DOD Quantum AI

Kevin McFarland
01290240

Old Dominion University - School of Cybersecurity
CYSE 495: Spring 2024
Dr. Josephine Leach

Department of Defense Quantum AI
Document Version: 1.1
Date: 10 April 2024

Table of Contents

Introduction

The current state of cybersecurity and Risk Management Frameworks have a running countdown clock. That clock can be attributed to the future of computing with the development of Quantum Computing. The application of Quantum Computing once fully developed will not just affect the Department of Defense, though they likely will have access to it first, but every other network and system out there. Current cryptographic protocols that take upwards of years to break or crack, once Quantum Computing enters the picture, will only take minutes to solve. In the same breath Artificial Intelligence will only enhance what Quantum Computing's capabilities are. Regardless of that future the Department of Defense under the U.S. Cyber Command has started a new cyber strategy by working with other government agencies. This is due to recent cyber attacks from both China and Russia. Here will be an exploration into how a RMF within DOD will look like with Quantum Computing and Artificial Intelligence in the future.

The Department of Defense already employs Artificial Intelligence in certain capacities, and it is a fair assumption that DOD will be one of the first with access to Quantum Computing.

> The Cybersecurity and Infrastructure Security Agency (CISA) warns that this will be a widespread challenge that companies and governments must face. "As this technology advances over the next decade, quantum computing is increasing risk to some encryption methods widely used to protect customer data, complete business transactions, and secure communications," notes CISA (Walker).

At least some government agencies already have this on their radar, but NIST needs to get in gear to begin addressing the future challenges of RMF for Quantum Computing and Cryptology.

This system will be a Top-Secret level Department of Defense Quantum Leap - Artificial Intelligence Data Systems (DOD QL-AIDS (pronounced Kool-aid)) for use in data sharing and retrieval from databases and data assets. The ability for the DOD and other agencies to share data assets and information in near instantaneous speeds might only benefit their operations. And since U.S. Cyber Command has already currently adjusted their Cybersecurity posture to work jointly with other federal agencies, this seems like a logical future step. There should be a machine learning component for extrapolation and problem solving in getting the data requested based on whatever query parameters are used. This means a particular bit to me, I am a retired Navy Chief, I've always been called to service. I've decided to start a second career in Cybersecurity to continue that call to service, and if I can contribute or provide ideas like this to the people that matter, then maybe my efforts will matter.

As far as an encryption system goes, lets also refer to initiatives already in the works. One such type, according to Dilki Rathnayake, a guest author at *Tripwire.com*, describes it as such, "Quantum Cryptography, more accurately described as Quantum Key Distribution (QKD), is a quantum-safe method introduced to exchange key exchange between two entities. It works by transmitting photons, which are polarized light particles, over a fiber optic cable. QKD protocols are designed according to the principles of quantum physics (Rathnayake)." Others are also preparing and developing policy to prepare for a quantum future. According to Walker,

> "Government agencies are already preparing enterprises for Q Day. Currently, work is ongoing to develop quantum-secure cryptography. The National Institute of Standards and Technology (NIST) is in the process of selecting the encryption algorithms to become part of its planned post-quantum cryptographic (PQC) standard (Walker)."

The NIST has started a PQC Standardization project in order to produce Quantum-resistant or quantum-safe cryptography standards and is urging businesses in the industry to begin preparations as well.

Report - System Categorization

System Categorization Form			
System Name	Department of Defense Quantum Leap - Artificial Intelligence Data Systems DOD QL-AIDS		
Version Number	v.3.13		
Table 1 List of RMF Team Members			
Role	**Name**	**Organization**	
PM	Amber Rose	Program Management Team	
Administrator	Nate Dogg	Quantum Admin Team	
Team Member 1	Tim Bradley	Junior Admnitrator	
Team Member 2	Colin Goring	Junior Admnitrator	
Team Member 3	Scott Foxy	Junior Admnitrator	
Auditor	Karen Gonzo	Senior Program Analyst	
Category of System		Sensitive	
Releasability of Information		Top Secret	
Any interconnected Systems/External Services which could elevate impact level?		Department of Defense Artificial Intelligence Systems	
Does clearance/Need to know requirement for data vary by role/personnel?		No, all Top Secret and above, for all positions.	

Information Type	Confidentiality / Breach Impact	Integrity / Breach Impact	Availability / Breach Impact
Privacy / PII	High	High	High
Financial	Low	Low	Low
Information Management	High	High	High
System and Network Monitoring	High	High	High
Information Sharing	High	High	High
Information Security	High	High	High
Continuity of Operations	High	High	High
Contingency Planning	High	High	High
Service Recovery	High	High	High
Security Management	High	High	High
Program Monitoring	High	High	High
Strategic Planning	High	High	High
Workforce Planning	High	High	High
Help Desk Services	High	High	High
Services Acqusition	High	High	High
System Development	High	High	High
Research and Development	High	High	High
OVERALL SYSTEM SECURITY CATEGORY		High	

Report - System Plan

Test Plan

Department of Defense Quantum Leap - Artificial Intelligence Data Systems
321704
DOD QL-AIDS

Document Version: 3.13
Date: 01 APR 2024

Prepared By:
Kevin McFarland

SYSTEM TEST PROFILE

SYSTEM NAME	Department of Defense Quantum Leap - Artificial Intelligence Data Systems
VERSION	1.1
SYSTEM ID	321704
SYSTEM STATUS	DOD QL-AIDS
TEST DATES	Pending
TESTING SITE	Pending
HOSTING FACILITY	DOD QCTAMS (Quantum Computer and Telecommunications Area Master Station}
NETWORK	Defense Information Systems QSIPRNet (Quantum Secret Internet Protocol Router Network)
PROGRAM MANAGER	Amber Rose
POC NAME AND CONTACT	Kevin McFarland (757)-867-5309

1.1. TEST OBJECTIVES

DATE COMPLETION	MILESTONE	DELIVERABLES/COMMENTS
TEST EVENT 1: INSTALL, CONFIGURE, AND TEST (DOD Quantum AI)		
1 MAY 2024	QUANTUM DATACENTER	VALIDATE QUANTUM DATACENTER IMPLEMENTATION
1 MAY 2024	ARTIFICIAL INTELLIGENCE SERVICES	VALIDATE ARTIFICIAL INTELLIGENCE SERVICES IMPLEMENTATION
TEST EVENT 2: INSTALL, CONFIGURE, AND TEST APPLICATIONS		
TBD	PROGRAM ONBOARDING	VALIDATE PROGRAM ONBOARDING PROCESS AND PROCEDURES - CREATED AND VETTED THROUGH TESTING
TEST EVENT 3: INSTALL, CONFIGURE, AND TEST CRYPTO		
TBD	QUANTUM CRYPTO	TEST QUANTUM KEY DISTRIBUTION (QKD)
TBD	QUANTUM SIPR DATA EXCHANGE	TEST QUANTUM SIPR DATA RETRIVAL DURING CONTROLLED AUDIENCE PREVIEW

2. ROLES AND RESPONSBILITIES

NAME	RESPONSIBILITY
Moira McFly	TEST DIRECTOR
Nate Dogg	PROGRAM ADMIN
Rick Grimes	ARCHITECT
Daryl Dixon	CONSULTANT

3. TEST EVENT ARHITECTURE

3.1. CONFIGURATION

AI CPU Core started and operational IAW DODAI 10X.XX. DOD QSIPR servers started and operational IAW DODID 20.3X.XX.

3.2. TEST STRATEGY

TEST SCHEDULE

EVENT/PHASE	LOCATION	TEST TIME FRAME	DURATION
TEST EVENT 1	DOD QCTAMS	TBD	UNTIL AI IS STABLIZED
TEST EVENT 2	DOD QCTAMS	TBD	UNTIL MIGRATION OF AI ONTO QUANTUM SIPR IS VERIFIED
TEST EVENT 3	DOD QCTAMS	TBD	UNTIL AI DATA RETRIVAL IS VERIFIED
TEST EVENT 4	DOD QCTAMS	TBD	UNTIL INTERAGENCY ACCESS IS VERIFIED VIA QKD

4. HARDWARE LIST

4.1. TABLE HARDWARE DIAGRAM

DEVICE NAME	VERSION	PURPOSE	ONSITE OR VM
Defense Information Systems QSIPRNet		WEB SERVER	ONSITE
ARTIFICIAL CENTRAL CORE	DODPT-9	AI CPU	ONSITE

5. SOFTWARE LIST

5.1. TEST SOFTWARE

5.2. TABLE SOFTWARE

APPLICATION	VERSION	PURPOSE	ONSITE OR VM
DOD AI	DODPT-9	DATA RETRIEVAL AND MACHINE LEARNING	ONSITE
QUANTUM DATABASE NETWORK	QSIPR	ENABLES ACCESS TO DATA ASSETS BETWEEN AGENCIES	ONSITE

6. CHECKLIST

6.1. TABLE CHECKLIST

CHECKLIST ITEM	COMPLETION STATUS	ESTIMATED START DATE	ESTIMATED END DATE
Complete traditional security checklist IAW PQC	TBD	TBD	TBD
Ensure system numbers are accurate	TBD	TBD	TBD
Ensure topology is acceptable	TBD	TBD	TBD
Ensure Recommendation Summary is included	TBD	TBD	TBD
Ensure that a detailed description of test and timeline have been well represented	TBD	TBD	TBD
Ensure POCs are listed	TBD	TBD	TBD

Report – Hardware and Software

Hardware/Firmware Lists					
Device Name	Manufacturer	Model Number	Firmware Version	Purpose/Function	Virtual Server
QSIPRNet	COTS	Various	v1.2.3	Web and Database server	No
AI Central Core	Raytheon	DODPT-9	v4.5.6	Artificial Intelligence	No
QKD	Lockheed	QC45	v7.8.9	Quantum Key Distribution	Yes

Report - Security Control & Test Results

Control	Control Assessed	Status
CA-1: Policy and Procedures	Policies established	Compliant
CA-2: Control Assessments / Security Assessments (Version differences)	Controls have been assessed	Compliant
CA-3: Information Exchange / Information System Connections	Reviewed information exchange	Compliant
CA-4: Security Certification	Reviewed security certificaitons	Compliant
CA-5: Plan of Action and Milestones	Reviewed POAM	Compliant
CA-6: Security Authorization	Reviewed security authorizations	Compliant
CA-7: Continuous Monitoring	Reviewed continous monitoring strategy	Compliant

Report - POAM

POAM							
System / Project Name	DOD QL-AIDS	POC Name	Kevin McFarland				
System Type	Quantum AI Database	POC Phone	(757) 867-5309				
Date	4/1/2024	POC Email	mcfarlak@dod.mil				
POAM ID	**Control Vulnerability Description**	**Scheduled Completion Date**	**Milestones with Completion Dates**	**Status**	**Comments**	**Devices Affected**	**Recommendations**
3300	AI Hardline Cutoff	6/5/2024		Pending	Immediate Attention	AI CPU Core	Verify Hardline disconnects AI from network.
3301	Quantum Password Compexity	6/27/2024		Pending	Algorithms being revised	Interagency Assets	WIP
3302	Connection agreement	7/1/2024		Pending	In the works	All Areas	National Security Council sign off on revised interagency access agreeements.
3303	Fire extinguisher	5/5/2024		Pending	Planned	Server room	Place where necessary for Class 'C' Fires.
3304	Change control Log	5/6/2024		Pending	In the works	Environment	WIP

Summary Timeline

- Step 1: Prepare Phase: (Approximately 6 mo.)

Tasks	Primary Responsibility	Supporting Roles
Organizational Level		
Task P-1 Risk Management Roles	U.S. Cyber Command DOD Deputy Assistant Secretary DOD Security Officer	Authorizing Official – Professor X Risk Executive – Magneto Cyber Command Security Officer – Scott Summers
Task P-2 Risk Management Strategy	U.S. Cyber Command	Risk Executive – Magneto Chief Information Officer – Jean Grey Cyber Command Security Officer – Scott Summers
Task P-3 Risk Assessment - Organization	Risk Executive – Magneto Cyber Command Security Officer – Scott Summers DOD Security Officer	DOD Deputy Assistant Secretary Authorizing Official – Professor X Raytheon and Lockheed
Task P-4 Common Control Identification	Cyber Command Security Officer – Scott Summers DOD Security Officer	DOD Deputy Assistant Secretary Risk Executive – Magneto DOD Deputy Assistant Secretary Common Control Provider – Juggernaut U.S. Cyber Command
Task P-5 Continuous Monitoring Strategy - Organization	Risk Executive – Magneto	DOD Deputy Assistant Secretary DOD Security Officer Raytheon and Lockheed U.S. Cyber Command Authorizing Official – Professor X
System Level		
Task P-6 Mission or Business Focus	Raytheon and Lockheed	DOD Deputy Assistant Secretary U.S. Cyber Command Steward – Beast

		Cyber Command Security Officer – Scott Summers DOD Security Officer
Task P-7 System Stakeholders	Raytheon and Lockheed U.S. Cyber Command	DOD Deputy Assistant Secretary Risk Executive – Magneto Steward – Beast Cyber Command Security Officer – Scott Summers DOD Security Officer Chief Acquisition Officer – Gambit
Task P-8 Asset Identification	U.S. Cyber Command	Authorizing Official – Professor X Raytheon and Lockheed Steward – Beast Cyber Command Security Officer – Scott Summers DOD Security Officer System Administrator – Nate Dogg
Task P-9 Authorization Boundary	Authorizing Official – Professor X	DOD Deputy Assistant Secretary Raytheon and Lockheed Steward – Beast Cyber Command Security Officer – Scott Summers DOD Security Officer System Administrator – Nate Dogg
Task P-10 Information Types	U.S. Cyber Command Steward – Beast	System Security Officer – Wolverine Raytheon and Lockheed DOD Security Officer
Task P-11 Information Life Cycle	DOD Security Officer U.S. Cyber Command Steward – Beast	DOD Deputy Assistant Secretary Raytheon and Lockheed -Security Architect -Privacy Architect -Enterprise Architect -System Security Engineer -Privacy Engineer

Task P-12 Risk Assessment - System	U.S. Cyber Command -System Security Officer -System Privacy Officer	Risk Executive – Magneto Authorizing Official – Professor X Raytheon and Lockheed Steward – Beast
Task P-13 Requirements Definition	Raytheon and Lockheed Steward – Beast U.S. Cyber Command -System Privacy Officer	Authorizing Official – Professor X DOD Security Officer DOD Deputy Assistant Secretary System Security Officer Chief Acquisition Officer Security Architect Privacy Architect Enterprise Architect
Task P-14 Enterprise Architecture	Raytheon and Lockheed -Security Architect -Privacy Architect -Enterprise Architect	DOD Deputy Assistant Secretary Authorizing Official – Professor X Cyber Command Security Officer – Scott Summers DOD Security Officer Steward – Beast U.S. Cyber Command
Task P-15 Requirements Allocation	Security Architect Privacy Architect System Security Officer System Privacy Officer	DOD Deputy Assistant Secretary Authorizing Official – Professor X Raytheon and Lockheed Cyber Command Security Officer – Scott Summers DOD Security Officer U.S. Cyber Command
Task P-18 System Registration	U.S. Cyber Command	Raytheon and Lockheed DOD Deputy Assistant Secretary System Security Officer System Privacy Officer

- Step 2: Categorize Information Systems: (Approximately 2 mo.)

Tasks	Primary Responsibility	Supporting Roles
Task C-1 System Description	U.S. Cyber Command	Authorizing Official – Professor X Steward – Beast System Security Officer System Privacy Officer
Task C-2 Security Categorization	U.S. Cyber Command Steward - Beast	Risk Executive – Magneto DOD Deputy Assistant Secretary Authorizing Official – Professor X Cyber Command Security Officer – Scott Summers DOD Security Officer U.S. Cyber Command
Task C-3 Security Categorization Review and Approval	Authorizing Official – Professor X DOD Security Officer	Risk Executive – Magneto DOD Deputy Assistant Secretary Cyber Command Security Officer – Scott Summers

- Step 3: Select Security Controls: (Approximately 5 mo.).

Tasks	Primary Responsibility	Supporting Roles
Task S-1 Control Selection	U.S. Cyber Command Common Control Provider	Authorizing Official – Professor X Steward - Beast
Tasks S-2 Control Tailoring	U.S. Cyber Command Common Control Provider	Authorizing Official – Professor X Steward – Beast System Security Engineer Privacy Engineer System Security Officer System Privacy Officer
Task S-3 Control Allocation	Security Architect Privacy Architect System Security Officer System Privacy Officer	DOD Deputy Assistant Secretary Authorizing Official – Professor X Raytheon and Lockheed Cyber Command Security Officer – Scott Summers DOD Security Officer

Task S-4 Documentation of Planned Control Implementations	U.S. Cyber Command Common Control Provider	Authorizing Official – Professor X Steward – Beast System Security Engineer Privacy Engineer System Security Officer System Privacy Officer
Task S-5 Continuous Monitoring Strategy – System	U.S. Cyber Command Common Control Provider	Risk Executive – Magneto DOD Deputy Assistant Secretary Cyber Command Security Officer – Scott Summers Authorizing Official – Professor X Steward – Beast Security Architect Privacy Architect Systems Security Engineer Privacy Engineer System Security Officer System Privacy Officer
Taks S-6 Plan Review and Approval	Authorizing Official – Professor X	Risk Executive – Magneto DOD Deputy Assistant Secretary DOD Security Officer Cyber Command Security Officer – Scott Summers Chief Acquisition Officer

- Step 4: Implement Security Controls: (Approximately 4 mo.)

Tasks	Primary Responsibility	Supporting Roles
Task I-1 Control Implementation	U.S. Cyber Command Common Control Provider	Steward – Beast Security Architect Privacy Architect Systems Security Engineer Privacy Engineer System Security Officer System Privacy Officer Enterprise Architect System Administrator – Nate Dogg
Task I-2	U.S. Cyber Command Common Control Provider	Steward – Beast Security Architect

Update Control Implementation Information		Privacy Architect Systems Security Engineer Privacy Engineer System Security Officer System Privacy Officer Enterprise Architect System Administrator – Nate Dogg

- Step 5: Assess Security Controls: (Approximately 6 mo.)

Tasks	Primary Responsibility	Supporting Roles
Task A-1 Assessor Selection	Authorizing Official – Professor X	DOD Deputy Assistant Secretary DOD Security Officer Cyber Command Security Officer – Scott Summers
Task A-2 Assessment Plan	Authorizing Official – Professor X Control Assessor – Karen Gonzo	DOD Security Officer Cyber Command Security Officer – Scott Summers U.S. Cyber Command Common Control Provider Steward – Beast System Security Officer System Privacy Officer
Task A-3 Control Assessments	Control Assessor – Karen Gonzo	Authorizing Official – Professor X U.S. Cyber Command Common Control Provider Steward – Beast Cyber Command Security Officer – Scott Summers System Security Officer System Privacy Officer
Task A-4 Assessment Reports	Control Assessor – Karen Gonzo	U.S. Cyber Command Common Control Provider System Security Officer System Privacy Officer
Task A-5 Remediation Actions	U.S. Cyber Command Common Control Provider	Authorizing Official – Professor X DOD Security Officer Cyber Command Security Officer – Scott Summers Risk Executive – Magneto

		Steward – Beast Systems Security Engineer Privacy Engineer System Security Officer System Privacy Officer
Task A-6 Plan of Action & Milestones	U.S. Cyber Command Common Control Provider	Steward – Beast System Security Officer System Privacy Officer DOD Security Officer Cyber Command Security Officer – Scott Summers Chief Acquisition Officer Control Assessor – Karen Gonzo

- Step 6: Authorize Information System: (Approximately 7 mo.)

Tasks	Primary Responsibility	Supporting Roles
Task R-1 Authorization Package	U.S. Cyber Command Common Control Provider	System Security Officer System Privacy Officer DOD Security Officer Cyber Command Security Officer – Scott Summers Chief Acquisition Officer Control Assessor – Karen Gonzo
Task R-2 Risk Analysis and Determination	Authorizing Official – Professor X	Risk Executive – Magneto DOD Deputy Assistant Secretary DOD Security Officer
Task R-3 Risk Response	Authorizing Official – Professor X	Risk Executive – Magneto DOD Deputy Assistant Secretary DOD Security Officer U.S. Cyber Command Systems Security Engineer Privacy Engineer System Security Officer System Privacy Officer
Task R-4 Authorization Decision	Authorizing Official – Professor X	Risk Executive – Magneto Chief Information Officer – Jean Grey Cyber Command Security Officer – Scott Summers

		DOD Security Officer
Task R-5 Authorization Reporting	Authorizing Official – Professor X	U.S. Cyber Command Steward – Beast System Security Officer System Privacy Officer DOD Deputy Assistant Secretary DOD Security Officer

- Step 7: Monitor Security Control: (Approximately 6 mo.)

Tasks	Primary Responsibility	Supporting Roles
Task M-1 System and Environment Changes	U.S. Cyber Command Common Control Provider DOD Deputy Assistant Secretary DOD Security Officer	Risk Executive – Magneto Authorizing Official – Professor X Steward – Beast System Security Officer System Privacy Officer
Task M-2 Ongoing Assessments	Control Assessor – Karen Gonzo	Authorizing Official – Professor X U.S. Cyber Command Common Control Provider Steward – Beast System Security Officer System Privacy Officer DOD Deputy Assistant Secretary DOD Security Officer
Task M-3 Ongoing Risk Response	Authorizing Official – Professor X U.S. Cyber Command Common Control Provider	Risk Executive – Magneto DOD Deputy Assistant Secretary Cyber Command Security Officer – Scott Summers Authorizing Official – Professor X Steward – Beast Security Architect Privacy Architect Systems Security Engineer Privacy Engineer System Security Officer System Privacy Officer
Task M-4	U.S. Cyber Command Common Control Provider	Steward – Beast System Security Officer

Authorization Package Updates		System Privacy Officer DOD Deputy Assistant Secretary DOD Security Officer
Task M-5 Security and Privacy Reporting	U.S. Cyber Command Common Control Provider DOD Deputy Assistant Secretary DOD Security Officer	System Security Officer System Privacy Officer
Task M-6 Ongoing Authorization	Authorizing Official – Professor X	Risk Executive – Magneto Chief Information Officer – Jean Grey Cyber Command Security Officer – Scott Summers DOD Deputy Assistant Secretary DOD Security Officer
Task M-7 System Disposal	U.S. Cyber Command	Authorizing Official – Professor X Steward – Beast System Security Officer System Privacy Officer Risk Executive – Magneto DOD Deputy Assistant Secretary DOD Security Officer

Background

While the news is recently abundantly full of stories related to Artificial Intelligence (AI), it is still considered an emerging technology. The knowledge of how it works and operates is not entirely grasped. The basics of AI includes a program using machine learning algorithms to approximate the intelligence of a human being. Bernd W. Wirtz, the Chair of Information and Communication Management at the German University of Administrative Sciences Speyer, Germany, provides this basic description of AI,

> While the current understanding of AI refers to "the capability of a computer system to show human-like intelligent behavior characterized by certain core competencies, including perception, understanding, action, and learning," recent developments in AI indicate that the latter is about to become superior to human intelligence (Wirtz et al).

The recognition of those developments of AI becoming superior to human intelligence is catching on. Government organizations are beginning to realize the potential benefits of AI, and it is being used in certain limited capacities. Wirtz again,

> Public organisations and governments increasingly acknowledge the great potential of AI for enhancing organisational performance, governmental decision-making, public service delivery and public value creation by incorporating AI into their organisational or governmental strategy and investing heavily in it (Wirtz et al.).

There are risks with AI's use and implementation, for instance terrorists, criminals, or authoritarian states and other bad actors. There is also the idea that an AI could go "rouge" and be outside the control of, or making decisions without humans. Quoting Wirtz again,

> the primary risk is that "AI systems can escape the control and understanding of their operators and programmers", which is commonly referred to as the "black box" problem

> of AI, in which decisions are made that can no longer or only partially be retraced by humans (Wirtz et al).

Losing control of an AI or its misuse could lead to detrimental effects in healthcare, energy systems, military and civil defense, communications and more. But none of this directly refers to use of AI under a Risk Management Framework (RMF), but there is an entity that has already begun to just that, NIST.

NIST AI RMF

The National Institute of Standards and Technology has developed an AI RMF, *NIST AI 100-1*. The RMF is built around "functions;" these functions organize AI RMF into for main categories. "Govern" is the first, applies to all functions, is for establishing policies, procedures, accountability and establishing a culture that understands risk. Next is "Mapping", which provides context on how to measure and manage risk with AI. Followed next by "Measure" of AI's to analyze, assess, benchmark and monitor the risk thereof. Lastly "Manage" prioritizes and treats risk.

For this particular project, the Department of Defense Quantum Leap - Artificial Intelligence Data Systems (DOD QL-AIDS), will have to undergo the RMF processes of both *NIST 800-37 Rev 2* and *NIST AI 100-1*. Utilizing both RMF processes will ensure that all applicable best practices and policies are implemented to protect both the system and protect humanity. Of course, there are the regular concerns of data protection and confidentiality, integrity and availability (CIA), but then there are the additional concerns of harm to people, organizations and ecosystems due to AI. The main sticking point according to *NIST AI 100-1,* AI risks or failures that are not well-defined or adequately understood are difficult to measure quantitatively or qualitatively. The inability to appropriately measure AI risks does not imply that

an AI system necessarily poses either a high or low risk (NIST). There are risk related to third-party software, hardware and data, tracking emergent risks, availability of reliable metrics, different stages of the AI lifecycle, inscrutability, and human baseline.

First step in the process will be the prepare phase, starting with identifying all the key players and positions. U.S. Cyber Command as Head of Agency, Jean Grey as Chief Information Officer, Professor X is the Authorizing Official, Magneto as the Risk Executive and myriad of other role assignments with-in U.S. Cyber Command and Quantum Computer and Telecommunications Area Master Station (DOD QCTAMS) the installation location. With those positions filled, a Risk Management Strategy will be developed for risk tolerance with expected outputs. This followed by a risk assessment organization wide considering the totality of risk especially with data exchange on internally and externally owned systems. Also in this prepare phase, a continuous monitoring strategy needs to be developed, but it needs to have two branches. One dedicated to the overall QSIPR enterprise and one dedicated to the AI alone. Raytheon and Lockheed will have a line on the mission along with identifying the system stakeholders. Asset identification will also need to have two branches, one to have hardware and policy in place to "black box" the AI and the other branch for the overall QSIPR enterprise. There should be both and information lifecycle for the data to be transferred within the system and interagency connections, and AI lifecycle stage tracking. The risk assessment of the system will be precarious, especially because of the potential unknowns with AI. The prepare phase finishes out with a system registration in accordance with policy, describing the characteristics of the system and the risk, security and privacy posture.

Next major task in the RMF process would be to Categorize. Develop a system description and document the characteristics. Categorization will be fairly simple, as this is to be

an advanced DOD system, it would be all just Top Secrect so overall categorized as High. Once this document is developed it will need reviewed and approved by U.S. Cyber Command.

The control phase will be a more complicated step as risk will be possibly more unknown due to AI. Controls protecting the QSIPR Enterprise will be fairly standard based on experiences with previous versions of SIPR. The challenge will be with the "AI" side of the house, a "black box" method is not the only measure to take. Governance would come into play here, asking, "(1) What are major risks associated with the development and use of AI? (2) What specific guidelines exist to regulate and govern these risks? (3) How can AI risks and guidelines be categorised and conceptualised?(Wirtz). Baseline controls are a pre-defined set of controls to address the protection needs of the organization, privacy, information and information systems. A lot of these controls will be generated and tailored by the organization, Raytheon, and Lockheed, as this is a highly specialized system. These planned control implementations will be all documented, which allows for traceability prior to and after deployment of both the QSIPR and AI systems. This documentation will be taken to the Authorizing Official Professor X, for plan review and approval to move forward.

Once the controls selection has been approved by the Authorizing Official it will be time to implement controls. DOD QCTAMS will use best practices while implementing controls, including methodologies, concepts and principles related to privacy and security engineering. If any of the identified controls could not be implemented as planned, updates and revisions to the control implementation information will be documented. During this timeframe and leading into the assess phase of the RMF, DOD QCTAMS will also implement the Measure profile from *the NIST AI 100-1*, monitoring, analyzing, assessing, and recording benchmarks of the AI.

Initially the organization will conduct an internal assessment of all systems, after that they will call in the technical experts. There will be two assessment teams, each team experts in each field at play, enterprise RMF and AI RMF. They will be outside of the organization, probably from the private sector as long as they meet the security requirements. Security and privacy assessment plans will come from these external teams, as they are the fields experts. During the assessment, they will be checking to what extent the controls were implemented correctly, operating as intended, and the desired results for the system and organization are displayed. These assessments will happen as early as possible as they are considered developmental testing and evaluation, to validate the plans put forward and approved. Results and recommendations will be compiled into assessment reports, which will be key information for the authorizing official. All recommendations and remediations will be compiled into a Plan of Action and Milestones to resolve all issues in a timely manner.

Conclusion

If properly understood and implemented the RMF for both a Quantum Computing Enterprise and Artificial Intelligence systems in concert will hopefully address all concerns. With the National Institute of Standards and Technology having already addressed RMF for AI, they will only have to update and adjust as that develops. It's Quantum Computing that they are not yet prepared for. Since it is a good chance that the Department of Defense will have first access to Quantum Computing systems, what is the expectation of NIST getting an RMF developed for it in enough time? At least CISA which is also under the purview U.S. Department of Commerce is already aware of the pending challenges. In the meantime, the Department of Defense and U.S. Cyber Command are addressing current cyber security concerns, working in partnership with other federal agencies. Hopefully they will keep in mind the cryptographic concerns related to both AI and Quantum Cryptography. The Quantum SIPR system with Artificial Intelligence data retrieval and extrapolation will help address U.S. Cyber Commands needs for interagency cooperation on the cyber security front. The items listed int eh POAM will be resolved in the next 8 months. Requesting a 24-month continuous authorization to operate approval with a continuous monitoring program in conjunction.

References

Barraza de la Paz JV, Rodríguez-Picón LA, Morales-Rocha V, Torres-Argüelles SV. A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems*. 2023; 11(5):218. https://doi.org/10.3390/systems11050218

Joint Task Force. (2018, December). *Risk management framework for information systems and* ... National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Joint Task Force. (2023, January). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Rathnayake View Profile, Dilki. "The Impact of Quantum Computing on Cybersecurity." *Tripwire*, 3 Apr. 2023, https://www.tripwire.com/state-of-security/impact-quantum-computing-cybersecurity.

Walker, Jonathan. "Quantum Computing Is Coming: How Will It Impact Cybersecurity?" *Entrepreneur*, Entrepreneur Asia Pacific, 14 Nov. 2022, https://www.entrepreneur.com/en-au/technology/quantum-computing-is-coming-how-will-it-impact/439060.