System	
PM	
Architect	
Engineering Lead	
Date Created	

Total Score	100	Summary
Maturity	Basic	
Model	C2M2	
Compliant	Yes	
Health Check	Average	

Domains		Criteria Rating Scale											Rating	Weight	Score	Next Steps
	Score	0	1	2	3	4	5	6	7	8	9	10				
Security Controls	Scale	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	10	1	10	
	1	None	Systems are secured by a network-defined boundary; access granted by VPNs; implement ACLs			Bring security internal to the network; lock down systems and components; implement security groups			Implement Defense in Depth		Implement Zero Trust Architecture					
	Note															
	Score	0	1	2	3	4	5	6	7	8	9	10				
Vulnerability Scanning and Assessments	Scale	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	10	1	10	
	1	None	Manual or ad hoc testing of arbitrary components			Automated scanning of system and networks against an established baseline			Continuous scanning of system and network		Adaptive scanning based on machine learning algorithms					
	Note															
	Score	0	1	2	3	4	5	6	7	8	9	10				
Identity and Access Management	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	10	1	10	
	1	None	Enforce basic policies (e.g. password rotation, account lock-outs)				Use federated solutions across multiple systems and sites		Implement multi-factor authentication and just-in-time access		Use biometric and behavioral data to predict and manage access					
	Note															
	Score	0	1	2	3	4	5	6	7	8	9	10				
Cyber Threat Intelligence	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	10	1	10	
	1	None	Receives bulletins as a passive consumer		Participates in the security community (e.g., IARCP, ISC2)			Active participant and subscriber of Federal intelligence feeds			Discover, analyze, and distribute intelligence to the community					
	Note															
	Score	0	1	2	3	4	5	6	7	8	9	10				
Cyber Incident Response	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	10	1	10	
	1	None	Pure reactive incident response		Implementation of a Security Operations Center (SOC)			Executes mitigation solutions, techniques, or tools (e.g., DDOS mitigation, quarantining)			Comprehensive, proactive, and well-funded cyber crimes unit					
	Note															
	Score	0	1	2	3	4	5	6	7	8	9	10				

System Monitoring	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	**10**	1	10	
	1	None	Collect systems logs into a centralized monitoring system and alert based on deviations			Establish a comphrensive baseline; monitor and alert using infrastructure tools (e.g., IDS)			Audit, tune, and perform continuous improvements		Derive threat indicators from existing metrics and predictive analytics				
	Note														
	Score	0	1	2	3	4	5	6	7	8	9	10			
Systems Security Testing	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	**10**	1	10	
	1	None	Manual or ad hoc testing for a subset of components			Formalized security test plans and tools; automated testing			Continuous security testing within a DevSecOps framework and proactive inclusion in development and sustainment life cycles						
	Note														
	Score	0	1	2	3	4	5	6	7	8	9	10			
Vendor Security Management	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	**10**	1	10	
	1	None	Receive and action vendor security bulletins and patch notifications			Performs internal security testing to verify and validate tools prior to inclusion in the system architecture			Collaborate with vendors to proactively identify issues, analyze potential security threats, and discuss future actions						
	Note														
	Score	0	1	2	3	4	5	6	7	8	9	10			
Security Operations Center	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	**10**	1	10	
	1	None	Implement a 3-tier SOC for incident management and response				Establish Tier 4 capability with senior personnel experienced with discovery and analysis techniques (e.g., RCA)			Incorporate Red Team capabilities; perform malware decoding and threat analysis; support the cyber crimes unit					
	Note														
	Score	0	1	2	3	4	5	6	7	8	9	10			
Governance, Risk, and Compliance	Scale	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	**10**	1	10	
	1	None	Aligns with Federal policies for secure systems			Regularly audits system and components; provides training to systems and network teams			Monitor upcoming policy changes, understand system impact, and incorporate necessary updates into project roadmap						
	Note														
Total Score (60 or more = Go, <60 = further work needed)													**100**		100	