Powering Secure Growth through Compliance, Automation, and Awareness with Mobius Consulting

A Professional Readiness Experiential Program (PREP) Project Effort

----- Authors / Student Project Team Members -----

Taylor Le is a student at George Mason University graduating with a bachelor's degree in information technology with a concentration in Cybersecurity.

----- Industry Participant / Mentor -----

Lashdeep Singh Director of Operations Mobius

William Ogus Technology Solutions Architect Mobius

----- Faculty Member -----

Brian K. Ngac, PhD Instructional Faculty, Dean's Teaching Fellow, & FWI Corporate Partner Faculty Fellow George Mason University's Costello College of Business <u>bngac@gmu.edu</u>

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

Mobius is an award-winning, SBA HUBZone-certified, Woman-Owned Small Business specializing in government contracting and commercial work. We provide solutions in cybersecurity, systems engineering, modeling and simulation, and intelligence analysis. I joined Mobius back in Fall 2024, where I learned the ropes of the organization's infrastructure and security initiatives. I came back in Spring 2025, where I was given more autonomy over my work, as well as trust, which enabled me to make meaningful contributions and strengthen my technical and problem-solving skills. The program provided me with a unique opportunity to tackle real-world security challenges while contributing to the organization's efforts to improve its contract management processes and security awareness.

Business Challenge

Mobius is committed to achieving and maintaining a strong security posture across its operations. As a growing organization working with sensitive government contracts, it must continuously align with evolving cybersecurity standards, including CMMC Level 1 certification. CMMC is a recently mandated framework that aims to protect government contract information processed through information systems. It is a core requirement to bid on government contracts. At the start of my internship, several processes such as NDA/TA document generation and contract funding changes lacked automation and efficiency. Additionally, raising employee awareness about social engineering threats was critical for organizational security.

Activities Done to Address the Business Challenge

CMMC Level 1 Readiness

As Mobius prepares for CMMC Level 1 certification, I contributed to foundational readiness activities aimed at improving compliance with federal cybersecurity standards. This certification is an essential step in being able to bid on future government contracts. These activities involved scoping our information systems, evaluating current processes, and ensuring alignment with the FAR 52.204-21 guidelines. I lead efforts to document and track remediative actions to ensure compliance, which included categories such as access control, identity/authentication, system/information integrity, physical facility protection, and system/communication protection. These contributions helped strengthen Mobius' security baseline and brought the organization closer to certification readiness.



Caption: This is the document used to track our actions taken in the pursuit of CMMC Level 1 compliance.

Phishing Simulation

Each quarter, our security department at Mobius conducts a phishing simulation to test employee awareness and the organization's ability to respond to social engineering threats. In the previous round, we crafted a convincing email impersonating Microsoft's Security Team, warning users of a data leak. The urgent and credible nature of that message prompted users to pause and assess the situation carefully, resulting in fewer compromises. This time, we shifted our approach to test a more casual, less thought-provoking phishing attempt: a generic "Microsoft Teams Voicemail" notification. Despite featuring more obvious red flags, the simplicity and familiarity of the content led to more users clicking without thinking—demonstrating that people are often more vulnerable to routine, loweffort phishing emails than highly sophisticated ones that trigger critical thinking.

You hav	e a voicemail from Frank Privitera				
MS	MicroTeam Voice Support < Microstrategy@aws.mobus.com> To: ⊚ Taylor Le		← Repl	y 🐔 Reply a	➡ ~ 🔗 🔡 … Tue 4/22/2025 12:27 PM
	Dear Taylor,				
	You received new URGENT voicemail through Microsoft Teams from:				
	Franc Privtera				
	Duration: 00:01:22				
	Click the buton below to listen to the mesage:				
	Listen to Voicemail				
	This message was automatically generated by Microsoft Teams Voicemail Service. Do not reply to this email, message z	inloo	<u>k.com</u> for su	pport.	
	← Reply → Forward				

Caption: This is the attack simulation phishing email that was sent out to all users in our organization.

George Mason University Costello College of Business Professional Readiness Experiential Program (PREP) | Page 4 of 6

Workflow Automation for NDA/TAs and Contract Funding Changes

In efforts of streamlining administrative workflows, reducing human-error, and improving tracking capabilities, I led the automation of Mobius' Non-Disclosure Agreement (NDA) and Teaming Agreement (TA) workflows, along with building a process for managing funding changes on our contract management tool. Using Power Automate, Power Apps, Dataverse, Adobe Sign, and Dynamics 365, I developed a unified system that allows the business development department to initiate, track, generate, and process NDAs and TAs through a centralized dashboard. Each agreement type is clearly flagged to enable the department's visibility of status through the process' lifecycle. An automation I developed allowed the NDAs and TAs to be automatically populated and generated through the associated data stored in our database. I also built out a workflow that automatically processes funding changes for auditing purposes. These systems have reduced the processing time, improved data accuracy, and enhanced transparency of our processes.

Dynamics 365	Octane	SANDBOX 🛛 +	7 @ ? @					
E Home			🕑 Share 🗸					
Pinned V	Modification	- MOD 4 - Saved						
ly Work	General Related \checkmark							
b Dashboards								
Activities	Name	- MOD 4						
ompanies	Direction	Incoming	~					
Accounts	Agreement		Q					
Contacts	Modification Number	1						
ontracts Summary	Madification Trees							
Contracts	Modification Type	Funding	\sim					
Line Items	Effective Date	4/29/2025						
Modifications	Mod Status		~					
Modification Lines	Notes	** × ジ × 専 Segoe UI × 11 × B Z U S ♥ × ▲ × 参 田 目 ∈ モ モ 44	+A 99 V V ²					
Labor Details								
Requisitions		Enter text						
Vendor Reviews								
ositions								
Billets								
Workshares								
Staff	Modification Details							
osts	Modification Details							
Rates	Modification Lines	+ New Modification	Line 🖔 Refresh 🗧					
Fee Rates	□ Line Item ↑ ~	Change in Cost Fun 🎽 Change in Fee Fun 🎽 Change in Cost Ceil 🌱 Change in Fee Ceil 👻 C	hange in FFP/T&M ~					
Milestones		\$95.24 \$4.76						
Budgets		\$9.523.81 \$476.19						
tuals		\$952.38 \$47.52						
Actual Costs		3736.30 347.06						
ther Data	Rows: 3							

Caption: This is a modification record, along with a subgrid of related modification line records, which were automatically created when a requisition was approved and completed.

George Mason University Costello College of Business

Professional Readiness Experiential Program (PREP) | Page 5 of 6

Testing Automation - Saved Opportunity · Opportunity ~				Agency Est. Award Date	Pipeline Value	Total Con	vitract Value
Lead to Opportunity Sal Active for 35 days	Qualify	Develop	2	NDA (35 D)	Team	ing Agree	ment
Summary Files Related \vee				Active for 35 days		E ×	
Opportunity information	Import	ant dates		Internal Request For ND	A No Processing	\sim	
Name of Opportunity *	Date In	itiated		Run Flow	Processing		
Testing Automation	Draft R	FP Release Date		Complete Internal Revie	W * Mark complete	\sim	
Description	RFP Rel	ease Date		Send NDA Run Flow	Processing		estions new and stay
Solicitation Vehicle		al to Pursue re Decision			< Nex	t Stage	
>>	Propos	al Bid/No Bid	Pending		tal pane		

Caption: This is an opportunity record, where the Business Development Department can populate the data into our user-friendly dashboard, and automatically generate NDA/TA documents.

Cloud Security Workshop Development

I helped develop and organize a hands-on cybersecurity workshop in collaboration with Mobius and the PREP program, called *Blue Team Security Workshop: Deploy Your Own Security Operations Center (SOC) Lab in the Cloud*, which will be delivered to university students in the upcoming fall semester. The workshop aims to give students real-world experience in the defensive side of cybersecurity by guiding them through the creation of a cloud-based SOC lab using Azure and Sentinel. The students will learn the whole setup and incident remediation process from provisioning virtual machines, setting up analytics workspaces, enabling telemetry collection, writing customer detection rules, and responding to the simulated incidents. Students will walk away with a fully functional SOC lab that can be expanded upon and added to resumes.

Blue Team Security Workshop	*
Lab Infrastructure	
This lab runs in Microsoft Azure with a layered setup that simulates a real- world SOC. We will create virtual machines, connect telemetry, and build detection rules in a cloud environment similar to modern enterprise security.	Microsoft Azure
Microsoft Azure Cloud platform used to host and manage all lab resources.	Resource Group
Resource Group A container that holds services used in the lab.	Log Analytics Workspace Microsoft Sentinel
Log Analytics Workspace Collects, stores, and queries event log data.	Virtual Machine
Microsoft Sentinel Detect, investigate, and respond to threats in real time.	
Virtual Machine System that simulates endpoint behaviors in the lab.	
Virtual Machine System that simulates endpoint behaviors in the lab.	

Caption: This is one of the workshop's slides that goes over the lab infrastructure.

Results & The Positive Impact

- The automated NDA and TA workflows cut down processing time and allowed for greater visibility across departments.
- Our phishing simulation helped measure user awareness, and the training component reinforced secure behavior.
- The improved contract funding workflow process increased data consistency, reduced inefficiency, and supported contract compliance requirements.
- Security action improvements contributed directly to Mobius' ongoing readiness for CMMC Level 1 compliance, allowing them to bid on federal contracts.
- The cloud security workshop is positioned to be a powerful community outreach and hands-on lab to get students excited about the cybersecurity field.

Conclusion

My time at Mobius provided hands-on experience in solving real-world cybersecurity and business process challenges. By leveraging Power Platform technologies and applying cybersecurity principles, I was able to deliver solutions that will scale with the company as it grows. The collaborative environment, combined with the trust and autonomy given to me, enabled meaningful contributions and strengthened my technical and problem-solving skills.

PREP Student Reflection

The PREP experience at Mobius exceeded my expectations. It gave me the opportunity to build and deliver production-grade solutions that directly supported a real business. I grew both technically and professionally – from learning how to automate contract processes using the Power Platform, to working cross-functionally with security, operations, and finance teams. I also gained valuable insight into federal cybersecurity standards like CMMC. This experience not only prepared me for a future in cybersecurity and cloud solutions but also gave me a deeper appreciation for the intersection of technology, compliance, and business efficiency.