Managed IT, Security, & Cloud Services

DRIVING INDUSTRY FORWARD

Cybersecurity Maturity Model Certification (CMMC)

Department of Defense (DoD) requires proof of CMMC compliance to ensure protection of controlled unclassified information (CUI) from nation-state and nefarious actors, while keeping the supply chain running safely. Is your Cybersecurity maturity plan at the desired level to participate in the US government contract bidding process?

As breaches continue to be more commonplace, data infractions have continued to grow as well. In addition, threats to critical government assets also continue to increase in frequency and stealthiness. It is, therefore, paramount that agency visibility, control and cybersecurity plans continue to expand to face these threats by protecting national security and uninterrupted production. Fortunately, the DoD and other critical government groups have begun mandating cybersecurity capabilities for all vendors in their supply chain to meet NIST 800.171, NIST 800.53 and CMMC today.

How can you implement and stay compliant with these new best practices for managing cybersecurity? Ntiva, a proven leader in managed IT support and IT security services, is now a CMMC-AB Registered Provider Organization (RPO). This means we are accredited to provide CMMC consulting and support to Organizations Seeking Certification (OSC) in the Defense Industrial Base (DIB).

We do NOT conduct CMMC audits as this would be in conflict with our services. We provide a wide range of technology services to our government contractor clients, with cybersecurity services being an important focal point. **Ntiva can meet you where you stand to proactively protect your IT investments and advise you on CMMC prerequisites.**

- Acquire greater visibility into the data assets you are responsible for securing
- Test and identify vulnerabilities with next step solutions and compliance
- Review system security plans and help prepare for a visit from the assessors
- Rapidly mitigate the impact of a security incident with a comprehensive incident response plan
- Win government contracts requiring CMMC cybersecurity compliance
- Receive advanced cybersecurity capabilities such as threat hunting, security monitoring, continuous security testing and incident response
- Customize and scale flexible visibility into situational awareness for your cybersecurity assets all in one place to suit your unique needs

Cybersecurity Maturity Model Certification (CMMC) defines 5 maturity levels to determine level of cybersecurity for each DIB member. The chart below shows the processes, practices, and types of sensitive information as related to each Maturity Level.

Maturity Levels in CMMC

MATURITY LEVEL	PROCESSES	PRACTICES	TYPES OF SENSITIVE INFORMATION
1	Performed	Basic Cyber Hygiene	FCI
2	Documented	Intermediate Cyber Hygiene	CUI
3	Managed	Good Cyber Hygiene	CUI
4	Reviewed	Proactive	CUI & APT
5	Optimized	Advanced/Progressive	CUI & APT

FCI: Federal Contract Information, CUI: Controlled Unclassified Information, APT: Advanced Persistent Threats

CMMC Table of Services based on domains and capabilities required.

The CMMC framework specifies a range of security maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks and other references, as well inputs from the Defense Industrial Base (DIB) and Department of Defense (DoD).

CYBERSECURITY MATURITY MODEL CERTIFICATION			NTIVA CMMC COMPLIANCE			
				MATURITY LEVEL		
DOMAIN	NAME	HOW TO COMPLY	HOW NTIVA HELPS	1	2	3
Access Control	**AC**	Establish who has access to your systems, control internal system access, and limit data access to authorized users and processes.	We will establish and maintain a domain structure which uniquely identifies users, enforces security and CUI policies, and controls local and remote access. We handle the IT onboarding and offboarding of employees and grant and revoke access to your information and systems, whether on-premises or in the cloud.	✓	✓	✓
Asset Management	**AM**	Locate, identify and log inventory of all your company assets.	Our automated tools constantly poll your internet connected computers. Hardware and software inventories are provided on your schedule. We also track warranty and license expirations.			✓
Audit & Accountability	**AU**	Have a process in place to track users that have access to your CUI and perform secure audits of those logs to ensure accountability.	We will define your audit requirements, perform the audit, identify and protect your audit information, as well as review and manage your audit logs. We will maintain audited events for as long as you subscribe to the service.		✓	✓
Awareness & Training	**AT**	Put security awareness training programs in place for all employees.	We provide monthly phishing prevention training and regular employee security awareness activities.		✓	✓
Configuration Management	**CM**	Establish configuration baselines as a measure to judge the efficiency of your systems.	We will establish your baseline configuration and perform configuration and change management tasks on an ongoing basis.		✓	✓
Identification & Authentication	**IA**	Ensure the proper roles within your organization have the correct level of access and can be authenticated for reporting and accountability purposes.	We can ensure only users authorized by you have the credentials to access data and systems. We also handle all aspects of user account creation and maintenance.	✓	✓	✓
Incident Response	**IR**	Establish an incident response plan that detects and reports events, implement responses to a declared incident, post-incident reviews and test responses to measure your preparedness in the event of an attack.	We will create an incident response plan, test the incident response plan, detect and report ongoing events, develop responses to declared incidents and perform post incident reviews.		✓	✓

CYBERSECURITY MATURITY MODEL CERTIFICATION			NTIVA CMMC COMPLIANCE			
				MATURITY LEVEL		
DOMAIN	NAME	HOW TO COMPLY	HOW NTIVA HELPS	1	2	3
Maintenance	**MA**	Have a maintenance system in place to effectively operate your systems.	System patches will be pushed on recurring weekly and monthly schedules. Zero-day vulnerabilities will be pushed within 24 hours.		✓	✓
Media Protection	**AM**	Provide proof that your media is identified and marked for ease of access. Additionally, provide evidence that a media protection protocol, sanitation protocol and transportation protection is in place.	We can help identify and mark all media, put processes in place to protect and control media, and sanitize and protect media for transport.	✓	✓	✓
Personnel Security	**PS**	Ensure all personnel will be properly screened and have background checks completed. Provide evidence that CUI is protected during personnel activity such as employee turnover or transfer.	We provide customized onboarding and offboarding checklists to ensure your business process is reflected in user account management. Only designated client POCs can request changes to access.		✓	✓
Physical Protection	**PP**	Provide evidence of the physical security surrounding your assets and prove they are protected.	While mainly a client activity, we can assist with system maintenance, vendor coordination, and best practice consulting.	✓	✓	✓
Recovery	**RE**	Keep and log backups of media necessary to your organization, and log for the purpose of continuity and to mitigate lost data.	We can automate backups on the schedule that meets your needs, by either adapting your existing systems to comply with CMMC or implementing a new, compliant system.		✓	✓
Risk Management	**RM**	Identify and evaluate the risk that affects your company using periodic risk assessments and vulnerability scanning - both yours and your vendors.	We can create Risk Management Plans and offer custom consulting for specific risk mitigations strategies and actions.		✓	✓
Security Assessment	**SA**	Put a system security plan (SSP) in place, define and manage controls and perform code reviews.	We can create or update your SSP/POAM as part of a CMMC Readiness Assessment, during a discovery phase and/or as part of your on-boarding to Ntiva services.		✓	✓

Capabilities Maturity Model Certification

CYBERSECURITY MATURITY MODEL CERTIFICATION			NTIVA CMMC COMPLIANCE			
				MATURITY LEVEL		
DOMAIN	NAME	HOW TO COMPLY	HOW NTIVA HELPS	1	2	3
Situational Awareness	**SA**	Establish a threat monitoring system to help keep your organization secure in event of cyber incidents.	Managed EDR and IDR with our 24/7 SIEM/SOC solution allows for rapid detection and mitigation of threats to your environment.			✓
System & Communications Protection	**SC**	Define the security requirements of each system and communication channel you use to provide evidence that you have control of communications at system boundaries.	We help define your requirements and then implement the tools, technologies, and processes to protect your systems whether on-prem or in the cloud - especially important in today's remote workforce.	✓	✓	✓
System & Information Integrity	**SI**	Identify and manage flaws with your system, identify hazardous and malicious content in-system, implement email protections and monitor your network and systems.	Vulnerability scans and remediation, EDR, IDR and cloud-based email protections block malicious content, monitor your network, and alert our 24/7 SOC and Service Desk of any suspicious behavior.	✓	✓	✓

Achieving NIST, DFARS, CMMC Compliance with Ntiva –3 Step Program

ASSESSMENT/SSP/POAM

The first step is to conduct a detailed assessment of your current environment. A system security plan (SSP) will be created to document the security measures that need to be put in place, and a Plan of Action and Milestones (POA&M) will outline the action items needed to reach compliance.

REMEDIATION

The next step is to address the items called out in the POA&M. This could be as simple as implementing a few minor changes, or as complex as doing an overhaul on outdated systems.

COMPLIANCE MONITORING & MAINTENANCE

Finally, ongoing cyber security monitoring and incident response can be provided by Ntiva. Cyber incidents must be reported to the DoD within 72 hours, and all systems and controls must be constantly assessed and maintained to remain compliant.

We provide a wide range of technology services to our government contractor clients, with cyber security services being an important focal point. We routinely deploy the safeguards needed to comply with NIST, DFARS and CMMC including:

- NIST, DFARS, CMMC Assessments and Remediation
- Intrusion Detection and Response
- Advanced Endpoint Protection
- Microsoft Office 365 Gov
- Business Continuity/Disaster Recovery
- IT User Policies
- Security Incident Response Plan
- Multi Factor Authentication
- Security Awareness Training