







Chinese Manufactured Unmanned Aircraft Systems

INDUSTRY ALERT

As commercial unmanned aircraft systems (UAS) sales in the United States rapidly rise and their capabilities evolve, organizations are beginning to strongly consider integrating the technology into security and safety operations. UAS can serve as a beneficial tool for businesses, providing a reliable, effective, cost-saving way to reduce risk to employees, improve operational efficiency, and increase situational awareness. Many organizations have already started to leverage versatile UAS in a number of ways:

-  **Security** – Identify security gaps and vulnerabilities. They are also being used as a response alternative, assisting in searching difficult to reach areas, and performing advance functions to identify potential issues before a security team arrives at a location.
-  **Surveying** – Survey large plots of land in a fraction of the time, and capture more detailed information about the current state of an area.
-  **Monitoring** – Monitor and secure remote areas, incorporating a mechanism for quick response to places that are time consuming or difficult to reach on the ground.
-  **Inspection** – Conduct site inspections, often times cutting back on costs, and improving efficiency.

Although UAS can provide various benefits, U.S. intelligence and security officials have repeatedly warned about the cyber and data security risks associated with information or communications technologies designed, manufactured, or sold by commercial enterprises operating under the control or influence of a foreign authoritarian state. While the risk of compromise is inherent in any technology that generates or collects sensitive data or otherwise has access to critical systems, the risk increases dramatically where the technology is made or sold by a company that could be persuaded or compelled to access that data or abuse that access on behalf of a foreign government that does not share our Constitutional norms and values, including meaningful and independent judicial review. The United States government has strong concerns about any technology product that takes American data into the territory of an authoritarian state that permits its intelligence services to have unfettered access to that data or otherwise abuses that access. Those concerns apply with equal force to certain Chinese-made UAS-connected devices capable of collecting and transferring potentially revealing data about their operations and the individuals and entities operating them, as China imposes unusually stringent obligations on its citizens to support national intelligence activities. Security professionals should mitigate these risks in the same manner that they would any other connected technology.

Potential Risk To An Organization's Information

With technology evolving, the convergence of physical and cyber threats is becoming more prominent. Organizations need to be aware of the various risks that UAS present to their information. As with all connected devices, the protection of sensitive information or intellectual property remains a top priority and significant challenge. Organizations that conduct operations impacting national security or the Nation's critical functions must remain especially vigilant as they may be at greater risk of espionage and theft of proprietary information.

Chinese Manufactured UAS can expose your organization's information through the following:



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

Organization's information is at risk if employing technology that has been corrupted by malware, or contain automatic data transmission back to a third party. Manufacturers and vendors can build in malware or collect data from your UAS device without your knowledge.

Data Theft

Organizations are susceptible to theft of information if the UAS device and your organization's network are not properly secured, and if the communication feed that the UAS is operating on is unencrypted.

Network Intrusion

UAS can expose organizations to network breaches, which could lead to unauthorized access to data sets and other information.



How Organizations Can Reduce Risk

UAS threats to information affect organizations of all sizes, and require the collective attention and involvement of all levels of an organization, from employees to executives. To help their companies address risks posed by UAS, it is imperative that these individuals work together to identify comprehensive risk mitigation solutions that inform necessary security protocols and procedures.

Before incorporating UAS into your organization, consider the following:

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. Be cautious when purchasing UAS technology from Chinese manufacturers as they can contain components that can compromise your data and share your information on a server accessed beyond the company itself.

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.

Determine how your UAS will interact with infrastructure and networks

To avoid compromising proprietary 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.

Perform a risk assessment

Risk assessments should be performed to identify physical and cyber threats to your organization's information. Assessments can inform how to appropriately incorporate UAS into security and safety operations while reducing the risks of data compromise to market competitors or malicious actors. Protective and response strategies should be incorporated into emergency action plans.

Implement a layered security approach

Develop policies, strategies, and plans that collectively address the UAS device, its components, the operator, and your organization's physical and cyber infrastructure.

Potential Mitigating Measures for Chinese Manufactured UAS



Deactivate internet connection from device used to operate the UAS.



Take precautionary steps prior to installing updated software or firmware.



Remove secure digital card from the main flight controller/aircraft.



If SD card is required to fly the aircraft, remove all data from the card after every flight.

For more information please visit
www.dhs.gov/cisa/uas-critical-infrastructure.