Risk Assessment

Detailed Report and Mitigation Plan

Updated with Additional Testing and Analysis

Executive Summary

Updated March 2020

Disclaimer and Use Restrictions

This Report was developed by Booz Allen Hamilton Inc. ("Booz Allen") exclusively for its client, PrecisionHawk, Inc. ("Client") specifically for Client's internal purposes and Client's interactions with certain United States Federal Government departments and agencies (each, along with any other third party(ies), a "Third Party"), and for no other purpose. Client acknowledges and agrees that this Report may only be distributed in its complete and original version, and may not be revised, nor may portions of this Report be distributed, disclosed or made a part of other documents. No Third Party may use, distribute, publicly quote or republish this Report, in whole in part, without the express written consent of Client and Booz Allen, prior to each instance of use and/or distribution, to be granted in Client's and Booz Allen's separate and sole discretion. Each Third Party hereby acknowledges and agrees that it is not entitled to rely on this Report for any reason whatsoever and that it would be unreasonable to do so. In addition, it is acknowledged and agreed by Client and any Third Party accessing this Report that the Report addresses the specific assessment criteria delineated in the Report only and is not intended to be comprehensive or address any other criteria not specifically identified herein. Further, it is acknowledged and agreed that Booz Allen does not provide, and is not qualified to provide, definitive opinions regarding legal, tax, accounting or compliance issues, even if these areas are tangential to the assessment performed by Booz Allen. To the maximum extent provided under applicable law, each Third Party hereby waives any and all claims and causes of action against Booz Allen arising out of or in any way related to Third Party's access and/or use of this Report. Except as expressly stated herein or pursuant to Booz Allen's separate services agreement with Client, Booz Allen makes no, and hereby expressly disclaims, all warranties, whether express or implied, with respect to this Report, including any warranty of merchantability, reliance, sufficiency, completeness, or fitness for a particular purpose.

Prepared exclusively for PrecisionHawk, Inc.

PRECISIONHAWK

Booz | Allen | Hamilton

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

EXECUTIVE SUMMARY

Background

As the U.S. government increasingly strives to stand up programs designed to leverage technology innovation in support of the warfighters and citizens of this Nation, government agencies continue to acknowledge the advantage of using small unmanned aircraft systems (UAS) in a variety of situations, from emergency disaster response to infrastructure inspection. As the demand for UAS support continues to grow within the government, proponents of this new technology have faced numerous challenges related to the perceived security of these devices. PrecisionHawk and Booz Allen Hamilton recognized the need for a cost-effective and efficient solution for validating new firmware, software, and application updates to provide government agencies a methodology to assess the security risks associated with current and future UAS procurement and services. The Unmanned Aircraft Systems Technology Center of Excellence (UAS COE), was developed so best in class industry leaders and partners can better assist government clients to conduct risk assessments, identify vulnerabilities, and develop tailored mitigation strategies to elevate the government's confidence in safely leveraging UAS technology without imposing undue mission risks.

Objective

PrecisionHawk collaborated with Booz Allen, an industry leader in cybersecurity, to conduct pilot risk assessments with the objective of documenting and reporting a timely and cost-effective methodology for cyber risk assessments and providing accurate and detailed results of findings. These tests are a critical first step that will create a framework for testing and validating UAS security. The framework established by the UAS COE with these initial security risk assessments will define the strategic foundation for the needed, more tailored work to be done in partnership with government clients. As such, these tests were focused on ports of entry and attack vectors, specifically targeting interface points of data to and from UAS and areas for potential transfer of data. Comprehensive preliminary testing was conducted to identify gaps for further testing. The details on the processes, tools, and further mitigation strategies developed during this testing were collected in a full report. This Executive Summary provides a brief synopsis of the results of this testing.

To demonstrate the effectiveness of the cyber assessment framework, the UAS COE chose to assess three specific drone models manufactured by SZ DJI Technology Co., Ltd (DJI), a Chinese manufacturer. Two of the three platforms tested were government edition (GE) models configured and designed for U.S. government agency use. The third platform, while not configured for use by government agencies, was chosen because it is sought after by some government agencies for its dual sensor capability and was additionally used as a baseline for comparison with the GE models. These specific models, the DJI Matrice 600 GE; DJI Mavic Pro GE; and DJI Mavic 2 Pro Enterprise, were selected for this assessment due to the prevalence of DJI technology in this market space (estimated at 76.8% market share in 2019), the current geo-political climate between the United States and China, and the prior assessments conducted on these models, particularly a 2019 assessment conducted by the Department of the Interior (DOI).

Testing Framework and Limitations

The testing for this evaluation was intended to be streamlined, using widely-available commercial-off-the-shelf products and tools, and focused on accomplishing a number of preliminary tests in a brief period of time to identify areas of interest for potential further testing. Analysis conducted under this framework should not be considered a comprehensive analysis

of all cybersecurity risks for any platform. No customized exploits, such as reverse engineering, were created for this evaluation.

PrecisionHawk coordinated the acquisition of the UAS platforms from DJI, whereby the platforms were delivered directly to the Booz Allen testing facility in Lexington Park, MD. Due to the specialized GE platforms, which are not publicly available for purchase, the UAS platforms were acquired from, and sent by, PrecisionHawk and DJI. The assessment findings and results were limited to the specific drones received. This limitation is unique due to the fact that the vehicles were acquired from the manufacturer for purposes of testing as opposed to purchasing random commercially available off-the-shelf units. When conducting a rapid cyber assessment on owned or a recently purchased fleet of UAS, testing two randomly selected vehicles for each platform model would suffice, one as a primary testing source and one as back-up and validation

Testing

Booz Allen's team of cyber security experts performed a number of tests associated with penetration testing, also known as ethical hacking, where cybersecurity experts attempt to compromise an asset to provide an assessment of its vulnerabilities. For this assessment, penetration testing was intentional, purposeful testing designed to simulate the potential vectors a hacker would employ to breach an asset or system. Penetration testing of the systems includes network and IP enumeration, radio frequency (RF) analysis and USB analysis tests.

a. Network and IP enumeration is a set of testing procedures that includes the tools and analysis performed on the network components. These tools are used as a method for network discovery and are used to determine the logical network communications for all the system devices.
b. The RF enumeration testing is used to validate the claims by the original equipment manufacturer of advertised RF emissions. It is used to verify Federal Communications Commission (FCC) compliance and to ensure that the device is not emitting any foreign or unknown RF signals.
c. The intent behind USB testing is to identify how the drone, tablet, and controller utilize the prevalent USB interfaces. The goals were to discover overlooked or misused attack surfaces and possible entry points.

These penetration tests simulated cyber-attacks and testing in a phased approach. The initial phase entailed planning and reconnaissance to define the test scope and gather network information to understand how an asset works and its potential vulnerabilities. Then, scanning tools were used to understand realistic threats and identify vulnerabilities that might allow for those attacks.

In February 2020, software updates were provided for additional analysis. The software updates only affected the network and IP enumeration analysis, and initial testing found that this analysis and their results are dependent on the software application and are independent of the specific drone. Therefore, the network analysis and IP enumeration was retested on the second M600 GE drone with the updated software.

Results

Government agencies have specific standards and expectations of how systems, technology, and data should be handled. Assuming that end users would be government agencies, the cyber team identified 13 vulnerabilities associated with one or more of the three platforms tested. It is generally assumed in cyber security testing that vulnerabilities will exist to some degree regardless of the UAS platform. For the purposes of this analysis and report, the term

vulnerability is defined in accordance with industry standards as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. The results of research and testing for each of the following vulnerabilities indicated a deviation from expectations and standards set forth by government agencies.

The table below provides an overview of the 13 identified vulnerabilities, relevant the phase of testing, the systems impacted by that vulnerability in initial testing, and whether that vulnerability was identified in the retesting of the Matrice 600 GE. The table also indicates those vulnerabilities requiring physical access to the drone and/or controller for the vulnerability to be present.

Of primary concern are potential vulnerabilities relating to unauthorized access to data (such as imagery or flight telemetry) via network pathways. By the conclusion of testing, only two vulnerabilities associated with Network & IP Enumeration were found. The first was momentary detection of two GE drones on commercial applications (#7), and the second involved connections by the three drones to network sources when the "Allow Map Services" feature is enabled by the user (#8). In the case of Map Services, our testing of the latest version of software (DJI Pilot 1.6.2pe and 1.3.2pe) indicated connections to IP addresses registered in within the U.S. (AWS, Google and McAfee) and Germany (Akamai). Any drone that provides the feature of externally-sourced map services would be expected to make such connections and to present similar vulnerabilities. Each of these two network & IP vulnerabilities have procedural mitigations, such as to not install or use the commercial applications, or to check settings and confirm that Allow Map Services is turned off before each flight. All remaining discovered vulnerabilities require either physical access to the drone, or (in the case of #6) for the attacker to be located within radio range of the drone's radio signal during its operation. It is very difficult to verify custodianship of any data when using cloud based services; however, our limited testing of the latest versions of the software for the three drone products, showed no evidence of connections to China or to DJI.

Summary of Vulnerabilities

#	Vulnerability	Requires Physical Access	Initial Testing			Retest
			Matrice 600 GE	Mavic Pro GE	Mavic 2 Enterprise	Matrice 600 GE
Reconnaissance Phase of Penetration Testing						
1	**Passcode/Authentication capability features are not implemented on the GE versions.**	✓	✓	✓	-	**N/A**
There is no authentication required to fly the Matrice 600 GE or the Mavic Pro GE drones. There are several points where this vulnerability exists and where an authentication feature could be implemented to provide additional layers of protection. Authentication features should be implemented to use and fly the drone, for firmware updates, when a connection is made between PC and DJI Assistant application, or when a connection is made between DJI Assistant application and the drone. This vulnerability can be mitigated by a software strategy of adding an authentication capability, as detailed in the full report.						
2	**Passcode capability did not restrict operators from accessing flight data.**	✓	-	-	✓	**N/A**
The passcode/authentication capability on the Mavic 2 Enterprise did not prevent operators from accessing flight data. It is worth noting that when the flight data was accessed, it was encrypted. This is still considered a potential vulnerability because flight logs collect a significant amount of data. If the drone was to land or lose battery power out of the flight zone and/or is captured, the flight log data could be accessed and potentially unencrypted. Attempts to unencrypt the data were outside the scope of this testing. This vulnerability can be mitigated by a software strategy of adding and authentication requirement and encryption, as detailed in the full report.						

#	Vulnerability	Requires Physical Access	Initial Testing			Retest
			Matrice 600 GE	Mavic Pro GE	Mavic 2 Enterprise	Matrice 600 GE
3	**No remote sanitization/zeroization exists on the drones.**	✓	✓	✓	✓	N/A
	Currently, there is no way to remotely remove all data collected on the drone. This is identified as a potential vulnerability because if the drone was to land or lose battery power out of the flight zone and/or is captured, there is no mechanism in place to remotely remove the data on the drone. This vulnerability can be mitigated by software and hardware strategies involving the addition of data sanitization capabilities, as detailed in the full report.					
4	**No data-at-rest (DAR) encryption on the SD cards to securely protect contents.**	✓	✓	✓	✓	N/A
	Currently, there is no DAR encryption function to protect data from unauthorized view. Exploitation of this potential vulnerability requires access to the SD card physically inside the drone. However, this is identified as a potential vulnerability because if the drone was to land or lose battery power out of the flight zone and/or is captured, the SD card is easily accessible. The data is vulnerable because there is no prevention mechanism to stop someone from accessing and reading it. Additionally, data remanence on SD cards could provide aggregation of historic flight data. The lack of encryption would allow users the ability to retrieve this data. This vulnerability can be mitigated by software and procedural strategies involving the addition of authentication and encryption capabilities and processes, as detailed in the full report.					
5	**The internal storage modules are likely solid state or flash store modules (similar to SD cards) with possible attack vectors to retrieve data off these modules.**	✓	✓	✓	✓	N/A
	Based on tester knowledge of these devices, it is assumed internal storage modules are similar to, and act like, SD cards and, therefore, have the same weaknesses as SD cards. For example, other DJI drone models, such as the Phantom, use this type of internal storage device. Testers could not verify this assumption without deconstructing the devices; however, it is believed there are still attack vectors to retrieve data off these modules. Further discussion with the manufacturer is needed on where firmware updates are stored. This vulnerability can be mitigated by software and hardware strategies involving data sanitization, encryption, and erasure, as detailed in the full report.					
6	**Lightbridge uses Triple DES encryption. AES encryption is recommended, and AES-256 encrypted link is currently the highest government standard.**	-	✓	✓	-	N/A
	Manufacturer documentation indicates that only the Ocusync 2.0 link, deployed on the Mavic 2 Enterprise, utilizes AES-256 encryption to secure the datalink. AES-256 is currently recognized as an approved encryption format for transmission of information protected at some of the highest levels by the U.S. government and, therefore, often required for certain U.S. government applications. While the AES-256 algorithm itself is considered approved, it should be noted that the implementation of the cryptographic module providing the AES-256 algorithm used by DJI has not been approved by National Institute of Standards and Technology (NIST) for U.S. Government use.[1,2] There is no literature openly available that identifies the encryption standard of the Lightbridge (Matrice 600 GE) or Ocusync 1.0 (Mavic Pro GE) video transmission and control link. The manufacturer, however, notified the cyber assessment team that the encryption on Lightbridge's up control link uses Triple DES and the video transmission and down control link are not supported. Triple DES encryption is not a recommended					

[1] https://csrc.nist.gov/Projects/cryptographic-module-validation-program
[2] https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search

#	Vulnerability	Requires Physical Access	Initial Testing			Retest
			Matrice 600 GE	Mavic Pro GE	Mavic 2 Enterprise	Matrice 600 GE

encryption method for government applications. Additionally, since the video link is not encrypted, this provides a limited window attack vector during video transmission.

The cyber assessment team was also notified that the Ocusync 1.0 uses AES-128 control link (uplink and downlink) and the video transmission is not supported. AES-128 is an approved encryption method but the implementation of the embedded cryptographic module toolkit that encrypts the datalink has not been validated as conforming to Federal Information Processing Standard (FIPS) 140-2, and is, therefore, considered vulnerable to attack. FIPS 140-2 and Committee for National Security Systems Policy No. 15 and 28 mandate the minimum encryption standards for securing data streams. As with the Lightbridge, the video link is not encrypted, providing a limited window attack vector during video transmission. Due to the limited scope of this analysis, no testing was performed on these datalinks to determine overall security posture.

This vulnerability requires an attacker to be located within radio range of the drone's radio signal during its operation. In addition to indicated software mitigations to update the data link encryption, a procedural mitigation would include the implementation of physical security steps to limit persons who are within radio range of the drone during operation.

	Network & IP Enumeration Phase					
7	**GE model drones are momentarily detected on the commercial applications on tablet devices.**	✓	✓	✓	-	✓

The GE models were able to connect to the commercial application. This connection seemed to be fully operational for a few seconds before it disconnected. While there is a mechanism in place that identifies when the connection is made and kicks out the unauthorized user, this connection is identified as a potential vulnerability. These few seconds of connection provide a possible avenue of attack. If there was any staged payload or malicious content on the tablet, it could communicate with the drone and possibly access data in an unintended way. Additionally, if the same authentication sequence allows the drone to exchange communication for both the commercial and the GE tool, then it exposes the GE version to more attacks. This suggests that attacks that work on the commercial applications could possibly work on the GE drones. Specific testing for this element did not occur and further testing was recommended.

During retesting it was found that the Matrice 600 GE could now fully connect to both the upgraded software version (1.3.2pe and 1.6.2pe). The original vulnerability was noted due to the default connections the original privacy software made (1.6.1pe). Since both upgraded software versions present themselves as privacy editions and no longer establish as many connections, this vulnerability is partially mitigated.

This vulnerability can be further mitigated by software strategies involving authentication, as detailed in the full report and can be further mitigated procedurally by users by implementing procedures that avoids installing or using the commercial applications.

8	**GE model drone was able to connect to commercial server for firmware update.**	-	✓	-	-	-

During initial testing the Matrice 600 GE systems registered, and connected to, the commercial Assistant 2 software and was permitted to execute a firmware update without any restrictions. This resulted in one of the tested drones receiving a non-GE edition firmware build. A network capture verified the drone retrieved the firmware from an external source over the Internet and additional network connections were made during this update. As noted in vulnerability #7, the ability to connect and initiate a firmware upgrade provides a possible avenue of attack.

During retesting of the second Matrice 600 GE, results indicated that the systems no longer registered and connected to the commercial Assistant software, and therefore is no longer considered a vulnerability.

#	Vulnerability	Requires Physical Access	Initial Testing			Retest
			Matrice 600 GE	Mavic Pro GE	Mavic 2 Enterprise	Matrice 600 GE
9	**With "Allow Map Services" enabled, both DJI Pilot 1.3.2pe and DJI Pilot 1.6.2pe applications communicate location data and IP address information to outside network sources**	-	✓	✓	✓	✓

Currently, when "Allow Map Services" is enabled in both DJI Pilot 1.3.2pe and DJI Pilot 1.6.2pe applications, network connections are made to outside sources. Connections are to IP addresses registered to locations within the U.S. with the exceptions of pings to Adjust GmbH out of Thuringia, Germany. These connections make location and IP address data available to those outside sources. Any additional data sent is encrypted using HTTPS, so the additional data that is being communicated was not determined at this time; however, there is the assumption that location data is shared as the populated maps are associated with GPS position. Further testing could unencrypt the data and reveal what information is being sent. Data may be innocuous, but the mere fact that these are not closed systems presents a potential vulnerability. This vulnerability can be mitigated by software strategies involving removing the software, establishing firewalls, and user-selected permissions, and also may be mitigated procedurally by users by going into settings and confirming that Allow Map Services is turned off before each flight.

	USB Analysis Phase					
10	**USB debugging mode may be possible via the multimode USB connection from the drones.**	✓	✓	✓	✓	**N/A**

The drones run a small Linux operating system and when connected to a USB it is potentially possible to send a signal to a USB connection that could allow for full control of the device. Debugging mode is often used by developers to gain access to functions usually restricted. Additionally, the multimode connection exposes the network addresses and serial connection. The testers did not attempt to take control of the device due to the scope of penetration testing. Research into the nature of the device in multimode connection indicated a potential avenue for attack. This vulnerability can be mitigated by software strategies involving control of the USB device or removal of the debugging capability, as detailed in the full report.

11	**USB multimode connection from the drone exposes a PC or tablet to new attack vectors such as serial, mass storage device, and ethernet over USB.**	-	✓	✓	✓	**N/A**

When the drone is connected to a PC through the USB connection, it behaves as multiple devices, which has two primary implications. First, this can allow for an attack vector from the drone to the PC or tablet; if there is something malicious on the drone, it can expose the PC or tablet to attacks from the drone. Second, the drone can pull data from a locked PC or tablet by having the USB device imitate an ethernet device. Additionally, this multimode connection exposes both the PC and tablet to attacks common with serial and ethernet over USB. It presents attack vectors because when the drone is plugged in it communicates to the computer and a new port is connected. When this occurs, the firewall rules and policies are not yet set for the new device and a default, low security, setting occurs, presenting attack surfaces. No attacks were observed, but an attack surface exists. More analysis is would be required to understand what attack surfaces exist. This vulnerability can be further mitigated by software strategies involving evaluation and control of communication channels and connections, as detailed in the full report.

#	Vulnerability	Requires Physical Access	Initial Testing			Retest
			Matrice 600 GE	Mavic Pro GE	Mavic 2 Enterprise	Matrice 600 GE
12	**File Transfer Protocol service found on the Remote Network Driver Interface Specification network, 192.168.43.0/24, when USB cable was connected to drone.**	-	-	✓	✓	N/A

FTP is designed to accommodate upload and download of files and data between devices over TCP/IP. It is common to have anonymous access on FTP servers, allowing unauthenticated users the ability to access the contents of file systems and media stored on the hosting device. FTP services is known to be a common attack vector. In many cases, anonymous access is also used to facilitate upload of data, including configuration files, software upgrades, or miscellaneous files. FTP service was detected was during the time that the USB cable was connected to the drone, but further testing is recommended to verify that exposure to this service is limited to that timeframe only. Due to the scope of penetration testing, no attempts to gain access to the FTP service occurred. The assumptions of the test team was that this FTP service existed as part of a maintenance or automated system feature used by the DJI Assistant applications. It is recommended that further testing be conducted to verify proper configuration and security controls on FTP accessible files. An adversary with malicious intent could potentially utilize this service to exfiltrate data, manipulate configuration, or upload custom software. This vulnerability can be mitigated by software and procedural strategies involving FTP permissions and authentication, as detailed in the full report.

13	**192.168.4x.0/24 network discovered, and function or purpose is unclear.**	-	-	✓	✓	N/A

Additional network interfaces, even ones created by USB connections, pose entry points to access services and settings on the hosting system. Network traffic was observed using 192.168.4x.0/24 addresses, and although the intent or purpose of this traffic was not determined, it is likely that it is used for some controlling or back-end system. This exposes an attack surface. The network address starting with 192.186 is a local network that exists between drone and devices. These local networks usually have limited firewall restrictions considered a trusted environment and usually allows for significant communications. Currently, securities on the network are unknown and additional enumeration and fingerprinting is recommended to expose insecure services or devices using this connection. Firewall settings are often configured for specific networks and do not universally extend to all network adapters, even on the same machine. Therefore, a properly configured firewall may only be blocking a specific interface and that the creation of a new interface may bypass the security rules protecting inbound and outbound communications. This vulnerability can be further mitigated by software strategies involving evaluation and monitoring of necessary communication channels, as detailed in the full report.

Mitigations

As vulnerabilities were identified, our cyber team of experts developed mitigation strategies grouped into three potential areas for consideration: (1) software changes (changes in the UAS programming, for example, that would add password or encryption for data protection), (2) hardware changes (such as adding hardware components to erase data if unauthorized access occurs), or (3) procedural changes (by mandating steps in flight procedures that disable or avoid certain features on the platform). Software and hardware changes are the preferred strategy; however, given current manufacturing and technological limitations, not all software or hardware mitigations are feasible. Therefore, operators should consider implementing procedural mitigation strategies as an initial step and discuss the feasibility of additional software and/or hardware mitigation strategies with the manufacturer, if applicable. Mitigation strategies for each vulnerability were summarized in the previous section; details for these strategies are provided in the associated full report. By implementing these mitigation strategies in the UAS or its systems, the potential risks presented by the vulnerabilities could be reduced and therefore boost the government's confidence in using these specific UAS platforms.

Risks

Using the vulnerabilities and potential mitigations identified for the three UAS platforms, our cyber team conducted a risk analysis to assign risk scores of the identified vulnerabilities within the context of two use cases relevant to current private and public sector UAS practice: Emergency Response and Infrastructure Management. UAS are frequently employed in emergency response preemptively, for real time and post-emergency purposes (e.g., flood, wildfire, and other sever climate events). Using imagery and video from a UAS, first responders can plan their mission more thoroughly on the scene while keeping teams out of harm's way, whether in urban or remote settings. The use of UAS to inspect existing infrastructure can be more cost-effective, faster, repeatable, and safer. This rapid data gathering provides the basis for improved strategic decision making for projects related to infrastructure management.

To perform the analysis, risks were first defined based on the identified vulnerabilities, the potential risk created by those vulnerabilities, and their relevance to one of the three fundamental cybersecurity tenets: (1) Confidentiality (ensure access to data is given to only those people and processes that need it to complete their duties), (2) Availability (ensure information is readily accessible to all authorized users at all times), and (3) Integrity (ensure the reliability and accuracy of the information is maintained at all times). Additionally, the team identified the three areas directly impacted by the risks: the data collected, the air vehicle's (AV) hardware or software, and the completion of the mission.

The table below defines each identified risk and displays the associated affected cybersecurity tenet(s), risk impact, and vulnerabilities.

Summary of Risk Areas

#	RISK	AFFECTED CYBERSECURITY TENET	RISK IMPACT	ASSOCIATED VULNERABILITIES
1	**Data Exposure:** Exposure to sensitive location data and flight data to remote sources.	Confidentiality	Data	7, 8, 9
2	**Unauthorized Access:** Localized unauthorized access to drone and data.	Confidentiality & Availability	Data	1, 2, 3, 4, 5, 10, 11
3	**Data Corruption:** Corruption or manipulation on drone data (Malware)	Integrity	AV	11, 12, 13
4	**Datalink Exposure:** Eavesdropping or manipulating drone's datalink	Integrity & Availability	Data & Mission	6
5	**Remote Access:** Remote access to drone network for takeover or eavesdropping.	Confidentiality, Integrity, & Availability	Data, Mission, & AV	7, 8, 9, 12, 13

The cyber team then assigned scores to each risk area based on specifications from the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1: Guide for Conducting Risk Assessments.* The following table displays how each risk was scored for both use cases, with and without mitigations. The presented risks on both use cases are moderate to low without mitigations in place. Once mitigations are applied, both use cases decrease their risk scores.

Summary of Risk Assessment Scores

#	RISK	USE CASE 1 RISK SCORE		USE CASE 2 RISK SCORE	
		Without Mitigation	With Mitigation	Without Mitigation	With Mitigation
1	**Data Exposure:** Exposure to sensitive location data and flight data to remote sources.	Moderate	Low	Moderate	Moderate
2	**Unauthorized Access:** Localized unauthorized access to drone and data.	Low	Low	Moderate	Low
3	**Data Corruption:** Corruption or manipulation on drone data (Malware)	Low	Very Low	Low	Low
4	**Datalink Exposure:** Eavesdropping or manipulating drone's datalink	Moderate	Low	Moderate	Low
5	**Remote Access:** Remote access to drone network for takeover or eavesdropping.	Moderate	Low	Moderate	Low

Conclusion

By applying this cyber assessment framework to three previously tested UAS platforms, the UAS COE team was able to quickly identify several areas of vulnerability that had not been addressed in previous rounds of assessment. Moreover, similar vulnerabilities are consistent on other platforms, and not specific to any individual manufacturer. By assessing a greater variety of UAS platforms, and quickly finding these vulnerabilities and quantitatively defining the associated risks, UAS users can respond by implementing powerful mitigation strategies that significantly reduce perceived risks associated with the UAS platforms. Furthermore, sharing these findings will help manufacturers fully understand the government's more stringent requirements and will enable them to build platforms that better meet the government's needs and requirements. Finding a secure and scalable way to empower the use of these inexpensive, yet powerful tools while concurrently ensuring data security and reliability is essential to the successful accomplishment of missions.

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.