- Understand how and where your UAS data is being stored.
- Determine how your UAS will interact with infrastructure and networks.

2.1 Purchase UAS Devices and Components from Reputable Vendors

Do your research and ensure that the vendor from whom you plan to purchase your device and its components is trustworthy. Considerations should include the country that the manufacturer is from.

Note that GSA will not approve any drone produced by or containing substantial or critical components from a prohibited source, as maintained on the Prohibited Sources and Supply Chain Risk Management (SCRM) InSite page, that includes the following as of November 2019:

- Dahua Technology Company
- Hangzhou Hikvision Digital Technology
- Huawei
- HyTera
- ZTE
- 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 a UAS if the cybersecurity, privacy, or supply chain risk is assessed to be unacceptable.

2.2 Understand How and Where Your UAS Data is Being Stored

Be aware of whether your UAS data is being stored by the vendor or other third parties. If it is being stored, find out how, where, and for how long. UAS device approvals will be limited to local storage or already authorized platforms (e.g., GSA's Google Drive instance).

2.3 Determine How Your UAS Will Interact with Infrastructure and Networks

To avoid compromising sensitive or controlled information, be sure to understand how to properly operate and limit your device's access to networks in order to avoid unnecessary

exposure of data to external threats. There are proactive steps that can be taken to deactivate vulnerable features of UAS that are detailed in Section 3.

3 General UAS Security

Although UASs 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 UASs 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 drones security best practices and consideration for securing like devices.

3.1 Installation and Use of UAS Software and Firmware

When employing UASs within an organization, an operator should use the following best practices related to the 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. 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.
    - 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 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; go through each screen manually to understand what options are being selected.
    - 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 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 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 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.
- 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.

3.3 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. 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:
  - 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 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 UASs with access to private or confidential data. Use Multi-Factor Authentication (MFA) whenever possible for accounts associated with UAS operations.
- 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.

4 UAS Testing and Approval Process

Before conducting operations which involve the use of a UAS for GSA related projects, the 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 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 Request for Unapproved UAS

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

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

The OCISO Security Engineering Division (ISE) will be 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 Procedure.

4.2 UAS Operator Approval and Recertification

In addition to using an approved device, UAS operators must be approved and annually recertified with GSA using this Google Form, which will require the following information:

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