



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**UNMANNED AERIAL SYSTEM CYBERSECURITY RISK
MANAGEMENT DECISION MATRIX FOR TACTICAL
OPERATORS**

by

Gary L. Lattimore

June 2019

Thesis Advisor:
Co-Advisor:

Raymond R. Buettner Jr.
Aurelio Monarrez Jr.

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2019	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE UNMANNED AERIAL SYSTEM CYBERSECURITY RISK MANAGEMENT DECISION MATRIX FOR TACTICAL OPERATORS		5. FUNDING NUMBERS R4M3G	
6. AUTHOR(S) Gary L. Lattimore			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) CRUSER, Monterey, CA 93943		10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The Department of Defense (DoD) does not have a defined cybersecurity operational risk management process for unmanned aerial systems (UASs). The DoD acknowledged this discrepancy and suspended all commercial-off-the-shelf (COTS) UASs on 23 May 2018. The suspension was followed by a rigid DoD COTS UAS waiver process effective 01 June 2018. COTS UASs are defined by the Deputy Secretary of Defense Memorandum using three different criteria: UASs sold in the same form to the public and government, those commercially available systems that have software and/or hardware modifications, and those with specific ground command and control elements, such as smart devices and tablets. Cybersecurity vulnerabilities can span the acquisition, strategic, operational, and tactical levels. This research focused on the tactical level. Tactical commanders often lack the tools to identify and mitigate UAS cybersecurity vulnerabilities. This effort leveraged the standards developed by the National Institute of Science and Technology drafted Federal Information Processing Standards and Special Publication 800 series to develop the proposed UAS Cybersecurity Risk Management Decision Matrix. The matrix can enable tactical commanders to conduct a cybersecurity risk determination for UAS operators. This mitigates risk and strengthens strategic and operational decisions. Furthermore, three recommendations for future work are offered which will improve the UAS cybersecurity processes within the DoD.			
14. SUBJECT TERMS UAS, unmanned aerial systems, cybersecurity		15. NUMBER OF PAGES 93	16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**UNMANNED AERIAL SYSTEM CYBERSECURITY RISK MANAGEMENT
DECISION MATRIX FOR TACTICAL OPERATORS**

Gary L. Lattimore
Lieutenant, United States Navy
BS, Trident University International, 2015

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
June 2019**

Approved by: Raymond R. Buettner Jr.
Advisor

Aurelio Monarrez Jr.
Co-Advisor

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Defense (DoD) does not have a defined cybersecurity operational risk management process for unmanned aerial systems (UASs). The DoD acknowledged this discrepancy and suspended all commercial-off-the-shelf (COTS) UASs on 23 May 2018. The suspension was followed by a rigid DoD COTS UAS waiver process effective 01 June 2018. COTS UASs are defined by the Deputy Secretary of Defense Memorandum using three different criteria: UASs sold in the same form to the public and government, those commercially available systems that have software and/or hardware modifications, and those with specific ground command and control elements, such as smart devices and tablets.

Cybersecurity vulnerabilities can span the acquisition, strategic, operational, and tactical levels. This research focused on the tactical level. Tactical commanders often lack the tools to identify and mitigate UAS cybersecurity vulnerabilities. This effort leveraged the standards developed by the National Institute of Science and Technology drafted Federal Information Processing Standards and Special Publication 800 series to develop the proposed UAS Cybersecurity Risk Management Decision Matrix. The matrix can enable tactical commanders to conduct a cybersecurity risk determination for UAS operators. This mitigates risk and strengthens strategic and operational decisions. Furthermore, three recommendations for future work are offered which will improve the UAS cybersecurity processes within the DoD.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	DEFINITION OF UAS.....	3
B.	PURPOSE OF STUDY.....	5
C.	APPROACH.....	6
D.	DESIRED END STATE	7
II.	UAS COMPONENTS, ATTACK SURFACE BACKGROUND, AND SUPPORTING STANDARDS.....	9
A.	UAS COMPONENTS.....	10
1.	Communications Systems.....	10
2.	Aircraft.....	13
3.	GCS	16
4.	Ground Support Equipment.....	17
5.	Software	18
6.	UAS Operators.....	18
B.	ATTACK SURFACE BACKGROUND	19
1.	Confidentiality Threats	20
2.	Integrity Threats	23
3.	Availability Threats	26
4.	FIPS 199	29
5.	FIPS 200.....	31
6.	NIST Special Publication 800–53	33
7.	NIST Special Publication 800–30	34
III.	APPLYING NIST AND FIPS SECURITY STANDARDS TO UAS	41
A.	CALCULATING UAS CYBERSECURITY RISK.....	42
B.	UAS CYBERSECURITY RISK MANAGEMENT DECISION MATRIX (CRMDM).....	47
1.	Threat Matrix.....	47
2.	Vulnerability and Security Control Matrix.....	49
3.	Impact Matrix	52
4.	Cybersecurity Risk Management Decision Matrix.....	53
IV.	CRMDM EXAMPLE AND ALTERNATIVE COURSE OF ACTION (COA) ASSESSMENT.....	57
A.	UAS CRMDM SCENARIO	57
B.	ALTERNATIVES TO THE UAS CRMDM.....	62

1.	Unrestricted Use of UAS without Cybersecurity	62
2.	Continue the Current Non-POR UAS Exemption Process	63
3.	Abandon DoD Use of Commercial or Non-POR UAS.....	66
V.	RECOMMENDATIONS AND FUTURE WORK	67
A.	RECOMMENDATIONS.....	67
B.	FUTURE WORK.....	68
	LIST OF REFERENCES.....	71
	INITIAL DISTRIBUTION LIST	75

LIST OF FIGURES

Figure 1.	Typical UAV Communications Scenario. Source: [11].	11
Figure 2.	ScanEagle® Size, Weight, Power, Performance, Sensor, and Data Information. Source: [14].	15
Figure 3.	ScanEagle® Unmanned Aircraft System (UAS). Source: [14].	17
Figure 4.	UAV System Cyber-Security Threat Model. Source: [11].	20
Figure 5.	UAS Confidentiality Threats. Source: [11].	21
Figure 6.	UAS Integrity Threats. Source: [11].	24
Figure 7.	UAS Availability Threats. Source: [11].	27
Figure 8.	Risk Assessment within the Risk Management Process. Source: [25].	35
Figure 9.	Relationship among Risk Framing Components. Source: [25].	36
Figure 10.	Generic Risk Model with Key Risk Factors. Source: [25].	37
Figure 11.	Risk Assessment Process. Source: [25].	39
Figure 12.	AOR Organization. Adapted from [29].	58
Figure 13.	Scenario UAS Cybersecurity Risk Management Decision Matrix Fly/No-Fly Scale.	61
Figure 14.	DoN Non-POR UAS Exemption Approval Process.	65

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	DoD UAS Group Descriptions. Source: [8].	4
Table 2.	Potential Impact Definitions for Security Objectives. Source: [22].	31
Table 3.	FIPS Security-Centric Areas Requiring CIA Protections. Source: [23].	32
Table 4.	Security Control Identifiers and Family Names. Source: [24].	33
Table 5.	Characteristics of Adversary Capability. Source: [25].	43
Table 6.	Range of Effects for Non-adversarial Threat Sources. Source: [25].	43
Table 7.	Vulnerability Severity. Source: [25].	45
Table 8.	Likelihood of Threat Event Resulting in Adverse Impacts. Source: [25].	45
Table 9.	Assessment Scale—Level of Risk. Source: [25].	46
Table 10.	UAS CRMDM Threat Scale. Adapted from [25].	49
Table 11.	UAS Vulnerability and Security Control Matrix. Adapted from [25].	51
Table 12.	UAS Impact Matrix. Adapted from [25].	53
Table 13.	UAS Cybersecurity Risk Management Decision Matrix. Adapted from [25].	54
Table 14.	Proposed UAS Cybersecurity Risk Management Decision Matrix Fly/No-Fly Scale.	56
Table 15.	Scenario Problem Framing. Adapted from [29].	59
Table 16.	Scenario Tactical UAS Drone-A CRMDM Results	60
Table 17.	Scenario Tactical UAS Drone-B CRMDM Results.	61

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BLOS	Beyond Line of Sight
C2	Command and Control
CIA	Confidentiality, Integrity, and Availability
COA	Course of Action
COTS	Commercial off the Shelf
CPS	Cyber Physical Systems
CRA	Cyber Risk Assessment
CRMDM	Cybersecurity Risk Management Decision Matrix
DASN RTD&E	Deputy Assistant Secretary of the Navy for Research, Testing, Development, and Evaluation
DDoS	Distributed Denial of Service
DIU	Defense Innovation Unit
DJI	Da-Jiang Innovations
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoN	Department of the Navy
DoS	Denial of Service
EMI	Electromagnetic Interference
EMW	Electromagnetic Warfare
EO	Electro-Optical
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Management Act
GCS	Ground Control System
GPS	Global Positioning System
IOT	Internet Of Things
IP	Internet Protocol
IS	Information System
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology

JFC	Joint Force Commander
JVAB	Joint Vulnerabilities Assessment Branch
LOS	Line of Sight
MAC	Media Access Control
MC	Mission Commander
NAVAIR	Naval Air Systems Command
NIST	National Institute of Science and Technology
NPS	Naval Postgraduate School
NRL	United States Naval Research Laboratory
NWB	Naval Waiver Board
OIC	Officer in Charge
OPNAV N9I	Office of the Chief of Naval Operations, Warfare Integration
OS	Operating System
OTH	Over the Horizon
POR	Program of Record
Q-VAR	Quick Look Vulnerability Assessment Report
RF	Radio Frequency
RFI	Radio Frequency Interference
RMF	Risk Management Framework
SATCOM	Satellite Communications
SC	Security Control
SCRAMS	Supply Chain Risk Analysis and Management System
SE	ScanEagle
SP	Special Publication
SPAWAR	Space and Naval Warfare Systems Command
TCP	Transport Control Protocol
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
USMC	United States Marine Corps

ACKNOWLEDGMENTS

A very special thank you to my wife, Kahori Lattimore, and the team, Julian, Lily, and Oliver, for their understanding and support through many days and nights of research. I appreciate the time and effort Dr. Raymond Buettner, Mr. Aurelio Monarrez, and Mr. John Fulp spent guiding me throughout my thesis process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In December 2011, a U.S. RQ-170 Sentinel was commandeered, while in flight, by an Iranian cyber warfare specialist [1]. The event proved that capable threats exist and adversaries are actively working to exploit critical vulnerabilities in U.S. unmanned systems. This is an example of an event that should not have happened and this thesis develops a core process that provides tactical units with the capability to incorporate cybersecurity risk assessments that should mitigate the risk from such attacks in the future. In the Department of Defense (DoD) the term “cybersecurity” is defined as a “prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation” [2]. Systematic UAS cybersecurity assessments that consider system confidentiality, integrity, and availability will provide the foundation for a tool that will minimize the likelihood of future incidents similar to the 2011 RQ-170 event and mitigate the consequences when such attacks are attempted.

Threats to cybersecurity are prevalent on a global scale and wreak havoc in many different domains. The Internet, including the myriad of all of the attached devices, is characterized by an unfortunate emphasis on functionality over security. That is, industry has prioritized being quick *to* market (functionality), over being the most secure *on* the market (security). Attacks on DoD UAS, like the 2011 RQ-170 incident or more recent 2018 Russian Global Positioning Sensor (GPS) jamming on smaller U.S. UAS in Syria, has demonstrated the need for stronger cybersecurity implementations on this world-wide network of networks [3].

Internet of Things (IoT) is a collective term that describes a class of networked, data-sharing, quasi-autonomous entities that are designed to share data with little or no human interaction [4]. Commercial-off-the-shelf (COTS) Unmanned aerial systems (UASs), known more commonly as drones, share similar communications technology and traits with other IoT devices. These systems' underlying technologies are often

implemented with design vulnerabilities that can be exploited by malicious actors. Such vulnerabilities can go unnoticed and undetected unless an adequate cybersecurity assessment is conducted.

The DoD has demonstrated confusion over the best course of action with regards to cybersecurity threats that can place our tactical operators and UASs at risk. On May 23, 2018, the DoD issued a memorandum grounding all DoD operated UASs, with the exception of individual waivers granted to select U.S. forces and educational institutions to continue UAS operations [5]. This action was directly related to discovered vulnerabilities with popular COTS UASs currently utilized in some DoD environments. However, another reason for the ban was the simple fact that not a single military service had (or as this is currently written, has) a clear policy for mitigating risk while employing COTS UASs. As a result, UAS operators are left unprepared with neither a systematic method to identify and mitigate system risks, nor the criteria necessary to provide tactical commanders with a translation to operational risks to mission. This thesis targets this critical issue with the goal of providing a viable approach for including cyber risk for the tactical commander.

The popularity and availability of COTS UASs have significantly increased in the public and military where they serve a wide variety of applications. One military application is intelligence, surveillance, and reconnaissance (ISR). UAS ISR is a principal DoD capability that is used to collect, process, and disseminate actionable information to decision makers at various command levels with using a wide-range of platforms and sensor payloads. United States military UAS utilization grew rapidly in the wake of the 9/11 terrorist attacks on the World Trade Center. The first documented military drone was launched in 1917, 14 years after the Wright Brothers' landmark Kitty Hawk flight [6]. The Ruston Proctor Aerial Target was called a drone but functioned as a pilotless military munition [6]. Since then, technology has significantly advanced and has become a common tool in military and civilian applications. The U.S. defense budget allotted \$6.05 billion in the FY 2019 DoD budget request for UAS acquisitions, which is an increase of \$5 billion in the FY 2018 and FY 2017 requests [7]. From the \$6.05 billion, \$3.71 billion was allocated for procurement of new vehicles, \$2.14 billion was set aside for research and


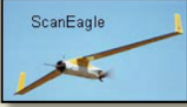
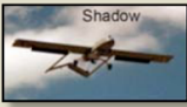

development, and \$198 million was allocated for military construction [7]. The DoD is expected to procure approximately 3,250 new UASs, of which 3,070 are considered small UASs, or sUASs [7].

This research explores: a) current cybersecurity assessments for tactical level sUASs, b) the security pillars and interconnectivity issues that sUAS cybersecurity assessments should address, and c) a methodology intended to create a sUAS Cybersecurity Risk Management Decision Matrix (CCRDM). Although this study primarily focuses on Group 1 through Group 3 UASs (e.g., Raven, ScanEagle, Puma, RQ-21), it is intended to function as a template for any and all future COTS or mil-spec UASs operating under DoD control.

A. DEFINITION OF UAS

While the issue of cybersecurity applies to all UAS, the boundaries of this study relate to small UASs (sUASs). sUASs contain multiple subsystems that should be independently assessed for cyber-centric capabilities. These subsystems should then be individually assessed for potential vulnerabilities that could result in operationally relevant violations to confidentiality, integrity, and availability (CIA). Scoping this study to a more manageable level is achieved by narrowing the research to only those UASs deployed at the tactical edge; which means DoD defined Groups 1 through Group 3 UASs as seen in Table 1.

Table 1. DoD UAS Group Descriptions. Source: [8].

UAS Groups	Maximum Weight (lbs) (MGTOW)	Normal Operating Altitude (ft)	Speed (kts)	Representative UAS	
Group 1	0 – 20	<1200 AGL	100	Raven (RQ-11), WASP	
Group 2	21 – 55	<3500 AGL	< 250	ScanEagle	
Group 3	< 1320	< FL 180		Shadow (RQ-7B), Tier II / STUAS	
Group 4	>1320		> FL 180	Any Airspeed	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)
Group 5		Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)			

UASs, as represented and discussed in this effort, are defined as “a system comprised of an unmanned aircraft and its associated elements required for operation” [8]. The aforementioned elements are broken down into subcategories that comprise the unmanned aircraft itself; payload, communications, control, support equipment, and the human operator. Aircraft types included in the study consist of fixed wing and quadcopter configurations, each varying with range and capability. Payloads come in a variety of different form factors, and can include electro-optical (EO) video cameras and electromagnetic warfare (EMW) sensors that may exploit networks or radar systems. In some cases, sUASs are used as network relay or communications hubs that connect geographically dispersed communications networks. Control communications can utilize Internet Protocol (IP) and Radio Frequency (RF) based protocols based on the specific aircraft configuration. Support equipment consists of Ground Control Stations (GCS), launch equipment, recovery equipment, and antennas. No system in this study is self-sustaining, meaning each system ultimately requires the interaction of a human operators. This interaction represents a potential cyber vulnerability in itself.

Unmanned aircraft are further classified by the DoD into groups that are differentiated by maximum weight, operating altitudes, and operating speed [8]. Group 1 UASs are often used for base security or small unit operations. These smaller UASs can be hand-launched, have a wide degree of self-containment, and are extremely portable. Group 2 UASs are small to medium sized platforms that conduct ISR and target acquisition mission sets. Portability and rapid deployment are reduced in this group of physically larger aircraft; however, the payload generally increases capability by adding features such as EO or infrared (IR) and laser range finding/designator (LRF/D) capabilities. Finally, Group 3 UASs conduct longer range missions with more enhanced payloads relating to EO/IR, LRF/D, signal intelligence (SIGINT), communications relay, and chemical biological radiological nuclear explosive (CBRNE) detection [8]. The detailed characteristics of each DoD UAS group is further explained in the DoD UAS Group Descriptions Table. The next section provides context to the purpose of this effort and the tactical military application.

B. PURPOSE OF STUDY

Implementing the use of emerging technologies, such as sUASs, into military missions requires an advanced risk assessment, at all levels - cradle to grave. A thorough understanding of each system's cyber vulnerabilities is critical for employing appropriate mitigation techniques and lessening the overall risk. This effort is intended to provide the UAS commanders at the tactical level the tools needed to mitigate cybersecurity risk to mission, equipment, and personnel. First and foremost, specific cybersecurity risk assessments need to be conducted by the trained personnel, at the appropriate level, with proven methodologies. The operators and mission commanders at the tactical level can then incorporate local threat capabilities with the assessment of available UAS mission platforms, to either waive or accept the calculated risk. There is no need to invent new cybersecurity operational risk processes, since a majority of non-UAS-specific cybersecurity techniques can be tailored to address UAS vulnerabilities. Adding the practice will provide tactical users an opportunity to properly assess each scenario, and allow them to make a better-educated risk decision.

Making an educated risk decision in cybersecurity is not generally a simple yes or no decision. Consequently, the cybersecurity risk decision process should be robust enough to provide tactical operators and mission commanders the opportunity to make decision based on an understanding of situational and inherent risk. The proposed process should permit the tactical decision makers an opportunity to assess and make the best possible decision as to which system to operate and what mitigation actions to take. This effort will focus on two central questions on the quest to create a UAS cyber risk matrix that can be used by tactical commanders. The first is: What processes and considerations should a streamlined, full spectrum, UAS cybersecurity decision matrix incorporate for evaluation? The second is: What elements of existing non-UAS cybersecurity frameworks should be incorporated into the UAS cybersecurity decision matrix? Utilizing well-known and validated cybersecurity risk processes and considerations will facilitate the development of a streamlined research approach.

C. APPROACH

Initially, an assessment of current tools or methodologies used for non-UAS cybersecurity risk assessments will be conducted. Next, the discovered tools and/or techniques will be correlated as applicable to UAS hardware and software. Upon correlation of applicable methodologies, proven cyber strategies will be applied to the tactical UAS life cycle. This effort will determine where the decision-making responsibility for cybersecurity risk assessments should reside from the tactical perspective. Finally, a study of current UAS missions, in coordination with the previous research, will help develop a mission-agnostic UAS cybersecurity risk assessment framework.

A general risk analysis assessment will be conducted focusing on RF and IP threats to UAS operations at the tactical level. Once the threats are identified, an initial UAS cybersecurity operational risk management decision matrix will be constructed. The initial matrix will be validated using accepted cybersecurity framework strategies promulgated by the National Institute of Standards and Technology (e.g., Federal Information Processing Standards (FIPS) and the Special Publications-SP800 series), and relevant DoD guidance.

The first objective involves the identification and assessments of potential threats to UAS operations. The methods to identify, correlate, and assign cybersecurity risk assessment methodologies will be determined by tailoring the cybersecurity fundamentals that already exist for non-UAS specific cybersecurity platforms. Once obtained, these will be recast into a tactical UAS cybersecurity risk decision management matrix. The aforementioned risk management decision matrix will be validated by an experienced tactical UAS operator; which may-in turn-lead to future work.

D. DESIRED END STATE

The purpose of this effort is to create a UAS Cybersecurity Risk Management Decision Matrix (CRMDM) that a tactical commander can utilize prior to launch. Integrating cybersecurity into tactical UAS operations will provide a framework for employing a critical military technology, while safeguarding sensitive information, and will act as a mission security multiplier. More information afforded to the appropriate decisionmakers will energize mission confidence, minimize the loss of sensitive data, and provide the mission commander (MC), officer in charge (OIC), or higher authority the opportunity to make a more educated cybersecurity risk decision. The CRMDM is not intended to be the decision authority, but merely a tool that will help bring UAS cybersecurity considerations to the attention of tactical commanders. The desired end state is to create a useable and understandable tool that shrinks the current gap between existing operational considerations and cybersecurity considerations for tactical applications of UAS technology. The next chapter provides a detailed background of system-agnostic UAS components and their functions.

THIS PAGE INTENTIONALLY LEFT BLANK

II. UAS COMPONENTS, ATTACK SURFACE BACKGROUND, AND SUPPORTING STANDARDS

The purpose and intent of sUAS employment has evolved since its inception, which is also true of the characteristics of sUAS internal design, diverse functionality, and inherent cyber-centric capabilities that classify a UAS as an IoT device. Compared to early models, late model sUASs have increased range, greater optical resolution, and provide the operator with real-time telemetry, command and control (C2) data, embedded sensors, and payload data. Flight times have significantly expanded. Early sUASs were lucky to see 20 minutes of flight time, and now 20 hours of flight time is routine for some of the Group 1 through 3 sUASs. The data capacity and data transfer between the sUASs and Ground Control Systems (GCSs) has evolved from its early design. sUAS form and function is a superb fit for both military and civilian C2 operations. It is important to understand the basic sUAS components and interfaces that are subject to malicious attacks, interception, and source localization by an adversary.

Once the system components are classified appropriately, then we will apply known federal information system (IS) security standards to mitigate potential risk to the mission, risk to the equipment, and risk to human life. The CRMDM must reduce potential compromise of sUAS CIA-centric information attributes. Potential cybersecurity mitigations can be identified by applying applicable Federal Information Processing Standards (FIPS), and Special Publications (SP) drafted by the National Institute of Science and Technology (NIST). The FIPS publications of interest include FIPS 199 Standards for Security Classification of Federal Information Systems, and FIPS 200 Minimum Security Standards for Federal Information and Information Systems. The SPs referenced by the aforementioned FIPS publications, and are utilized for risk mitigation standards, include the NIST SP 800–30 Revision 1 Guide for Conducting Risk Assessments and NIST SP 800–53 Recommended Security Controls for Federal Information Systems. It is important to understand UAS components in order to determine where vulnerabilities can exist, and which potential mitigations might address these vulnerabilities. This is covered in the next section.

A. UAS COMPONENTS

UASs vary greatly in design, capabilities, and the interconnected devices. However, most UASs share a moderate number of functions, features, and components. Understanding the basic UAS sub-model architecture is necessary to determine cybersecurity requirements and ultimately produce a more robust UAS CRMDM. Six major component groups, subdivided by function, should be analyzed for cybersecurity vulnerabilities. The first group is the communications system, the second group is the aircraft itself, the third group is the GCS equipment, the fourth group is the ground support equipment, the fifth group is the software, and the sixth group is the human operator.

1. Communications Systems

UAS communications possess a high adversary target value. It has this value since the RF communications are transmitted via wireless means, and thus vulnerable to observation capture, copy, retransmission, spoofing, and denial (jamming). Like other RF systems, two modes of in-flight communications exist within UAS communications suites: direct line-of-sight (LOS), and satellite-enabled over-the-horizon (OTH), which is also known as beyond line of sight (BLOS) [9]. An emerging OTH UAS communications technique is to use cellular connectivity for communications, which allows the UAS to send and receive communications through the cellular network, significantly extending the aircraft's range. Though this cellular connectivity provides OTH operator-to-UAS control; the actual RF mode is LOS. In one sense, this is a hybrid mode or method (multiple LOS circuits daisy-chained to provide OTH distances. Some UAS variants use tethered or optical communications. However, for sUASs the most common communication mode is LOS. UASs can use a single communication channel that multiplexes both payload and flight data, or these two data types can each be carried over dedicated channels [10]. A typical UAS communications scenario is illustrated in Figure 1.

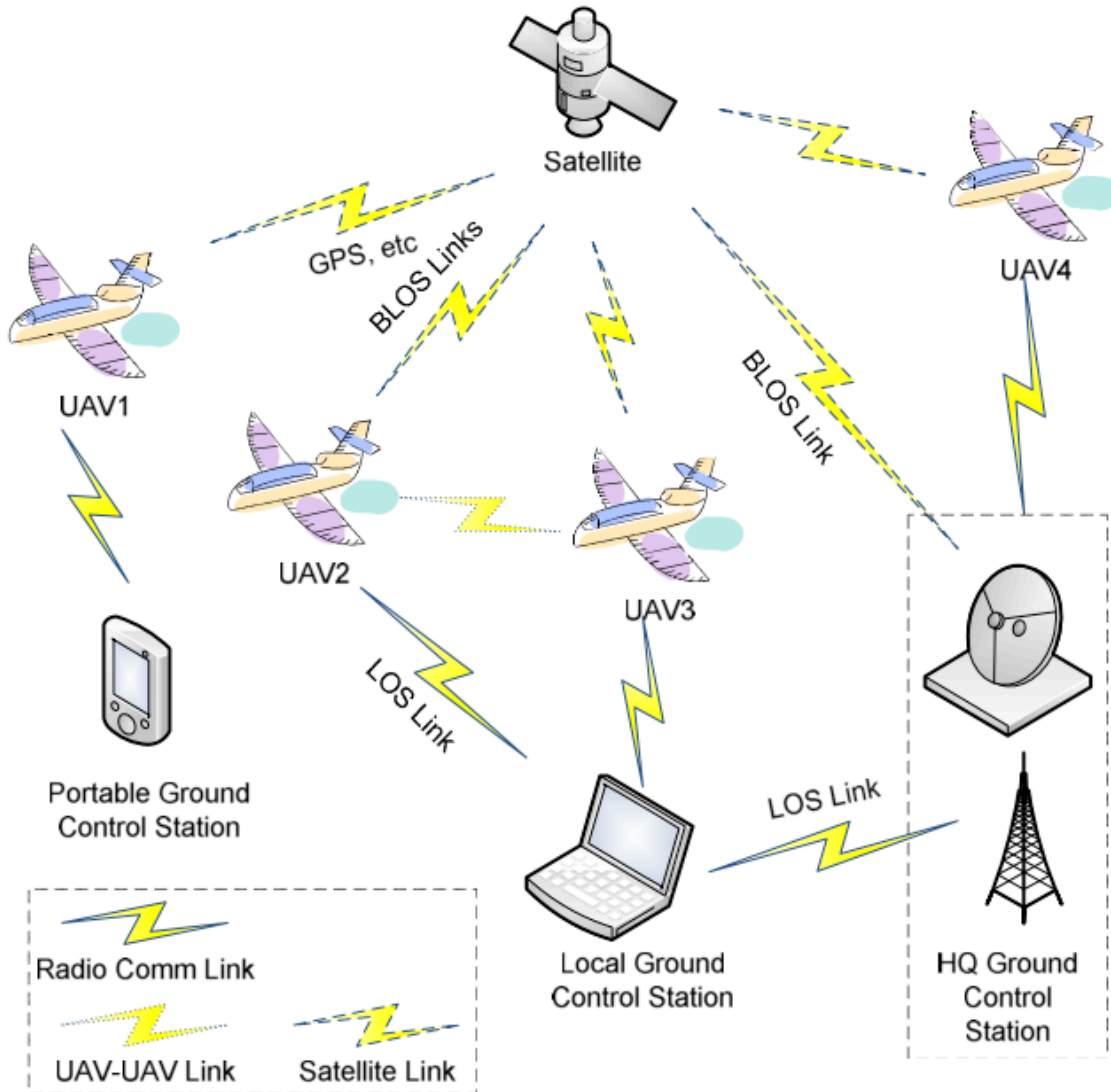


Figure 1. Typical UAV Communications Scenario. Source: [11].

LOS communications are the most common type of communications for Groups 1 through 3 UASs owing to size, endurance, range, and mission sets. Smaller aircraft have less room for fuel and flight sensors, and can stay operational for comparatively shorter durations than the Group 4 and 5 UASs. Satellite Communications (SATCOM) is used for larger, long-endurance, aircraft, such as the Northrop Grumman Global Hawk, that operate OTH [12]. Although SATCOM is an important topic in cybersecurity, the LOS communication techniques used in smaller UASs is where this thesis and resulting UAS CRMDM will focus.

RF-based LOS communications can span a wide range of the RF portion of the electromagnetic spectrum. However, most military LOS applications are centered in the Very High Frequency (VHF) and Ultra High Frequency (UHF) bands, with some reaching into the Super High Frequency (SHF) band. Examples of RF protocols operating in these bands include: microwave, Bluetooth, or 802.11 Wi-Fi communications [10]. Digital C2 and payload communications using TCP/IP onboard the aircraft must be modulated if transmitted from the aircraft to the GCS and vice versa. Integrated modems modulate and demodulate the UAS communications from digital signals into analog signals-and vice versa-for transmission. Modulated signals are attached to a carrier wave and transmitted and received using transceivers on the UASs and GCSs. Analog C2 and payload communications do not require the modulation and demodulation step and are transmitted using the same carrier wave methodology as modulated digital communications. LOS communication is increasingly moving into the microwave portion of the RF spectrum. This is due in part to the already inundated UHF band, in part to the increased bandwidth available at microwave frequencies, and in part to the fact that these higher frequencies are less affected by refraction than the lower frequency RF bands [13]. Bluetooth communications are not ideal for long range C2 or payload designs, since Bluetooth can only operate out to a nominal 40-foot range. Despite this range constraint, Bluetooth communications can exist onboard the aircraft or at the GCS and can be modulated for longer distance transmissions. Wi-Fi is another shorter distance UAS communications option, but it can be used in the same way as Bluetooth. Bluetooth communications reside in the 2.4Ghz RF range and Wi-Fi covers both the 2.4Ghz and 5Ghz RF ranges. Both Bluetooth and Wi-Fi operate in the common unlicensed Federal Communications Commission (FCC) RF bands. UAS communications transmit using the same technology radios, wireless routers, as any typical LOS communications transmission technique. This means that without mitigations, communications using these technologies are susceptible to the same threats encountered when they are used in non-UAS environments. In fact, the risk can be considered greater given the longer distances over which the RF-carried data is exposed.

UAS communications do not only exist between the GCS and aircraft. GCSs, aircraft, and associated ground equipment can be configured for TCP/IP communications and connect to an intranet or the Internet. Some COTS UASs, such as the Da-Jiang Innovations (DJI) family of Unmanned Aerial Vehicles (UAVs), communicate and transmit flight data back to the parent company using proprietary software from the UAV to the GCS, and then from the GCS through the user's network. Some military GCSs and aircraft communicate with ground support equipment via fiber optics, ethernet, or through wireless communication protocols. UAS internal and external communications designs, as noted above, can include standard configurations, proprietary configurations, or use a combination of both. Standard configurations include well known and commonly used software and hardware packages that span multiple UAS variants. Proprietary configurations are those that are specific to a certain family or brand of UAS, and not available for use on any type of UAS foreign to the manufacturer. These configurations may not be available to the operator. Each system operator should have, at a minimum, a basic understanding of the communications paths, protocols, and data processing components. Next, the aircraft is one of the top two critical components of the UAS.

2. Aircraft

Airframes come in many shapes, styles and sizes. Despite the variety in airframe appearance, the basic components are relatively similar. The UAS airframe itself is constructed with lightweight material and is aerodynamically stable. Obviously, there is no room for a pilot, which makes the avionics even more critical. The variance in avionics depends on the UAS manufacturer. Some examples of UAS avionics include the flight computer, flight processor, and power distribution assembly [10]. Additionally, aircraft components include payloads that support both the airframe design and meet the mission needs, mission or payload controllers, and communications capabilities [10].

The flight computer is the brains of UAS aircraft and interlinks onboard sensors with the UAS specific control surfaces with the sole purpose of collectively directing the aircraft's flight [10]. Sensors onboard that provide data input to the flight computer include altimeters, accelerometers, gyros, magnetometers, pressure sensors, and GPS systems [10].

The UAS control surfaces can include ailerons, elevators, elevons, propellers, rudders, and winglets [10].

Payloads are typically central to the aircraft design and some UASs have the capability to add additional payloads based on the design. Payloads often define the UAS mission and usually provide the capabilities for military and civilian entities interested in conducting dangerous, dull, and/or dirty missions with a much lower overhead cost [10]. Additional sensors include video cameras, infrared sensors, and environmental sensors are other forms of potential UAS payloads. UASs can process and retain data onboard the unit, transmit acquired data to the GCS or a secondary observation station for analysis, or consist of a hybrid of both onboard and external data processing [10]. The ScanEagle UAS illustrated in Figure 2 is a common Group 2 system used by the DoD.



Figure 2. ScanEagle® Size, Weight, Power, Performance, Sensor, and Data Information. Source: [14].

Mission and payload controllers are used to control the payload sensors onboard. These controllers constitute another computing and operational UAS component that leverages wired or wireless data paths that links operator control to the installed sensors [10]. Payload controllers can also direct payload data back to the operator for real-time or near real-time mission processing [10]. Mission and payload controllers are typically configured prior to launch, but there are some applications that permit real-time mission and payload manipulation to meet changing mission sets [10].

The design and functionality share the same techniques and procedures as a simple computer system or IoT device. Little attention was focused on the cyber-side of UASs until the DoD issued the UAV vulnerability memorandum [5]. The major differences between a standard IT infrastructure and the UAS are the operating altitude, proximity to

the threat, dependency on other systems (i.e., GPS), and nature of the mission. The UAS component that is essentially identical to the traditional computer systems is the GCS.

3. GCS

UAS GCSs come in a variety of sizes and are considered the UASs primary mission controller. The GCS is the UAS's central node of communication that receives, transmits, processes, and distributes data collected from the aircraft's C2 and payload links [15]. The GCS subsystem can be further subdivided into two types, portable and stationary.

Portable sUAS GCS can consist of extremely basic components, such as a hand controller, ruggedized laptop, RF transceiver unit, and a controller box [15]. More simplistic GCS designs combine the four aforementioned portable GCS elements into a compact hand controller connected to a cellular phone or tablet, which is the standard for many of the COTS sUASs. The video feeds and other onboard sensors can be controlled by the aircraft operator, or they can be simultaneously controlled by an additional payload operator.

Larger UASs, still residing in the Group 1 through Group 3 size range, may utilize a fixed location GCS that maintains all the previously mentioned GCS functionality but incorporates a larger network construct that acts as a server for multiple onboard UAS sensors in addition to ground control equipment. A good example of a high-end fixed ground station is the one for the Boeing Insitu ScanEagle platform. The ScanEagle GCS consists of multiple directional antennas, antenna modems, data interface modems for data distribution, software environment servers and workstations, autonomous tracking computers, fiber optic trunk lines, a C2 hand controller, and a payload controller [16].

The GCS size and capability are not the key takeaway; however, the identified networking capabilities, data storage, data transmission, and wireless communications inherent to UAS design must, at a minimum, incorporate a cybersecurity assessment criteria prior to launch. The GCS components function in the same way as other DoD critical infrastructure, with the same intricacy as a network. The size and complexity of UAS ground support equipment variations are similar to the GCSs The ScanEagle example

illustrated in Figure 3 uses one workstation, configured for one operator, to operate the platform.



Figure 3. ScanEagle® Unmanned Aircraft System (UAS).
Source: [14].

4. Ground Support Equipment

Ground support equipment varies from almost nothing, in the case of small quadcopters, to fully tailored launching and recovery equipment that takes a team of operators to manage. Some of the launchers are isolated and require remoted or wired GCS interaction. Others are launched from a fully remoted network connection back to the GCS that can be feet or miles from the launch site. The larger the aircraft and the more sensors it can carry generally requires a larger ground support footprint. Ground support equipment that is connected to the GCS is considered an information device and should carry the same active security measures as any DoD IS. The Mark 4 Launcher, Compact Mark 4 Launcher and SkyHook® shown in the ScanEagle Unmanned Aircraft System figure are examples of the ScanEagle UAS ground support equipment.

5. Software

UAS software, like the ground support equipment, is typically proprietary and is a potentially exploitable. UAS software is vulnerable to attack if identified vulnerabilities are not addressed. Threats can exploit UASs via Internet-based connections or via portable software devices. Portable devices can include thumb drives or compact discs that provide system software updates. Certain UAS software actually transmits device usage data via IP connectivity that is stored off-site using cloud computing services for company consumption. External user data exfiltrated from the UAS was the driving factor behind the 2018 DoD UAS flight ban and heavy restrictions of UAS use in military applications. The difficulty in securing IP-based software updates on each unique UAS software system is complicated by non-DoD third-party vendors, which increases risk to mission, risk to equipment, and puts operational forces at risk of exposure.

6. UAS Operators

The human element is arguably the weakest links in cybersecurity. Systems, including IoT systems, are designed by human programmers and architects to perform specific functions. Just as in the case with the creation of the Internet, the desired intent of IP-based traffic was to exchange data over a distance with relatively high speed. Historically, security is often an afterthought in data processing system development. Identification of required features that fit seamlessly with system design and conceptualizing low-drag freedom of functionality are at the forefront of system design. Essentially, users wanted ISs that were extremely fast, use the fewest components to keep costs low, and were not complicated by overly restrictive policies.

The above-mentioned computer system approaches would be acceptable if not for malicious intentions on the part of bad actors. Malicious threats come in two forms, external and internal. Insider threats are further subdivided into intentional and unintentional actors. These actors have potential to induce irreversible damage to sensitive data, facilitate unauthorized access to network systems, and provide access to additional network assets. External threats are constantly probing system boundaries to gain access to sensitive information. Persistent external threats even try to leverage potential weaknesses

by exploiting internal threats. For example, the untrained and unwary technician can unknowingly open a back door to a UAS if they use an unauthorized storage device on UAS hardware to save data. Another operator could inadvertently connect a UAS laptop to an unsecured network rather than an authorized military network. The internal threats have significant potential to cause grave damage to national security ISSs, especially when bypassing active security protocols either intentionally or unintentionally. Regardless of the motive, the act puts the mission, equipment, and personnel at risk.

B. ATTACK SURFACE BACKGROUND

Modeling the UAS vulnerabilities under the Federal Information System Management Act (FISMA) defined three core security objectives of confidentiality, integrity, and availability to then apply mitigating security controls will introduce a proven approach to frame the issues [17]. The UAV cybersecurity threat model, shown in Figure 5, introduced in 2012 captures potential UAS threat vectors that can be compared to existing control measures for the UAS CRMDM [11]. Existing control measures from FIPS 200 and NISP SP 800–53 will then be used to correctly categorize the likelihood, overall impact, and finally to derive a risk weight. The next step is to dive a little deeper into the three core security objectives, relate each with the appropriate or known risks, and then apply security controls to mitigate the overall risk factor. If the mission commander and operators understand the potential cyber security risk based on the tailored mission, then an adequate go or no-go criteria can be applied to almost any scenario with some potential required adjustments. Dividing the UAS cybersecurity challenge into distinct areas of concern will frame the design of the CRMDM. The descriptions are discussed from the left to right using Figure 4 as the guide.

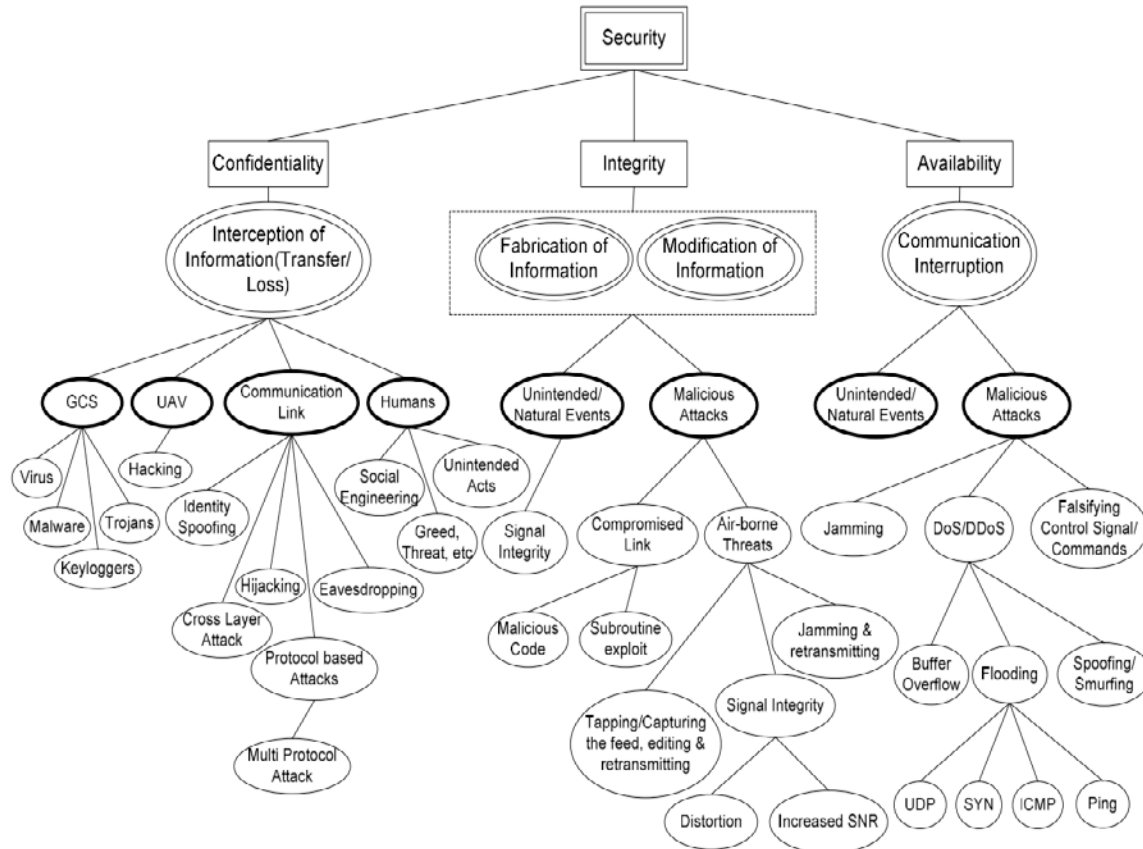


Figure 4. UAV System Cyber-Security Threat Model. Source: [11].

1. Confidentiality Threats

UAS confidentiality vulnerabilities exist when the interception of information (transfer/loss) occurs from the GCS, UAV, C2 links, and the human operator [11]. These four threat surfaces relate to systematic vulnerabilities commonly found in UAS design, protocol usage, network connectivity, and human error. Figure 5 frames the threats to UAS confidentiality, which are described in this section.

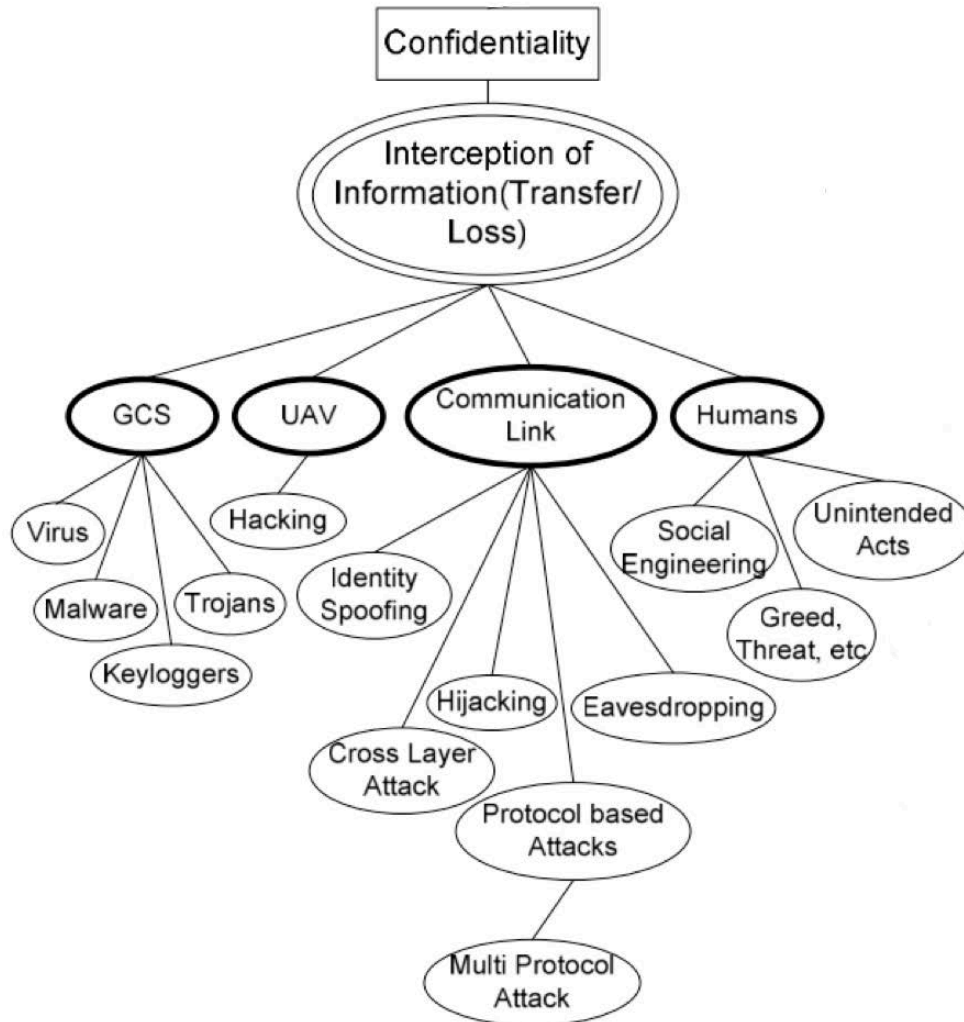


Figure 5. UAS Confidentiality Threats. Source: [11].

The GCS can be a large server rack, networked computing systems, or a small computing device. Just like any other computing systems, GCS are vulnerable to computer viruses. Viruses are computer code created with the intention of manipulating a system control or data. Malware, or malicious software, is a source for different viruses and system hijacking tools. Keyloggers are used to remotely collect or record input-output (IO) activity, such as keyboards strokes. Trojans, another form of malware, are disguised as legitimate software but work much differently under the covers. Trojans can be used to perform a number of malicious activities, for example control software systems and

exfiltrate data. The GCS is susceptible to any of the mentioned threats, and a careful approach must be applied to mitigate unnecessary risks.

UAV software is as susceptible to exploitation as the GCS suite, since they share common network paths and protocols designed to maintain system connectivity [11]. If the GCS is infected with malicious software or permits unauthorized access, then there is a high likelihood the UAV software could also be affected [11]. Unattended or unauthorized physical access to the UAV is also another potential threat vector that could put the UAV software at risk if malicious software is introduced to the aircraft.

The communications links are an integral part of UAS operations. Vulnerabilities, associated with communications, link a significant share of threats to confidentiality. C2 signals can be spoofed with an intended goal of de-authenticating the UAV with the GCS. ISs have experienced malicious protocol attacks at many layers of the protocol stack that induce various types of protocol malfunction. Newer cross-layer attacks, can impact UAV C2 through at least three methods. One method is Media Access Control (MAC) Poisoning, a second is known as Hammer-and-Anvil, and a third is the Transport Control Protocol (TCP) Timeout [18]. MAC poisoning is the act of periodically falsifying a frequencies channel reservation to cause the device to eventually switch to another channel [18]. Hammer-and-Anvil cross-layer attacks utilize a jammer and compromised network node to force traffic redirection through the compromised node [18]. TCP Timeouts occur when TCP flows are disrupted by increasing packet round-trip-time and forcing the sender to increase retransmission timeouts and delay forwarding packets [18]. The delay in forwarding packets causes TCP traffic to eventually enter a timeout state and results in dropped packets [18]. Due to the often uncontrolled transmission medium, C2 transmissions are also easily intercepted by eavesdroppers.

Confidential UAV communications links have the potential to become victims of eavesdropping or, even worse, hijacking. Confidentiality is lost when anyone who is not intended to intercept UAS communications can do so. Exposing UAS telemetry and payload communication data can offer system details, location, and even expose critical mission data if not protected. Hijacking UAS communications means essentially losing authenticated control, as a result of blocked or spoofed signals [19]. These intentional

interferences with UAV signals can include jamming the frequency at which the C2 or payload signals are received. Blocking, also known as jamming, is intended to prevent the receiver from detecting authenticated signals. The three well-known types of signal jamming are applicable to narrowband, broadband, and spread spectrum transmissions [19]. Spread spectrum signals are the least impacted by jamming due to the nature of their frequency hopping design, which helps avoid concentrating the signal into a predictable and targetable bandwidth.

The human element has consistently been the weakest link in cybersecurity, especially with the growing success rate of malware, phishing attempts, and social engineering. Another risk posed by humans is that of the disgruntled or unwitting personnel within the organization. Untrained, unknowing, and/or unhappy personnel can cause a threat to the UAS IS confidentiality.

2. Integrity Threats

UAS information integrity is comprised of two types of activities: “fabrication of new information” and “modification of exiting information” [11]. The information can consist of C2 and/or payload communications [11]. Natural phenomenon and malicious activities are two known ways to modify or fabricate RF information [11]. Figure 6 frames the threats to UAS integrity, which is described in this section.

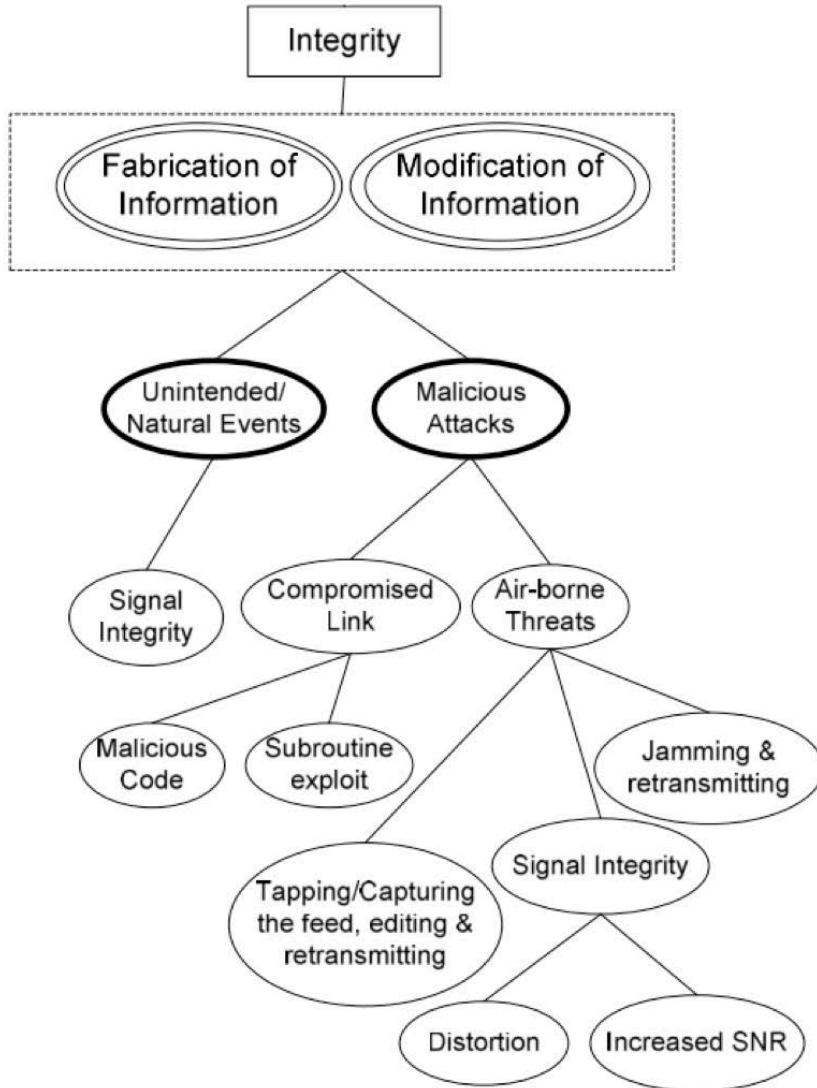


Figure 6. UAS Integrity Threats. Source: [11].

The integrity of UAS communications information can be compromised by unintended or natural events through radiofrequency interference (RFI) or electromagnetic interference (EMI) [20]. Unintended events can induce signal noise that may interfere with signal quality [20]. UASs, like many other RF communications systems cannot compensate when out of phase signals interfere with the original signal strength. Three different sources of interference exist; natural radiators, unintentional radiators, and intentional radiators [20]. Natural radiators include such elements as lightning or other atmospheric electrical discharges, strong solar activity, and meteorological events like snow or dust storms [20].

Unintentional radiators consist of man-made devices that radiate electromagnetic waves as a by-product of their intended function [20]. Examples of unintentional radiators can include high capacity power lines and transformers, household devices like microwaves and small consumer electronics, and direct current motors [20]. Intentional radiators are designed to utilize the electromagnetic spectrum and are a major competitor for RF spectrum allocation. Intentional EMI comes from anything that is transmitting RF, such as TV transmitters, Wi-Fi devices, cordless phones, hobbyist radios, and IoT devices [20]. Of the two types of information manipulators, unintended or natural events create a lesser concern and most UAS RF subcomponents can adjust to these rare anomalies, or are not generally operated in conditions that create this interference [11].

Malicious UAS communications attacks are a major threat to UAS integrity. Malicious attacks are known to come from compromised communications links, communications systems, and now airborne counter UAS systems [11]. Compromised communications from anywhere in the UAS can lead to devastating results on mission accomplishment, data integrity, and affect UAS confidentiality and availability. Compromised links simply mean the link is not completely under control of the dedicated GCS. Malicious actors can threaten UAS integrity by introducing malicious code into the UAS software and communications links [11]. Malicious code, found in an available Maldrone payload, is able to take over the control of UAVs using the ARM processor and Linux operating systems (OS) [21]. Air-borne threats are able to jam and retransmit UAS RF signals, distort or stomp signal integrity, and utilize captured communications feeds to facilitate a replay attack [11]. Signal jamming impacts both the integrity and availability of UAS communications [11]. Jamming distorts the receiver's ability to receive the correct signal and it can raise the RF noise floor up to a level that negatively impacts receiver sensitivity [11]. If jamming is followed by retransmitting, then the overall impact rests with UAS communications integrity, since the received signal is not the originally intended signal from the GCS or UAV [11]. Malicious actors can collect the transmitted UAS communications and replay them at a later point to confuse the UAV. Additionally, a skilled malicious actor can tap into the collected or live communications feeds and edit them for retransmission at a later point in the UAS mission [11].

The last component of the CIA trifecta, UAS availability, is as critical as confidentiality and integrity of the UAS information.

3. Availability Threats

The loss of UAS availability means that the system, or subcomponents of the system are not available to conduct the mission. The primary sources of UAS non-availability are communications jamming, denial of service (DoS), or falsifying C2 communications [11]. Figure 7 frames the threats to availability, which is described in this section.

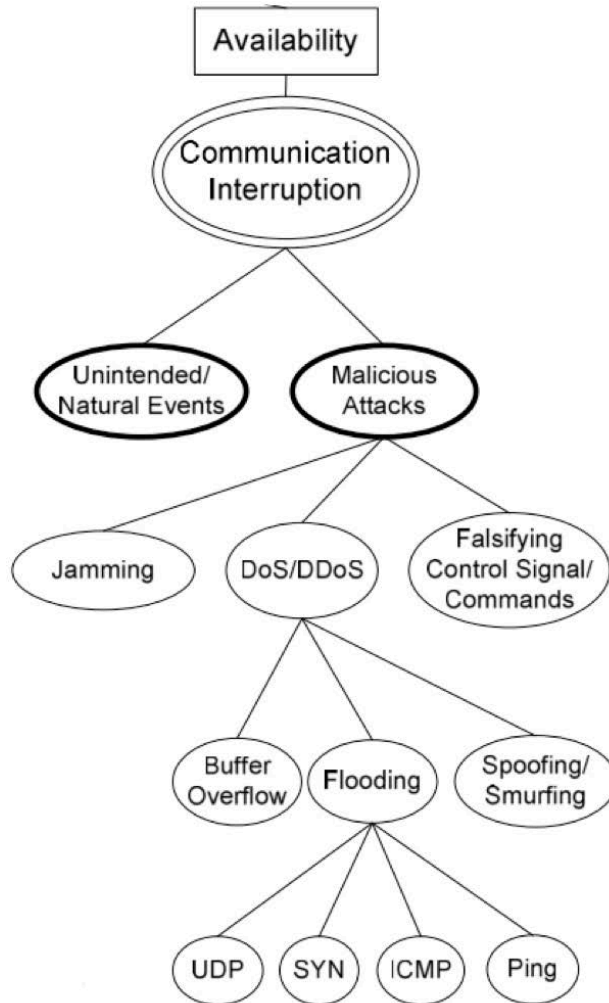


Figure 7. UAS Availability Threats. Source: [11].

DoS or Distributed Denial of Service (DDoS) attacks against UASs come in three types: buffer overflow, protocol flooding, and spoofing (or smurfing) [11]. A buffer overflow occurs when a program's allocated memory buffer is overrun and adjacent memory is overwritten. The adjacent memory would be utilized by the program to store in program instructions and pointers. When the required instructions are overwritten, then the program will likely crash or the attacker can attempt to execute shell code that can give the attacker access to the kernel shell. Once the attacker has access to the shell, then additional exploits can be installed on the OS. Flooding, or protocol flooding, exists when a node is bombarded with requests, for example synchronize (SYN), User Datagram Protocol

(UDP), and Internet Control Message Protocol (ICMP) requests [11]. Figure 7 shows *ping* as an attack vector. *Ping* is a system administrator tool that sends ICMP echo requests and awaits an ICMP echo reply from the desired recipient. Essentially both ICMP and Ping attacks use the system design against itself. Smurfing attacks utilize ICMP packets “spoofed” with the victim’s IP address that are forwarded to many different nodes, which in turn reply with many ICMP echo replies and bog down the network.

Falsified UAS C2 and critical data signals have the potential to cause the aircraft to receive false GPS input data or false control signals [11]. UAS telemetry data is heavily reliant on accurate GPS data and this is one of the most well-known threat vectors for the UAS aircraft. GPS uses a low strength signal, which means it is predisposed to jamming or false GPS signal injection. GPS spoofing is dangerous to aircraft operations and has left U.S. military units in the dark during ISR missions.

It is important to develop a credible risk management framework as a reference for the UAS CRMDM. The DoD, in conjunction with NIST, has worked to build a framework that addresses information security (also known as cybersecurity) requirements for federal ISs. Standards development started at NIST with its 2004 release of FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems” [22]. Shortly thereafter, NIST released FIPS 200, which is titled “Minimum Security Requirements for Federal Information and Information Systems” [23]. Appropriate security controls were released by NIST in the SP 800–53 “Recommended Security Controls for Federal Information Systems,” which align with three impact levels identified in FIPS 200 [24]. The NIST 800–30 Revision 1 is the “Guide for Conducting Risk Assessments” that outlines a six-step risk assessment process [25]. It is important to note that these references were not created as standards for Cyber Physical Systems (CPSs), such as sUASs. CPS introduces a dynamic not previously considered in traditional IT. For example, sUASs physically operate in adversarial territory at a distance from the operator as opposed to traditional IT that is normally controlled on friendly ground and at the operator's fingertips. The following sections discuss the core elements of each relevant FIPS and NIST cybersecurity process.

4. FIPS 199

In 2002, the E-Government Act was initiated as public law [26]. NIST was tasked by FISMA to create “standards to be used by all federal agencies to categorize all information and ISs collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels” [22]. Additionally, NIST was tasked to create recommended guidelines for each type of information and IS and to develop minimum information security requirements [22]. FIPS 199 addresses the first requirement to “develop standards for categorizing information and information systems” [22].

In FIPS 199, information and IS categorization is based on the potential impact to mission, asset protection, legal obligations, functionality, and personnel protection if an adverse event should occur [22]. Three primary security objectives were defined by FISMA; confidentiality, integrity, and availability (CIA) [22]. Confidentiality is defined as, “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” [22]. More specifically, if confidentiality is compromised then the “unauthorized disclosure of information” has occurred [22]. Integrity is defined as “guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity” [22]. Modifying information is considered a loss of integrity [22]. Availability is defined as “ensuring timely and reliable access to and use of information,” which means one cannot use the IS when needed [22].

FIPS 199 describes three impact levels: low, moderate, and high [22]. Low impact has a “limited adverse effect” on operations, assets, or individuals [22]. The low impact degradation to mission does not impact the primary mission function but may have limited results, minor damage to assets, low financial impact, and minor harm to personnel [22]. Moderate impacts to the CIA triad would reasonably be expected to induce “serious adverse effect” on operations, assets, or individuals [22]. The loss of CIA at a moderate level of impact could reasonably be expected to yield substantial degradation to the mission capability, duration, and effectiveness is considerably reduced [22]. High potential impact

to the operations, assets, or individuals will result in “sever or catastrophic adverse effect[s]” [22]. High impact equates to mission failure.

The FIPS 199 further applies the security category to the information types and ISs. This process applies the overall CIA impact to each type of system or type of information [22]. An example of this process is formed in the equation, “SC information type = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}” [22]. Security control (SC) is applied to the information type in this example. In practical application, the information type will be replaced by the type of information and the impact will be scaled using the aforementioned low, medium, or high categories. Information types can have a negligible impact level, below the low threshold and be assigned a “N/A” for not applicable [22]. This is not the case with IS, since there is at least a low minimum potential impact that is inherent when protecting system processes and functions that are necessary for the system to function. Generally, the highest impact category will be selected for each information type, which is known as the “high water mark” [22]. The culmination of mapping the security objectives with its potential of impact are further explained in Table 2.

FIPS 200 is the next sequential policy document on characterizing the IS.

Table 2. Potential Impact Definitions for Security Objectives.
Source: [22].

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

5. FIPS 200

FIPS 200 [23] is the second NIST document resulting from the E-Government Act of 2002 [26]. The publication furthers system categorization from FIPS 199 by specifying minimum security requirements for IS and information security and incorporates a risk-based process to select security controls that will meet minimum requirements [23]. The end-goal of FIPS 200 is to facilitate a “consistent, comparable, and repeatable approach for selecting and specifying security controls for ISs that meet minimum security standards” [23]. The IS impact levels remain consistent with those previously outlined in FIPS 200. The minimum-security requirements and security control selection are main focus of FIPS 200 [23].

Seventeen security-centric areas requiring CIA protections are defined in FIPS 200 that represent each area of concern with the security of Federal information and ISs are listed in Table 3 [23].

Table 3. FIPS Security-Centric Areas Requiring CIA Protections.
Source: [23].

Access Control	Media Protection
Awareness and Training	Physical and Environmental Protection
Audit and Accountability	Planning
Certification, Accreditation, and Security Assessments	Personnel Security
Configuration Management	Risk Assessment
Contingency Planning	System and Communications Protection
Identification and Authentication	System and Services Acquisition
Incident Response	System and Information Integrity
Maintenance	

According to FIPS 200, minimum-security control selection is based on the premise that each organization is required to ultimately achieve adequate security by implementing controls and assurance requirements that are outlined in NIST SP 800–53 [23]. FIPS 200 discussed the security controls in NIST SP 800–53 are all associated with the designated impact levels of the IS that were originally determined in the security categorization process [23]. More specifically, the low-impact IS must have low baselined controls in place, moderate-impact systems must utilize moderate controls, and the high-impact must use high baselined control measures [23]. All security controls must be employed in each security control area unless specific allowances permit tailored control measure implementation [23].

6. NIST Special Publication 800–53

NIST SP 800–53 is the security control source document that provides control measures in accordance with FIPS 199. The publication describes fundamentals in security control selection, provides a process for selecting controls, and is describes IS related controls for low, moderate, and high impact ISs [24].

The fundamental components in chapter 2 of SP 800–53 provide an outline for the security control structure, baselines, designation, and assurance [24]. This document aligns the security controls into identifiers and families. Table 4 provides the listing of security control classes, families, and digraph identifiers. The security control structure encompasses three distinct sections named the control section, the supplemental guidance section, and the control enhancement section [24]. Baselines are the initial minimum-security controls recommended for an IS based on the systems categorization in FIPS 199 [24]. The system categories are a product of the initial risk assessment [24]. Security control assurance is the level of confidence that is acquired once security controls are selected and in-place [24].

Table 4. Security Control Identifiers and Family Names.
Source: [24].

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

The process for selecting security controls in SP 800–53 involves: "selecting appropriate security control baselines; tailoring the baselines; documenting the security control selection process; and applying the control selection process to new development and legacy systems" [24]. The initial selection employs the FIPS 199 framework of

choosing the high-water mark from the ISs impact level based on CIA [24]. Once the initial baseline is selected, six follow-on steps need to be considered as an attempt to tailor the baseline [24]. The first follow-on step is to identify common security controls within the initial baseline [24]. The second follow-on step is to scope the baseline [24]. Scoping can be from a technology, infrastructure, scalability-centric, or a need to compensate from the initial control selection [24]. The third step is to consider implementing compensating controls [24]. Compensating controls are comparable controls, possibly adopted from alternate sources, that address organizationally defined minimum and maximum acceptable values [24]. The fourth step is to “assign security control parameter values” [24]. Assigning parameter values is conducted after the initial selection of compensating controls and assigned organizationally-centric values for each parameter [24]. The fifth step is to supplement the control baseline if additional security controls are required by laws or regulations, but not specifically listed in SP 800-53 [24]. The sixth step is to ensure the high-level abstract security statements include enough detail to answer what the control is for, how it is to be implemented, and the overall intent of the control [24]. Documenting the process creates a record of “relevant decisions taken during the security control selection process” and “provides sound rationale for those decisions” [24]. Finally, controls can be used for new systems, such as new UASs, as a "requirements definition" or legacy systems using a "gap analysis perspective" [24].

7. NIST Special Publication 800–30

NIST SP 800–30 is the federal guide to conducting risk assessments on IS and expands on NIST SP 800–39 “Managing Risk for Information Systems” guidance [25]. The guidelines were broadly developed, through a technical lens, and are translatable to similarly developed national security systems [25]. The applicability of SP 800–30 reaches each tier of the risk management hierarchy and provides step-by-step specifics for the risk assessment process [25]. Consistent monitoring is critical to ensure the risk levels are addressed when risk changes, and SP 800–30 offers guidance on the appropriate way to monitor risk on an ongoing basis [25].

The risk management process is illustrated using four distinct steps as shown in Figure 8. Framing the issue is the key to the risk management processes [25]. A company or agency can describe the operating environment where the risk decisions are initiated [25]. Framing addresses how risk is assessed, responded to, and monitored [25]. “Assess” encompasses the identification of threats, vulnerabilities, adverse impact, and likelihood of harm [25]. “Response” is how an organization plans to respond to risk after it is determined by the risk assessment [25]. Responding to risk involves developing different Courses of Action (COAs), evaluating the new COAs, selecting appropriate COAs that are aligned with the acceptable risk tolerance, and implementing risk response actions based on the desired COA [25]. “Monitor” determines the processes by which risk is monitored over time [25]. Monitoring risk includes assessing the effectiveness of risk response actions, defining risk-impacting changes in the systems environment, and verifying planned response actions are implemented and aligned with institutional regulatory directives or standards [25].

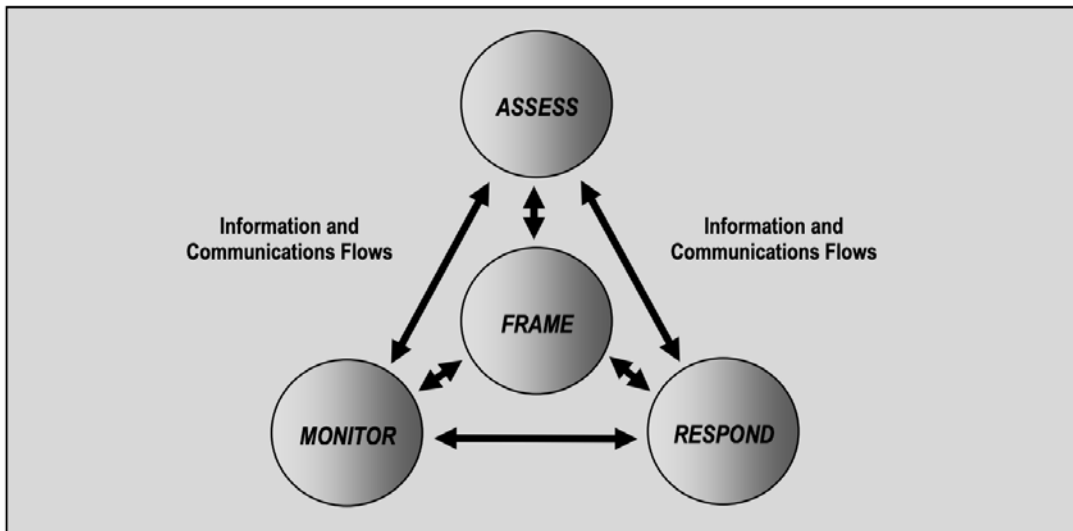


Figure 8. Risk Assessment within the Risk Management Process.
Source: [25].

The methodology consists of the actual risk assessment process, the risk model, an assessment approach, and an analysis approach [25]. The aforementioned components of the risk assessment methodology are illustrated in the risk assessment process of SP 800-30 (Figure 9). The process helps prepare organizations to prepare for the risk assessment process, to conduct the assessments, to communicate the results to key organizational components, and how to maintain risk assessments over time [25]. Risk models essentially provide context to the risk factors and their relationship [25]. Risk factors include the threat, threat events, vulnerabilities, impact, likelihood, and any affecting condition [25].

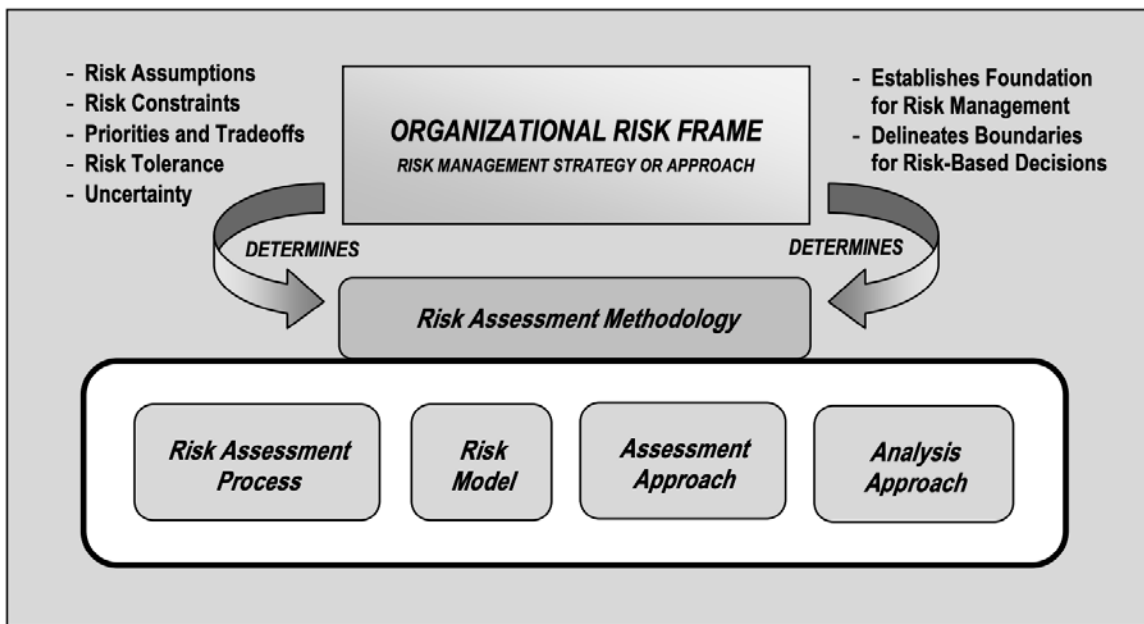


Figure 9. Relationship among Risk Framing Components.
Source: [25].

The risk model is developed to determine, through an identified process, the likelihood of a potential threat and the impact it will have on the IS [25]. An example of a generic risk model is shown in Figure 10. Threat modeling will provide a uniform path that analysts can feed credible intelligence data into and arrive at an effective understanding of organizational risk. Understanding the threat characteristics using the likelihood of success will provide a realistic, if not exact, match to pair with the vulnerabilities [25]. This will provide an overall degree of impact that produces an organizational risk to mission or the

organization itself [25]. The most user-influenced step within this risk model is the ability to mitigate vulnerabilities or predisposed conditions by enabling the proper security controls.

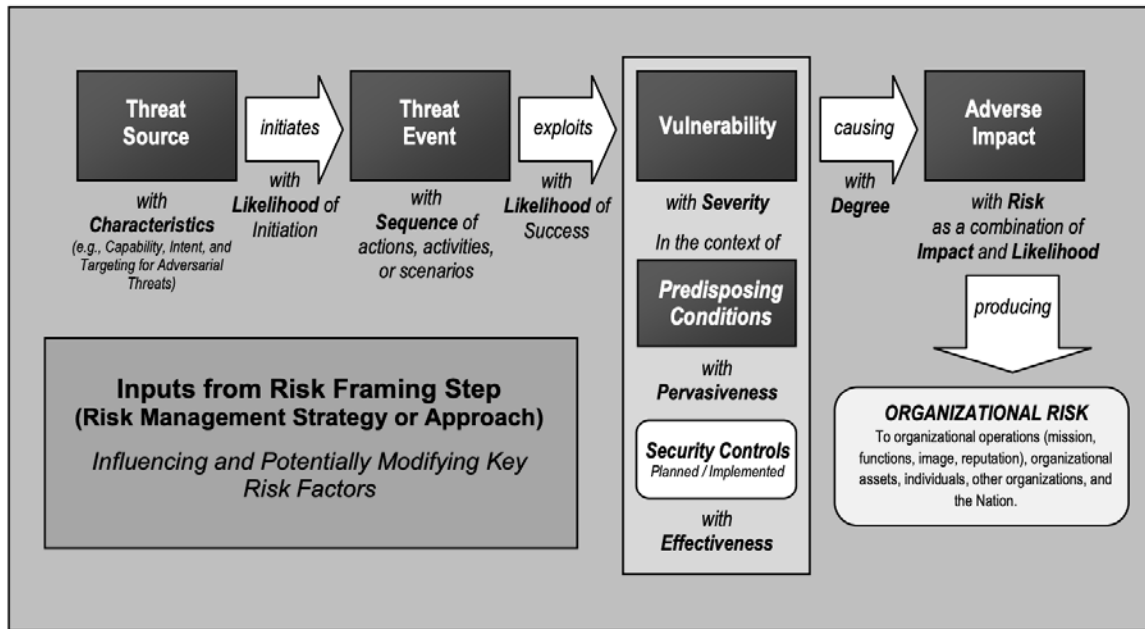


Figure 10. Generic Risk Model with Key Risk Factors. Source: [25].

The three assessment types outlined in SP 800–30 are: quantitative, qualitative, and semi-quantitative [25]. Quantitative assessments use a number-oriented methodology to determine the risk value [25]. Numerically assessing values requires interpretation and may lead to confusion when dealing with assumptions [25]. Qualitative assessments use high, medium, or low principals to assess risk without the use of numbers [25]. Finally, semi-quantitative uses a mixture of quantitative and qualitative methodologies that uses bins for value-ranges to determine an overall area high, medium, or low assessment value [25]. In order to successfully use the semi-quantitative value system, it is important to ensure each bin value is explicitly defined and provide understandable examples [25].

Assessment approaches come in three types: threat-oriented, impact-oriented, vulnerability oriented [25]. The threat-oriented approach is appropriate when the identified threat and defined threat events are known and can be used in an assessment scenario [25].

Also, threat-oriented approaches identify vulnerabilities using the threat as context, with impacts identified by the adversary's intent [25]. The impact-oriented approach is appropriate when the impacts or anticipated consequences from a threat event are used to determine the overall impact [25]. The vulnerability-oriented approach starts with the vulnerabilities, or pre-disposed conditions, in the IS or supporting environment [25]. Threat events are then identified that could exploit the known vulnerabilities [25].

Figure 11 details the actual risk assessment process. Chapter 3 of SP 800–30 provides a high-level overview on the actual process and provides sub-tasks for each step [25]. The steps are subdivided into four areas. The first step is to prepare for the assessment, the second is to conduct the assessment, the third is to communicate the results and the fourth is to maintain the assessment [25]. Preparing for the assessment involves identifying the purpose, scope, assumptions, constraints, sources of information, risk model, and analytic approach for the assessment [25]. Conducting the assessment involves identifying the threat sources, threat events, and vulnerabilities [25]. Additionally, conducting the assessment involves determining the likelihood a threat would instigate a threat event, determine the adverse impacts on the organization, and finally determine the IS security risks. Communicating and sharing the risk assessment results is step 3, and is vital to sharing any information gathered from the assessment to members or entities across the organization with emphasis in supporting additional risk management scenarios [25]. Sharing the information can be accomplished by any number of ways. For example, an executive brief or distributing assessment reports should be shared with organizational stakeholders in accordance with organizational policy [25]. Finally, maintaining the assessment is step 4 in SP 800–30, and could be accomplished using a log for historical reference and continuity for future assessments [25].

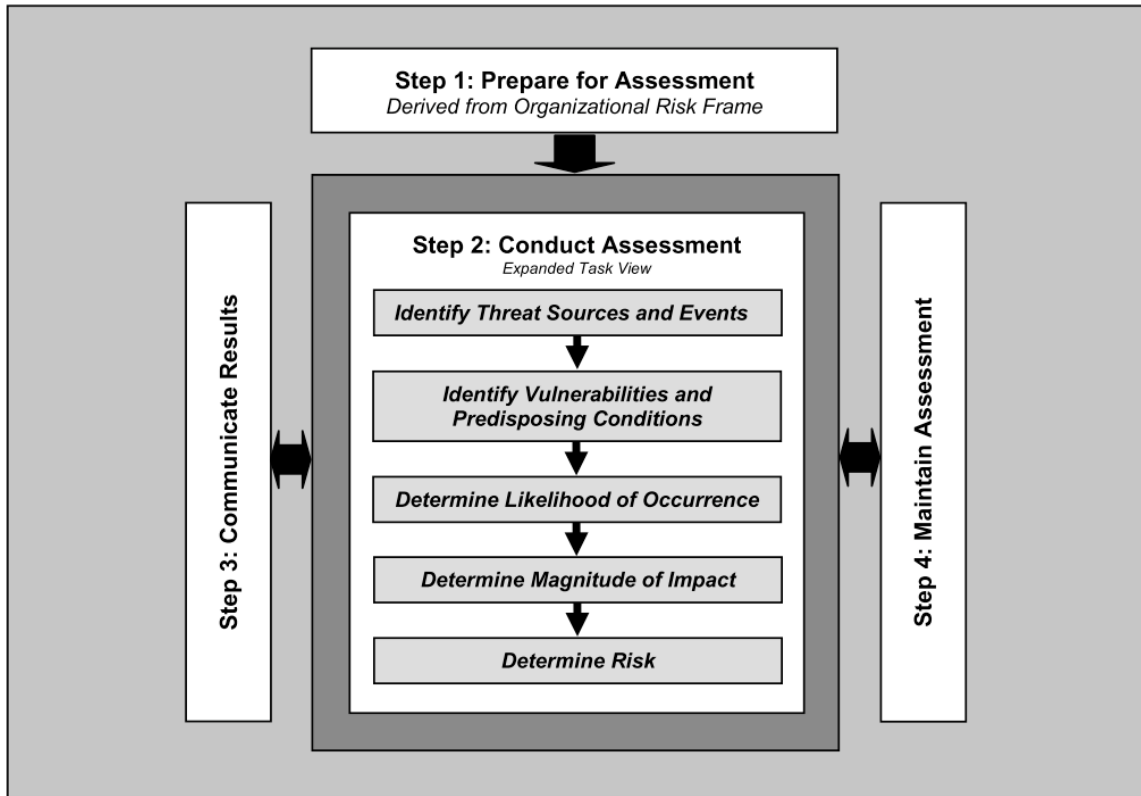


Figure 11. Risk Assessment Process. Source: [25].

Chapter III describes the process of translating each of these diverse requirements into a CRMDM for sUAS CPS.

THIS PAGE INTENTIONALLY LEFT BLANK

III. APPLYING NIST AND FIPS SECURITY STANDARDS TO UAS

The purpose of a UAS risk assessment is to provide a level of awareness and input for commander's the decision cycle. The assessment includes negative effects an adversary or natural phenomenon can introduce to UAS mission confidentiality, data integrity, and system availability. Once the potential threats are identified, a determination must be made as to the likelihood each threat could act on the UAS. Next, if the event occurs, determining the impact on the assets, individuals, component commands, or even the nation if the vulnerabilities were exploited [25]. Finally, the need to determine the overall sUAS cybersecurity risk assessment must be understood prior to system use, as is the case with any other operational or organizational risk management process.

While there is no fully validated or commonly accepted equation that can be used to calculate cybersecurity risk, this work relies on a reasonable and systematic approach to calculating the overall risk assessment of UAS C2 and payload information that is represented by a concise general equation described below. For the UAS application, the equation involves input and action at the strategic, operational, and tactical tiers of the UAS cybersecurity life cycle. Although this paper is geared toward the tactical tier, it is imperative that each tier be addressed to achieve the best possible risk assessment and determination for utilizing the UAS in tactical missions. We assume that the qualitative, semi-quantitative, and risk descriptions discussed in NIST SP 800–30 [25] also apply to UAS CIA.

UAS C2, payload information, and UAS CIA can be addressed using the SP 800–30. The critical considerations required to perform an effective UAS cybersecurity risk assessment are the threats, vulnerabilities, and potential impact suffered if the system is attacked. Ideally, UAS mission commanders would have pre-assigned values for each of these risk elements that could be referenced to assist in making go/no-go decisions. There are other methods to calculate cybersecurity risk, such as $Risk = Threat \times Vulnerability \times Consequence$, but there is no reduced vulnerability calculation when either removing or mitigating the vulnerabilities [27].

A. CALCULATING UAS CYBERSECURITY RISK

The NIST SP 800–30 generic risk model with key risk factors flow chart in Figure 10 (above) implicitly represents an equation that can help determine the overall risk, or “organizational risk” [25]. Threats are categorized by an entity that can conduct a malicious event. Vulnerabilities have inherent severity levels that are outlined as “predisposing conditions,” these can be mitigated by removal or applying security controls [25]. Exploited vulnerabilities can cause adverse impacts with a certain degree of likelihood. Although it is not explicitly written in the NIST SP 800–30, it is implicitly shown in Figure 10 that a relationship exists that can be used to determine the overall risk to the mission, assets, or personnel. This relationship can be expressed as an equation [25]:

$$(1) \quad Risk = Threats \times \frac{Vulnerabilities}{Security\ Controls} \times Impact$$

Optimally, if the strategic or operational commander requires UAS support as part of the mission, then some level of cybersecurity is required. Regional specific threat identification and analysis is necessary for each UAS operating area [28]. The ultimate goal, inspired by Defensive Cyberspace Operation concepts, is to reduce an attacker’s advantage by determining the overall cybersecurity risk and allowing tactical commanders the opportunity to understand the risks and make the appropriate risk-based decision (“go”, “no-go”, “go-despite-risk”) [28]. Knowing the potential threats, possible intent, and the targeting capabilities used in an attempt to disclose, deny, degrade, disrupt, or destroy information that affects operational success contributes to the cybersecurity risk management process. Additionally, knowing the range of potential effects from non-adversarial threat sources can benefit the overall assessment and help select from available control measures.

The threat characteristics model chosen for this study is outlined in Table 5 and the range of effects scale is shown in Table 6. If the UAS does not come with a valid Quick Look Vulnerability Assessment Report (Q-VAR) or NAVAIR Cyber Risk Assessment (CRA), then the overall UAS threat level selected will mimic the predicted impact level. These two scales will be tailored to fit the UAS CRMDM.

Table 5. Characteristics of Adversary Capability. Source: [25].

Qualitative Values	Semi-Quantitative Values		Description
	Score Range	Count	
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Table 6. Range of Effects for Non-adversarial Threat Sources. Source: [25].

Qualitative Values	Semi-Quantitative Values		Description
	Score Range	Count	
Very High	96-100	10	The effects of the error, accident, or act of nature are sweeping, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are extensive, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are wide-ranging, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are limited, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are minimal, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], and involving no critical resources.

UAS cybersecurity threat vectors relate to system vulnerabilities [25]. A sound assessment of each particular UAS is necessary to document known system vulnerabilities, weaknesses, and potential vectors for exploitation. Documenting and assessing the vulnerabilities and calculating the severity of each must be included in the risk assessment. POR UASs should come with a CRA or Q-VAR. UASs, especially smaller COTS systems, come with proprietary hardware and software that may render the vulnerability assessment

difficult and require more specialized assessments. Vulnerability, or red-team, testing is a proven methodology to determine if a particular UAS has vulnerabilities. Vulnerabilities must be identified and mitigated with the results used as input for the equation prior to conducting the cybersecurity risk calculation, or the results will be inaccurate. Entities such as the Defense Innovation Unit (DIU) Rogue Squadron and the Joint Vulnerabilities Assessment Branch (JVAB), under the authority of Naval Air Systems Command, may provide detailed assessments to the tactical teams. The UAV System Cyber-Security Threat Model [11] provides a generic outline of known possible UAS vulnerabilities based on laboratory studies and prior documented incidents. These vulnerabilities will be used as the vulnerability components in Equation 1. Additionally, as indicated in Equation 1, vulnerabilities are mitigated in one of two ways: removal or addressed using a competent security control. Reducing the vulnerability factor, or increasing the security control factor, are arguably the only components in the risk equation that can be manipulated by the system owner or operator. The vulnerability assessment scale chosen as a template for this study is outlined in Table 7. Table 7 does not offer an approach to assess the entire spectrum of vulnerabilities nor the myriad potential security control implementations. For example, it does not provide the correct value for a very high vulnerability that has a relevant security control fully implemented. This leaves too much interpretation with the tactical team and needs to be clarified for UAS assessments. The UAS CRMDM will address this challenge.

Table 7. Vulnerability Severity. Source: [25].

Qualitative Values	Semi-Quantitative Values		Description
	Score Range	Score	
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

The impact level shown in the risk assessment formula captures the characteristics of the threats that could adversely impact the mission, personnel, or equipment if exposed to a threat event [25]. The impact is a fixed numerical value that is assigned upon determining the level of impact that the unauthorized disclosure or compromise of any CIA component would have. The high water mark will be used to assign the correct impact value to the UAS, in the exact same way as assigned in FIPS 199 [22]. The impact assessment scale used in this research is shown in Table 8 below, which will be tailored to align with the CRMDM [25].

Table 8. Likelihood of Threat Event Resulting in Adverse Impacts. Source: [25].

Qualitative Values	Semi-Quantitative Values		Description
	Score Range	Score	
Very High	96-100	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

The overall level of risk will be determined on a similar scale, and modified to facilitate a straight-forward calculation, as derived from the threat, vulnerability, and impact tables. The threat, vulnerability, and impact values will be calculated to create an overall risk value. During the risk determination, very low risk equates to negligible adverse effects for the mission, personnel, or equipment [25]. Low risk will yield limited adverse effects, moderate risk levels will begin to show serious effects, and high risk may produce catastrophic adverse effects on the mission, personnel, or equipment [25]. Finally, calculated risk in the very high range indicates the potential for multiple catastrophic failures impacting the mission [25]. The overall risk scale from SP 800-30 shows the qualitative and semi-quantitative values assigned to each risk level in Table 9.

Table 9. Assessment Scale—Level of Risk. Source: [25].

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

The values listed in Tables 5 through 9 indicate two ways to calculate risk (e.g., qualitative, semi-quantitative). The calculation used in the CRMDM will calculate the semi-quantitative values to derive a qualitative value for each assessment. Transposing the accepted NIST IS descriptions and values will help forge the actual UAS CRMDM in the next section.

B. UAS CYBERSECURITY RISK MANAGEMENT DECISION MATRIX (CRMDM)

The UAS CRMDM has been derived using the framework outlined in FIPS 199, FIPS 200, and NIST SP 800–30 using similar values and descriptions with slight modification. Three individual scales will be used to assess, calculate, and assign semi-quantitative threat, vulnerability, and impact values used to produce an overall CRMDM risk score. The risk score will land on one of the four risk assessment zones. The zones will provide tactical commanders with a current cybersecurity risk snapshot that can be quickly communicated back up the operational and strategic chain-of-command. Once communicated, the appropriate commander would determine if the assessed UAS platform is a proper fit for the mission, if an alternative platform would yield a lower cybersecurity risk, or if the mission should not include sUAS at all. This determination would rest with the assigned Combatant Commander. Tailoring each scale into three logical matrices is the next logical step in the CRMDM creation.

1. Threat Matrix

According to NIST SP 800–30, threats are “any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an IS via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service” [25]. Table 10 illustrates a proposed threat matrix that can be used by the strategic or operational staff intelligence cells for CRMDM applications. The table provides the threat value to the tactical teams for inclusion into the overall risk calculation. Friendly force intelligence must have an accurate threat assessment that is tangible and proven. If no threat assessment is available, then the impact scale will be used to drive the threat scale. For example, without the strategic or operational threat assessment, a mission that could result in certain adverse impacts would yield a semi-quantitative factor of 10 on impact and the equivalent score on the threat scale. The lower the impact score, the lower the overall threat score used for the overall risk determination. Each description and semi-quantitative factor in Table 10 is directly transposed from the associated SP 800–30 scale.

The overall qualitative values are the products of accurately assessed threats or driven by the impact matrix when no assessments are provided. Severe values result from a very sophisticated adversary, who is well funded, and has the opportunity, intent and capabilities to conduct multiple, successful, and continuous attacks. Such results would earn a semi-quantitative factor of 10 that would be used in the overall risk calculation at the end of the assessment. High qualitative values with a somewhat sophisticated level of capability, have resources available, and demonstrates intent to conduct multiple threat events would earn an 8 on the threat matrix factorial. Moderately experienced adversaries, with available resources, and the opportunity to support multiple attacks would yield a 5 on the threat matrix. Finally, threats with limited expertise, resources, and opportunities to conduct multiple attacks on UAS earn a 2 on the threat matrix scale.

Table 10. UAS CRMDM Threat Scale. Adapted from [25].

UAS Threat Matrix		
Qualitative Values	Semi-Quantitative Factor	Description [25]
Severe	10	The regional adversary has a <u>very sophisticated</u> level of UAS exploitation expertise, is well resourced, and can generate opportunities to support multiple, successful, and continuous UAS CIA attacks.
High	8	The regional adversary has a <u>sophisticated</u> level of UAS exploitation expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	5	The adversary has <u>moderate</u> UAS exploitation expertise, resources and opportunities to support multiple successful attacks.
Low	2	The adversary has <u>limited</u> UAS exploitation expertise, resources and opportunities to support multiple successful attacks.

While the language in the “Description” column relies heavily on the language in SP 800–30, the qualitative values deviate from SP 800–30 to reflect the same wording used at the strategic and operational level.

The next factor in the overall risk equation is the vulnerability and security control component.

2. Vulnerability and Security Control Matrix

Table 11 illustrates a concise UAS vulnerability scale and considers the availability of security controls to mitigate the overall vulnerability risk in the CDRMM equation. The vulnerability and security control matrix use the same semi-quantitative factor and description as seen in SP 800–30. The qualitative values deviate from SP 800–30 to produce four distinct categories versus five in the SP 800-30.

According to NIST SP 800–30, vulnerabilities are “a weakness in an information system, system security procedure, internal controls, or implementation that could be exploited by a threat source” [25]. The vulnerability matrix is the source of the $\frac{\text{Vulnerability}}{\text{Security Control}}$ factor in the overall UAS risk assessment. This factor is the most operator, or blue force, influenced component in the entire UAS CRMDM. It is important to discuss the two methods of influencing the vulnerability factor. The first way is to completely remove the vulnerability, which would not require the use of a security control. The second method is to incorporate a tested security control to reduce the potential of an adversary exploiting the known vulnerability. NIST SP 800–53 lists a variety of tested security controls that can be leveraged to lower the semi-qualitative values.

Vulnerabilities that are assessed to be in the severe category are openly exposed, exploitable, and could result in severe UAS impacts to confidentiality, integrity, or availability. Vulnerabilities in the high qualitative value are of high concern based on exposure, ease of exploitation, and the severity of potential impacts effecting the UAS CIA elements. Moderately assessed vulnerabilities are also of moderate concern based on their exposure, lower effort to exploit, and overall severity of CIA influencing factors. Low vulnerability threats are deemed of minor concern and have been mitigated. The only mitigations that can reduce severe, high and moderate vulnerabilities are to completely remove the vulnerability or fully implement proven security controls. The third and final factor in the risk equation is to determine the overall impact if the CIA was compromised.

Table 11. UAS Vulnerability and Security Control Matrix.
Adapted from [25].

UAS Vulnerability and Security Control Matrix		
Qualitative Values	Semi-Quantitative Factor	Description [25]
Severe	10	The UAS vulnerability could result in severe impacts. Security Control (SC) Deduction: Fully implemented SC or vulnerability removed receives a semi-quantitative score of 2.
High	8	The UAS vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Security Control (SC) Deduction: Fully implemented SC or vulnerability removed receives a semi-quantitative score of 2.
Moderate	5	The UAS vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Security Control (SC) Deduction: Fully implemented SC or vulnerability removed receives a semi-quantitative score of 2.
Low	2	The UAS vulnerability is of minor or negligible concern. Security Control (SC) Deduction: Fully implemented SC or vulnerability removed receives a semi-quantitative score of 2.

While the language in the “Description” column relies heavily on the language in SP 800–30, the qualitative values deviate from SP 800–30 to reflect the same wording used at the strategic and operational level.

3. Impact Matrix

As defined in SP 800–30, “the level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability” [25]. The impact to UAS CIA exploitation can be shown via a straightforward metrics, as illustrated in Table 12, that can be correlated with the confidentiality of information flowing through the UAS, the impact to integrity of the information, or the overall availability of information produced by the UAS. The major requirement when determining the overall impact is critically assessing the level of damage that the unauthorized exposure, modification, or denial of UAS data or information could potentially impose on the mission, equipment, and personnel involved.

Severe impact is impact that is almost certain to have adverse effects on the mission, equipment or personnel. High impact is highly likely to result in adverse impact. Moderate impact is somewhat likely to cause adverse effects and low impact determinations are assessed to be those that are unlikely to produce any adverse impacts. Two examples of impact factors include the ISR information classification level and the adversary’s knowledge that a UAS is active in a sensitive area. Impact calculations should take precedence when determining the threat semi-quantitative values in the absence of a threat assessment from higher authority. The mission impact is a reasonable substitute if the threat is unknown or capabilities are unclear.

The last step is to calculate the overall risk score using the UAS CRMDM.

Table 12. UAS Impact Matrix. Adapted from [25].

UAS Impact Matrix		
Qualitative Values	Semi-Quantitative Factor	Description [25]
Severe	10	If the UAS threat event is initiated or occurs, it is almost certain to have adverse effects on the mission, equipment, or personnel.
High	8	If the UAS threat event is initiated or occurs, it is highly likely to have adverse effects on the mission, equipment, or personnel.
Moderate	5	If the UAS threat event is initiated or occurs, it is somewhat likely to have adverse effects on the mission, equipment, or personnel.
Low	2	If the UAS threat event is initiated or occurs, it is unlikely to have adverse effects on the mission, equipment, or personnel.

While the language in the “Description” column relies heavily on the language in SP 800–30, some wording has been changed or added.

4. Cybersecurity Risk Management Decision Matrix

According to NIST SP 800–30, “risk is a function of the likelihood of a threat event’s occurrence and potential adverse impact should the event occur” [25]. Risk associated with the unauthorized disclosure of UAS information, the loss of confidence in UAS information, or loss of the UAS itself are the major concerns of UAS risk-based assessments. Assessing each factor (i.e., threats, vulnerabilities, impacts) leads to an overall risk calculation that should be used prior to launch, and specifically during the selection of specific UAS platforms for each mission.

Table 13 outlines the proposed UAS CRMDM that is adapted from NIST SP 800–30. Each calculated value comes from multiplying the threat score, vulnerability (less security control) score, and impact scores together. Severe risk overall equates to multiple severe or catastrophic adverse effects on the UAS mission, the UAS, personnel, supporting or supported commands, or the United States. Severe risk values (800–1,000) could be

expected to introduce multiple adverse effects [25]. High risk (500–640) indicates that a successful threat event could adversely or catastrophically impact the mission, asset, personnel, associated units, or the nation [25]. Moderate risk (250–400) indicates the potential risk to UAS operations could result in serious adverse effect on the mission, asset, personnel, units, or the United States [25]. Finally, low risk (8–200) equates to limited effects on the five aforementioned consumers or equipment during UAS operations [25].

Table 13. UAS Cybersecurity Risk Management Decision Matrix.
Adapted from [25].

UAS Cybersecurity Risk Management Decision Matrix		
Qualitative Values	Semi-Quantitative Factor	Description [25]
Severe	800-1000	Severe risk means that a threat even could be expected to have multiple severe or catastrophic adverse effects on UAS operations, assets, individuals, other organizations, or the Nation.
High	500-640	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on UAS operations, assets, individuals, other organizations, or the Nation.
Moderate	250-400	Moderate risk means that a threat event could be expected to have a serious adverse effect on UAS operations, assets, individuals, other organizations, or the Nation.
Low	8 - 200	Low risk means that a threat event could be expected to have a limited adverse effect on UAS operations, assets, individuals, other organizations, or the Nation.

While the language in the “Description” column relies heavily on the language in SP 800–30, some wording has been changed or added.

A color-coded chart that uses the calculated UAS CRMDM score that facilitates an opportunity for decision makers to rapidly determine UAS safety of flight is illustrated in Table 14. The proposed UAS CRMDM Fly/No-Fly scale offers an efficient decision approach to commanders at all levels of operation. Table 13 was created using the combination of all possible values from the individual threat, vulnerability, and impact scores. This is only a proposed recommendation and it remains up to the tactical commander to accept the risks in context with the mission. Low-risk assessments shown in green on the fly/no-fly scale offer the largest footprint of opportunity. Tactical operators should mitigate vulnerabilities by removing them or implementing security controls. The moderate-risk scores are shown in yellow and represent more risk than green, but less than the high-risk represented in orange. Moderate-risk scores should only be used if the commander determines the benefits outweigh risks. High-risk scores should not be considered safe for operations and only used for absolutely necessary UAS. The high and severe risks will almost certainly produce a weakened or compromised CIA triad and yield devastating results. Severe risk scores should result in the decision process to consider alternate options or assets to conduct the mission. Severe risk is risk that cannot be mitigated and is highly likely to result in the loss of mission, equipment, or life.

Table 14. Proposed UAS Cybersecurity Risk Management Decision Matrix Fly/No-Fly Scale.

UAS Cybersecurity Risk Management Decision Matrix Fly/No-Fly Scale															
Threat	Vulnerability	Impact	Risk	Threat	Vulnerability	Impact	Risk	Threat	Vulnerability	Impact	Risk	Threat	Vulnerability	Impact	Risk
2	2	2	8	5	2	2	20	8	2	2	32	10	2	2	40
2	2	5	20	5	2	5	50	8	2	5	80	10	2	5	100
2	5	2	20	5	5	2	50	8	5	2	80	10	5	2	100
2	2	8	32	5	2	8	80	8	2	8	128	10	2	8	160
2	8	2	32	5	8	2	80	8	8	2	128	10	8	2	160
2	2	10	40	5	2	10	100	8	2	10	160	10	2	10	200
2	10	2	40	5	10	2	100	8	10	2	160	10	10	2	200
2	5	5	50	5	5	5	125	8	5	5	200	10	5	5	250
2	5	8	80	5	5	8	200	8	5	8	320	10	5	8	400
2	8	5	80	5	8	5	200	8	8	5	320	10	8	5	400
2	5	10	100	5	5	10	250	8	5	10	400	10	5	10	500
2	10	5	100	5	10	5	250	8	10	5	400	10	10	5	500
2	8	8	128	5	8	8	320	8	8	8	512	10	8	8	640
2	8	10	160	5	8	10	400	8	8	10	640	10	8	10	800
2	10	8	160	5	10	8	400	8	10	8	640	10	10	8	800
2	10	10	200	5	10	10	500	8	10	10	800	10	10	10	1000
Low Risk - Safe to Fly				Moderate Risk - Benefit Outweighs Risk				High Risk - Operational Necessity Only				Severe Risk - Do Not Fly			

Having derived the UAS CRMDM from existing federal guidance applied to COTS UAS, the next phase in this study is to demonstrate its utility, provide some counter-arguments, and explore its validity. This is done by comparing alternatives using a realistic scenario.

IV. CRMDM EXAMPLE AND ALTERNATIVE COURSE OF ACTION (COA) ASSESSMENT

The versatility of sUASs for military training, ISR, and combat applications reduces human exposure, provides unique surveillance perspectives, and sharpens tactical capabilities. In an age when threats reside in every domain, it is vital to reduce the risk to mission, protect limited assets, and provide a heightened level of safety for the operators. To meet these goals, advanced TTPs must be able to span multiple domains with emphasis on meeting the commander's objectives through economy of force, security of assets, and safeguarding personnel. The UAS CRMDM should help provide the commander an opportunity to methodically assess available assets. Using the CRMDM in a fictitious, yet realistic, scenario will demonstrate its potential utility and provide face validity.

Examining alternatives to the CRMDM will solidify the product of this effort and potentially justifies a tool in UAS missions that is long overdue. This chapter will offer three alternatives and a rebuttal to each. In the next section, the UAS CRMDM will be used in a step-by-step example.

A. UAS CRMDM SCENARIO

This section uses the proposed UAS CRMDM in a scenario to highlight its application in tactical, operational, and strategic UAS missions. The operational level UAS effort is currently being conducted by Major Gonzalo Santiago, United States Army, for his thesis titled "Cybersecurity Risk Management Process for Unmanned Aerial Systems (UAS) Operation" [29]. The scenario takes the threat assessment from the operational commander and includes it in a UAS CRMDM to calculate overall risk. The calculation is returned to the operational commander to assess if the available UAS ISR assets should be used based on their cybersecurity risk assessment score.

The current scenario is shown in Figure 12. One strategic commander, two operational commanders, and four tactical units are ordered to "defend national interests by defeating the current threat in all domains, deter and defeat any adversarial aggression,

effectively operate in cyberspace, and reduce risks to the operating forces in the Area of Operations (AOR)” [29].

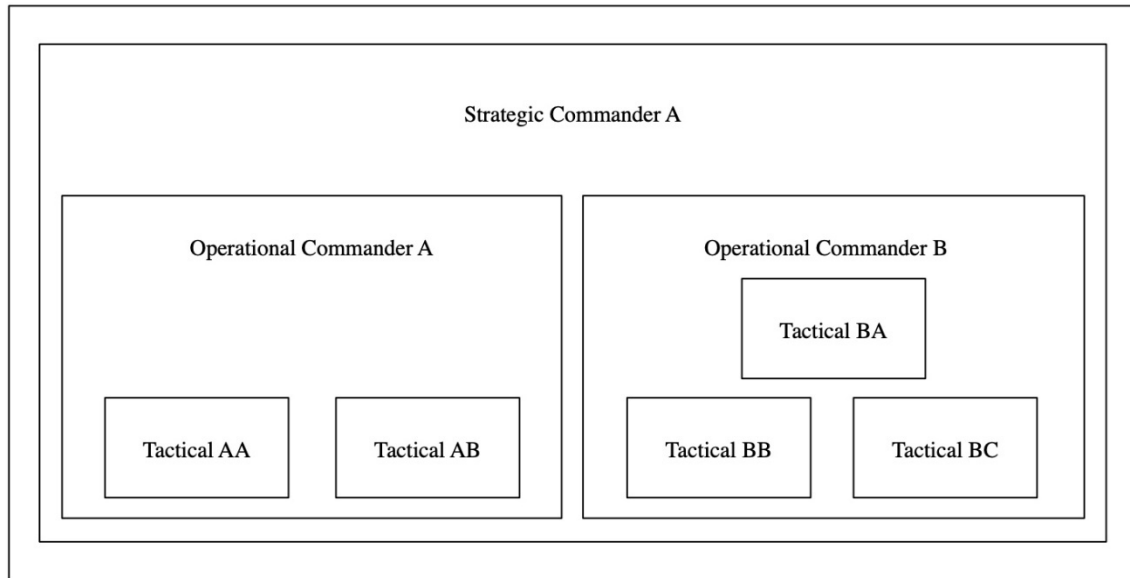


Figure 12. AOR Organization. Adapted from [29].

The operating environment is complex and a threat is identified that threatens the national interests [29]. The threat is capable of disrupting freedom of maneuver in cyberspace and indicates an increased level in violent extremist activities [29]. The extremists operate in small cells scattered throughout the AOR [29]. The cyber threat assessment is characterized as “a mid-level nation state actor with sophisticated understanding of advanced penetration techniques, is well-resourced, and intends to conduct cyber espionage to disrupt multiple organizations critical resources” [29]. Strategic Commander A provided tactical units AA and BB with the cyber threat assessment and an order to conduct a UAS risk assessment on available assets [29]. The threat assessment is illustrated in Table 15.

Table 15. Scenario Problem Framing. Adapted from [29].

Event Title: Cyber Threat Impact to UAS Operations.
Purpose: Determine the impact of the AOR's Cyber Threat to UAS Operations.
Cyber Threat Characteristics: Mid-level nation state cyber actor with sophisticated understanding of advanced penetration techniques, well-resourced, able to replicate and execute hacking examples found online with intent to conduct cyber espionage and/or disrupt multiple organization's key resources.

Tactical Units AA, BA, and BB provide ISR support with Group 1 and 2 UASs [29]. Only Units AA and BB are fully functional and each has a different type of small ISR UAS in the inventory. Unit AA is operating COTS Drone-A and it has a current NAVAIR Q-VAR on file. Unit BB is operating COTS Drone-B and also possesses a NAVAIR approved Q-VAR.

Drone-A consists of a quadcopter airframe and a GCS laptop. The Drone-A ISR payload consists of a 1080p high-resolution camera, and the aircraft has a five-hour flight time. The drone possesses three vulnerabilities that are listed in the in the Q-VAR, two of which are mitigated by security controls. The first vulnerability is a forced login telnet authentication bypass, which is mitigated by installing vendor-supplied patches. The second vulnerability is an unprotected telnet service running on the aircraft. Filtering the media access card traffic and hiding the SSID mitigate both the first and second vulnerabilities. The third vulnerability is susceptibility to a deauthentication attack, which is not mitigated due to encryption not being available on the C2 software.

Drone-B has three identified vulnerabilities. Drone-B is also a quadcopter airframe and only uses a handheld GCS that operates on C-band (4Ghz to 8 GHz) for C2 and uses Wi-Fi b/g/n standards for payload data. Drone-B has a 480p camera and has a three-hour flight time. The Wi-Fi is susceptible to eavesdropping; however, WPA2 encryption mitigates the risk. C-band C2 communications are prevalent in the AOR due to the large number of devices operating between 4–8Ghz. No mitigation is available for the loss of C2 with Drone-B if the RF spectrum is saturated.

A baseline RF assessment was completed by the UAS support element and it was determined that the RF spectrum was not saturated in the C-Band spectrum. No new RF

signatures were identified during the baseline and no additional threats were identified. Wi-Fi traffic was assessed as average for the area and not anticipated to interfere with Wi-Fi based systems.

The threat assessment puts the threat at an 8 (using Table 10), or high, due to the adversary’s sophisticated understanding, advanced penetration techniques, and abundant financial resources to conduct an attack. Drone-A has a known vulnerability that is of high concern due to the possible loss of mission critical confidentiality and availability, which also score an 8 on the vulnerability matrix (Table 11). Drone-B scored a 2 on the vulnerability assessment due to the assessed baseline and vulnerability mitigations. The impact assessment scored a 5 due to potential loss of equipment availability for both UASs. Both UASs do not store data onboard and adequate encryption is used to prevent the loss of confidentiality and compromised data integrity. Table 16 provides the assessed values of Drone-A and Table 17 shows the assessed values of Drone-B. Figure 13 illustrates where each drone landed on the UAS CRMDM Fly/No-Fly scale.

Table 16. Scenario Tactical UAS Drone-A CRMDM Results

Tactical AA Drone-A Assessment				
Threat	Vulnerability	Impact	Overall Risk	Tactical Commander Notes
8	8	5	320 (Moderate)	Requested platform despite higher threat assessment due to optical camera quality and increased endurance.

Multiply the threat, vulnerability, and impact score to calculate the overall risk.

Table 17. Scenario Tactical UAS Drone-B CRMDM Results

Tactical BB Drone-B Assessment				
Threat	Vulnerability	Impact	Overall Risk	Tactical Commander Notes
8	2	5	80 (Low)	Requested as a secondary platform if Drone-A risk is not acceptable to the overall mission.

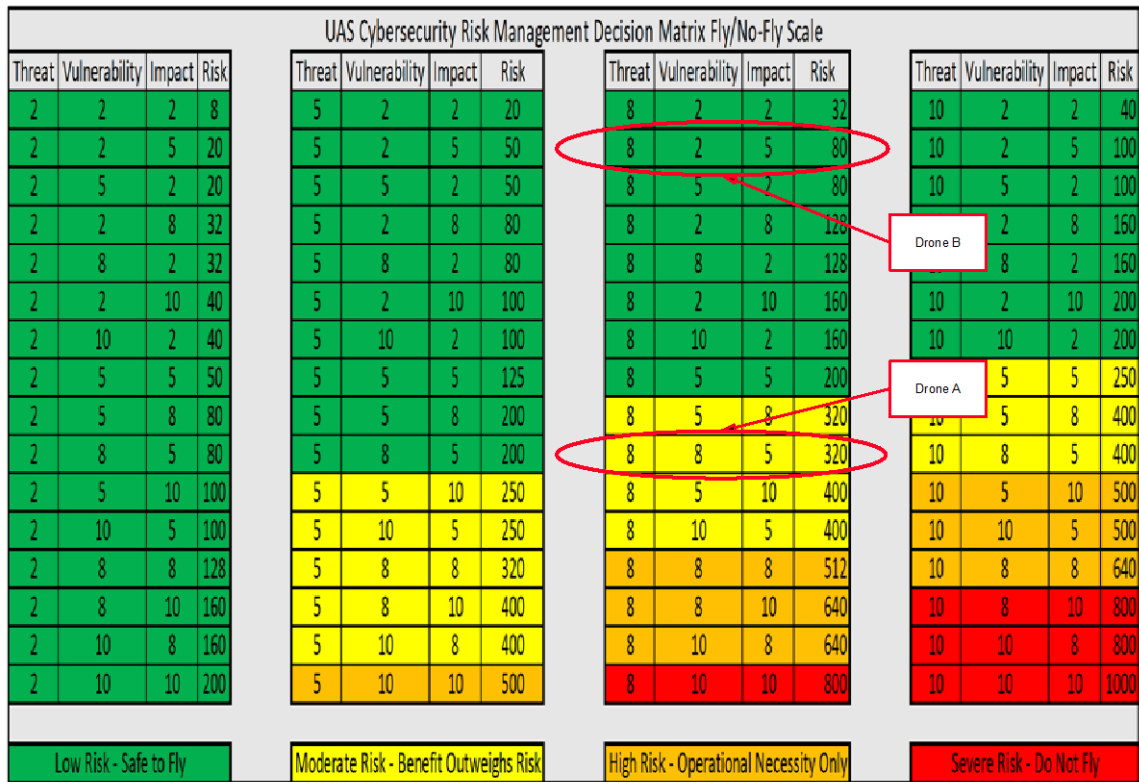


Figure 13. Scenario UAS Cybersecurity Risk Management Decision Matrix Fly/No-Fly Scale.

The UAS CRMDM is not a decisive directive, but it is a risk assessment tool that feeds the overall decision process. In this scenario, the higher-risk platform was requested as the primary platform due to two external factors, a better camera and longer endurance,

despite the higher risk assessment. The UAS CRMDM ensures that cybersecurity is incorporated into the decision cycle, but cybersecurity alone is not the ultimate decision authority.

Both UAS CRMDM risk assessments were submitted up the chain of command for review and approval. The UAS teams are awaiting feedback and authority to operate the mission. The next section compares the past, present, and potential future COAs resulting from the existing UAS cybersecurity processes.

B. ALTERNATIVES TO THE UAS CRMDM

A sound method to explore the validity of this research is to discuss alternative COAs from other processes or procedures that are relevant and can address the thesis original thesis questions. The first element of the counter-arguments, also addressed by the thesis reasoning, is: What processes and considerations should a UAS CRMDM incorporate for tactical UAS commanders? The second element to consider, is: what non-UAS cybersecurity frameworks can be incorporated into the UAS CRMDM? Three alternative processes will be compared with the UAS CRMDM. The first alternative is to do nothing and not implement any processes that incorporate cybersecurity into the tactical UAS operation determination. The second COA is to continue with the current non-POR UAS exemption approval process. The final COA to examine is to completely halt the DoDs use of all UAS.

1. Unrestricted Use of UAS without Cybersecurity

One alternative to the UAS CRMDM is to allow the unrestricted use of UAS without adopting a plan to mitigate cybersecurity threats on the systems. The time to assess cyber threat actors would be reduced at the strategic, operational, and tactical levels. This option would significantly increase speed of UAS deployment and substantially lighten the load on agencies conducting UAS Q-VARs and CRAs. More analysis time would be turned over to the individual units without the need for impact assessments. The immediate benefits would be quickly achieved, but the entire CIA spectrum would be left unassessed and potentially exploitable to the adversary's advantage.

The DoD was operating UASs without an integrated UAS cybersecurity process, found the lack of a cybersecurity process unacceptable, and issued a general ban on the operation of all COTS UASs on May 23, 2018 [30]. The ban was followed by a UAS procurement and operational exception process on June 1, 2018 [30]. The COTS UAS procurement and operational ban is still in effect unless an approved exemption is reviewed and approved. The ban and exemption process demonstrate the DoDs desire to implement a top-down UAS cybersecurity process. Failing to implement cybersecurity provided adversaries with an open invitation to exploit critical United States DoD missions. The lack of a UAS cybersecurity process was deemed insupportable and put UASs at risk, which created the current non-POR UAS exemption process.

2. Continue the Current Non-POR UAS Exemption Process

The second alternative COA is to continue using the agency specific non-POR UAS exemption approval process. Each service is permitted to create its own waiver process within specific bounds. The specific agency process for the Department of the Navy (DoN) illustrated in Figure 14 shows the current path required for all COTS DoN prior to approval to operate. The environment determination can flow in one of two ways; uncontrolled or controlled environments.

All uncontrolled/benign, or operational, environment UAS operational waiver requests go directly to the Office of the Secretary of Defense (OSD) board. The board is held either bi-weekly or monthly to determine if a UAS waiver is granted or denied. For the DoD, controlled and benign environment requests are handled through the use of a consumer-completed questionnaire. The questionnaire provides Naval Air Systems Command (NAVAIR) the opportunity to understand four key concepts considered cybersecurity. The first factor is the environment of which the UAS will operate. The second factor is the existence or type of C2 or payload encryption used on the subject UAS. The third factor covers the way data is stored either using real-time transmission to an off-system location or if the data is stored onboard. The fourth factor is that all systems must be recovered and accounted for at the end of each event.

The Naval Waiver Board (NWB) consists of representatives from nine commands and is chaired by NAVAIR Cyber. The board includes; the Office of the Secretary of Defense Chief Information Officer (DoD CIO); Department of the Assistant Secretary of the Navy for Research, Development, Test and Evaluation (DASN RDT&E); the United States Marine Corps (USMC) for USMC requests; Naval Postgraduate School; Office of the Chief of Naval Operations, Warfare Integration (OPNAV N9I) for Navy requests, Naval Sea Systems Command (NAVSEA), Space and Naval Warfare Systems Command (SPAWAR); and the Naval Research Laboratory (NRL). The results and recommendations are briefed bi-weekly in an executive brief to the Under Secretary of the Navy and Assistant Secretary of the Navy for Research, Development, and Acquisition where a waiver determination is approved, denied, or referred to OSD.

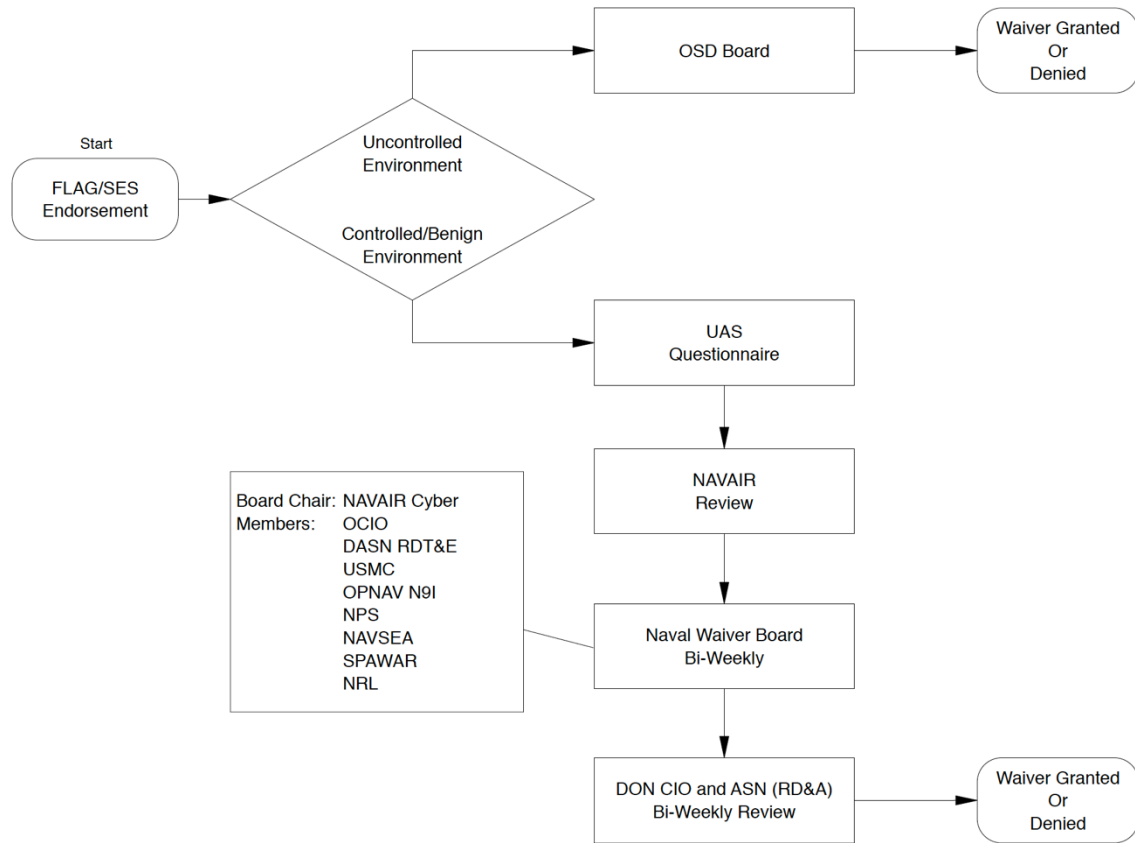


Figure 14. DoN Non-POR UAS Exemption Approval Process

Counter-arguments to using the NWB are now presented. The NWB is not a solidified process, but is constantly evolving. The NWS is an extremely high-level short-term fix to the DoD RMF, which is addressed in the proposed UAS CRMDM. If the NWB process is needed each time a command requires the use of UAS, then it could be at least two weeks before a waiver determination is complete. The UAS questionnaire is not listed as a component of the Uncontrolled Environment OSD board, which is arguably a higher risk environment. It is unclear if the DoD RMF drives the operational risk assessment work-flow. The controlled and benign environment UAS questionnaire only addresses C2 and payload confidentiality, the operating environment, data storage types, and recovery. The core principles of the DoD RMF include a six-step process that are all addressed in the streamlined UAS CRMDM. Categorizing the system is completed using the CIA trifecta. Vulnerability identification is completed, as well as security control selection and

implementation, using the RMF-centric Q-VAR and CRA processes by technical analysts. System risk analysis is conducted using a tailored NIST SP 800–30 semi-quantitative and qualitative scale. The scale is easily understandable and modifiable based on the level of risk the commander is willing or as directed by higher authority to accept. Willingness to accept risk is part of the DoD RMF, which is subsequently difficult when analyzing technology at the tactical level without the right tool [31]. The UAS CRMDM includes an assessment of non-adversarial threats into the calculus that are used to determine UAS vulnerabilities during extreme atmospheric or RF saturation. System and military unit-specific standard operating procedures may provide additional guidance; however, the UAS CRMDM will also provide additional considerations for the overall risk.

3. Abandon DoD Use of Commercial or Non-POR UAS

The final alternative COA examined is to completely abandon the use of commercial or non-POR UASs in the DoD. This is obviously not a wise decision, especially when considering the DoD allocated over \$3 billion to purchase over 3,200 new UASs for 2019 [7]. Additionally, exposure and availability of manned assets providing real-time long-endurance ISR will never match the DoDs UAS ISR capability or flexibility. UASs help keep the warfighter safe by identifying hazardous conditions, IED locations, adversarial movements, and enemy postures without putting United States military lives out front first.

The institution of the waiver process shortly after issuing the COTS UAS ban can be viewed as recognition that a total ban on COTS sUASs is impractical.

V. RECOMMENDATIONS AND FUTURE WORK

A. RECOMMENDATIONS

The need for cybersecurity has driven military organizations to develop processes and procedures that mitigate risk to their mission, equipment, and personnel while providing optimal functionality. Computing systems and devices that fail to incorporate TTPs designed to protect the CIA triad are subject to a challenging array of potential threats that may expose critical data, maliciously alter sensitive data, and significantly reduced system availability. This situation is ever present, regardless of the organization and IS.

Generally, cybersecurity processes help protect IT assets that are, usually, physically safe due to location but still require risk assessment and mitigation to logically function when incorporated into globally shared networks. If wings were installed on a computer, it wirelessly transmitted critical information between the computer and a remote-control station, add a tactical operator in control, and introduce the new asset into adversary airspace, we would have, essentially, a UAS. Federally mandated frameworks were created to protect information, assets, and personnel using federal systems. DoD is now placing cybersecurity ownership at the command level by using the NIST and DoD RMF to mitigate risk and understand the subject system's cybersecurity posture. All federal systems are mandated to incorporate the RMF into their cyber-system life cycle, which does not preclude UASs. It was only recently that UASs attracted attention due to discovered vulnerabilities, without appropriate security controls, that motivated senior leadership to act. Although the current NWP enables continued operations, it is not putting risk assessment techniques where they belong at the strategic, operational, and tactical levels. The proposed UAS CRMDM developed in this effort addresses this issue.

The UAS CRMDM provides a cybersecurity decision support tool for use at the tactical level. The tool not only provides a process to assess various UASs suites, but also provides tactical commanders and operators a cybersecurity culture enabler relevant to other risks they already manage. The breadth of the UAS CRMDM is significant, as it addresses each pillar of the CIA triad and incorporates individual threat, vulnerability, and

impact assessments into a risk equation. This tailorable process can be adjusted or modified to give the tactical and operational decision makers the ability to understand what risks they are willing to accept and where the boundary exists for what risks they cannot accept. The straightforward calculations make the UAS CRMDM a useful utility when trying to determine the right platform, for the specific mission, under time constraints. The research presented here demonstrates that cybersecurity processes can be tailored to fit the highly relied upon, mission critical, and environmentally adaptable, UASs. An additional benefit is that the matrix can be used by personnel who are not cybersecurity experts.

Even though the underlying risk model used as the basis for this work is not rigorously proven, it provides the foundation for a solid heuristic based process that would appear to be superior to any alternatives currently available, to enable the tactical operator to consider cybersecurity risk as an element of mission planning and execution.

B. FUTURE WORK

Four specific needs were identified during the course of this study. The first is a supply-chain process that assesses UASs before acquisition. The need is apparent, since we still have cybersecurity issues with acquired COTS UASs. Processes and procedures are already in place with POR acquisitions; however, the need for incorporating a supply-chain cybersecurity process does not only exist for POR systems, but should include COTS systems as well. Every level of the product life cycle should contain a process that helps mitigate and reduce unnecessary risk to the mission. One example of an effort that can support the supply-chain cybersecurity process is the Supply Chain Risk Analysis and Management System (SCRAMS) that was demonstrated by Strategic Mobility 21 Incorporated during the Joint Interagency Field Experimentation 19-3 at Camp Roberts, CA, from April 29 through May 3, 2019. SCRAMS is a software suite that can identify risk factors such as fake system components, fraudulent shippers, unsuccessful manufacturers, or other user-defined risk factors.

The second process that should be considered is a more rigorous validation of the UAS CRMDM. Providing this tool to a tactical unit would help flush out additional considerations and help the end-user fine-tune the process. Although an example scenario

is provided, it is important to validate the process with operating tactical units and adjust as necessary. Incorporating the culture of cybersecurity into tactical military units, faces barriers to acceptance, as with any organizational change; however, reliance on systems in the cyber domain depends on adequate processes to protect shared information and C2 networks.

The third future work consideration is the creation of a computer or portable device application that implements the CRMDM model. Such an application can allow the operator to conduct the UAS CRMDM and submit it to the tactical commander for incorporation into the decision cycle. Creating a simple, user-friendly step-by-step Android or IOS based application would offer the framework to the tactical consumer in a form that is similar to that used for other processes, such as organizational and operational risk management. Exploring these areas of future work would help determine how UASs can be used securely in a military context.

The fourth, and final consideration is to systematically collect data on the performance of CRMDM model to adjust the performance of the general equation. As previously stated, the equation used is neither supported by theory nor the result of any formal consensus. However, if a generally agreed upon equation for cybersecurity becomes available one should be able to easily incorporate the new model into the CRMDM, potentially improving its performance.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- [1] J. Keller, “Iran–U.S. RQ-170 incident has defense industry saying ‘never again’ to unmanned vehicle hacking,” *Military & Aerospace Electronics*, May 3, 2016. [Online]. Available: <https://www.militaryaerospace.com/articles/2016/05/unmanned-cyber-warfare.html>
- [2] *Cybersecurity Policy*, NSPD 54/HSPD 23, The White House, Washington, DC, USA, 2008. [Online]. Available: <https://fas.org/irp/offdocs/nspd/nspd-54.pdf>
- [3] C. Kube, “Russia has figured out how to jam U.S. drones in Syria, officials say,” *NBC News*, April 10, 2019. [Online]. Available: <https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931>
- [4] M. Rouse, “Internet of things (IoT),” *IoT Agenda*. Accessed March 19, 2019. [Online]. Available: <https://Internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>
- [5] Deputy Secretary of Defense, “Unmanned Aerial Vehicle Systems Cybersecurity Vulnerabilities,” official memorandum, Department of Defense, Washington, DC, USA, May 23, 2018.
- [6] L. Dormehl, “The history of drones in 10 milestones,” *Digital Trends*, September 11, 2018. [Online]. Available: <https://www.digitaltrends.com/cool-tech/history-of-drones>
- [7] D. Gettinger, “Summary of drone spending in the FY 2019 defense budget request,” *Cent. Study Drone Bard Coll.*, April 2018. [Online]. Available: <https://dronecenter.bard.edu/files/2018/04/CSD-Drone-Spending-FY19-Web-1.pdf>
- [8] UAS Task Force, “Unmanned Aircraft System Airspace Integration Plan,” Department of Defense, March 2011. [Online]. Available: <https://doi.org/1-7ABA52E>
- [9] K. Hartmann and C. Steup, “The vulnerability of UAVs to cyber attacks—An approach to the risk assessment,” in *2013 5th Cyb. Conf. on Cyb. Confl., Tallinn*, 2013, pp. 1–23. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6568373>
- [10] E. Pastor, J. López Rubio, and P. Royo, “A Hardware/Software Architecture for UAV Payload and Mission Control,” in *IEEE Aerosp. Elect. Syst. Mag.*, vol. 22, 2006, pp. 1–8. [Online]. Available: https://www.researchgate.net/publication/224057242_A_HardwareSoftware_Architecture_for_UAV_Payload_and_Mission_Control

- [11] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in 2012 IEEE Int. Conf. Technol. Homel. Secur., November 2012, pp. 585–590. [Online]. Available: <https://doi.org/10.1109/THS.2012.6459914>
- [12] Northrop Grumman, "RQ-4 Global Hawk Maritime Demonstration System," 2007. [Online]. Available: <http://www.northropgrumman.com/Capabilities/RQ4Block10GlobalHawk/Documents/GHMD-New-Brochure.pdf>
- [13] UST, "Antennas & microwave products." Accessed March 20, 2019. [Online]. Available: <https://www.unmannedsystemstechnology.com/category/supplier-directory/electronic-systems/antennas-microwave-products/>
- [14] Insitu, "Scan Eagle," 2017. [Online]. Available: https://www.insitu.com/images/uploads/pdfs/ScanEagle_SubFolder_Digital_DU032817.pdf
- [15] K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani, "Unmanned aerial vehicle smart device ground control station cyber security threat model," 2013 *IEEE Int. Conf. Technol. Homel. Secur.*, 2013, pp. 722–728. [Online]. Available: <https://doi.org/10.1109/THS.2013.6699093>
- [16] Insitu, "Operator's Handbook Unmanned Aerial Systems," Bingen, WA, USA: Insitu Inc., 2008.
- [17] Federal Information Security Modernization Act of 2014, Pub. L. No. 131–256 § 3552, 128 Stat. 3074. 2014. [Online]. Available: <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text>.
- [18] L. Zhang, F. Restuccia, T. Melodia, and S. M. Pudlewski, "Learning to detect and mitigate cross-layer attacks in wireless networks: framework and applications," 2017 *IEEE Conf. Commun. Netw. Secur.* 2017, pp. 1–9. [Online]. Available: <https://ieeexplore.ieee.org/document/8228631>
- [19] S. Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," in *RAST 2013 - Proc. 6th Int. Conf. Recent Adv. Sp. Technol.*, 2013, pp. 795–800. [Online]. Available: <https://doi.org/10.1109/RAST.2013.6581320>
- [20] A. Milne, "Common sources of interference." RF Venue. Accessed March 20, 2019. [Online]. Available: <https://www.rfvenue.com/blog/2014/12/14/common-sources-of-interference>
- [21] D. Storm, "Drones infected with malware can drop from the sky or be hijacked for surveillance," Computer World. Accessed March 20, 2019. [Online]. Available: <https://www.computerworld.com/article/2876912/drones-infected-with-malware-can-drop-from-the-sky-or-be-hijacked-for-surveillance.html>

- [22] National Institute of Standards and Technology, “Federal Information Processing Standards (FIPS) 199, Standards for security categorization of federal information and information systems,” Gaithersburg, MD, USA, 2004. [Online]. Available: <https://csrc.nist.gov/publications/detail/fips/199/final>
- [23] National Institute of Standards and Technology, “Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems,” Gaithersburg, MD, USA, 2006. [Online]. Available: <https://csrc.nist.gov/publications/detail/fips/200/final>
- [24] National Institute of Standards and Technology, “NIST Special Publication 800–53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations,” Gaithersburg, MD, USA, 2013. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- [25] National Institute of Standards and Technology, “NIST Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments,” Gaithersburg, MD, USA, 2012. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- [26] E-Government Act of 2002, Pub. L. No. 107-347. 2002. [Online]. Available: <https://www.govinfo.gov/app/details/PLAW-107publ347>
- [27] K. V. Impe, “Simplifying risk management,” SecurityIntelligence. Accessed May 24, 2019. [Online]. Available: <https://securityintelligence.com/simplifying-risk-management/>
- [28] B. T. Williams, “The joint force commander’s guide to cyberspace operations,” *Jt. Force Q.*, vol. 73, no. 2, pp. 12–19, 2014. [Online]. Available: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf?ver=2014-04-01-122156-563%5Cnhttp://ndupress.ndu.edu/Media/News/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/
- [29] G. Santiago, “Cybersecurity risk management process for unmanned aerial systems (UAS) operations,” M.S. thesis manuscript in preparation, Dept. of Information Sciences, NPS, Monterey, CA, USA, 2019.
- [30] Deputy Secretary of Defense, “Delegation of Authority to Approve Exemptions for Using Commercial-Off-The-Shelf Unmanned Aerial Systems in Support of Urgent Needs,” official memorandum, Department of Defense, Washington, DC, USA, June 1, 2018.
- [31] *Risk Management Framework (RMF) for DoD Information Technology (IT)*, DoD Instruction 8510.01, Department of Defense, Washington, DC, USA, 2014. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California