Red River

CMMC

SOLUTION BRIEF

RED RIVER CMMC 2.0

RED RIVER'S INITIAL COMPLIANCE WITH DFARS

Companies that serve the DOD are required to comply with an executive order called Defense Federal Acquisition Regulation Supplement (DFARS) 7. In order to show compliance, Red River sought out to build an environment in AWS GovCloud that meets DFARS and NIST 800-171 controls, of which CMMC 2.0 is based on, to enable Red River to receive and work on documents the DOD considered Controlled Unclassified or Controlled Defense Information (CUI/CDI).

Second Phase – MSP Gov Environment for CMMC/DFARS

DOD decided to make the original DFARS requirements more robust and to remove the self-assessment component that governed DFARS. This resulted in the creation of CMMC. Several drafts and a significant rewrite of the proposed CMMC framework have occurred over the last 2 ½ years. As a result, we began to hear from several Managed Services customers when we would comply with the revised CMMC 2.0 rules. At that point, Red River engaged in building a separate management stack in AWS GovCloud. The teams have spent the last 18 months building and preparing that stack for customers. In addition, we upgraded the corporate environment within the new build. This continues to serve the needs of Red River and preserves our ability to bid and win DOD work.

What is CMMC? Is it Finalized?

The Cybersecurity Maturity Model Certification (CMMC) program aligns with DoD's information security requirements for Defense Industrial Base (DIB) partners. CMMC is designed to enforce the protection of sensitive unclassified information that the Department shares with its contractors and subcontractors. The program assures the Department that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process controlled unclassified information (CUI). There have been two significant revisions over the last 2 ½ years. As a result, the framework is not finalized and needs to be accepted by DOD and made into law by Congress. The MSP stack that we built meets all controls we know about that are in the CMMC Level 2 framework (based on the NIST 800-171 controls) and can be made to meet additional controls CMMC may require in the future. There is also a possibility that CMMC will allow reciprocity with FedRAMP moderate controls. As such, Red River has written a document package to FedRAMP moderate controls.

When Can We Get Certified?

The CMMC Accreditation Body (AB) recently announced companies could hire C3PAOs (certified and approved independent auditors) for audits. However, any changes between now and when rulemaking is final will require a re-audit of any requirements gaps. We are monitoring the CMMC landscape and working to coordinate an optimal time to sit for an audit to optimize the LOE and audit costs.

Purpose of Red River's CMMC MSP Environment

The environment Red River has built to serve our customers' CMMC needs ensures we do not put their compliance at risk. This environment allows the customer to depend on Red River for monitoring of assets and log retention related to the tools used for monitoring. It does not negate the fact that the customer still has to go through their own CMMC assessment. Red River can bring partners in to assist customers as needed. Additionally, we should ask our CMMC customers if they have specific CMMC training so Red River staff understand their specific policies.

Tools in the CMMC Managed Services Stack

The following is a list of the tools included in the initial build of the MSP-Gov environment. Red River Managed Services considers this list to be the minimum required to continue offering monitoring and management services for our DOD contractor customers.

Managed Services Tools not listed below are considered outside of the CMMC boundary and should not be used to manage our CMMC customers.

TOOLS	DESCRIPTION	LIMITATIONS / NOTES
Kaseya / CMS	Fully functional CMS stack hosted in AWS Gov Cloud. Features include CMS scripts, Kaseya Agent, and Kaseya Remoting.	We are working closely with Kaseya to ensure they continue to fine-tune their FIPS 140-2 posture.
Secret Server	Privileged Password Management capabilities via an in-boundary instance of Secret Server. Same features as the SaaS commercial version including password vaulting, logging of cred access and use of Distributed Engine enabling credential rolling.	No known limitations to functionality.
Science Logic	Network & System infrastructure monitoring. Should be a 1:1 capability with LogicMonitor SaaS platform.	No known limitations to functionality.
ServiceNow Fed	ServiceNow FedRAMP instance: • ITSM – for Internal IT to maintain the CMMC environment from (INC, PRB, CHG) • CSM – MS to manage customer Cases & Change • RedConnect – Customer portal for cases and reporting	Minimum ITSM capabilities present enabling internal management and customer cases.
O365 GCC High	Utilizing GCC High O365 tenant for mail flow to and from customer systems, monitoring applications and SNOW-Fed	No limitations from a mail flow perspective.
AWS Workspaces Desktops	AWS Workspaces virtual windows desktops will be created for all Red River NOC/Service Desk/Tools Team/ IT staff that need to manage the CMMC stack and access tools in service of the CMMC customers	Desktops are locked down per CMMC / DFARS required controls. Changes and additions to the tools present must be requested. IT will work with stackArmor to review requests and validate the addition if possible.
Duo MFA	We are using a Cisco DUO commercial tenant to enable MFA to all the tools in the CMMC tenant. This includes IT, NOC, Service Desk and Onboarding staff. We will also use Duo to enable MFA access to customer access to the SNOW-Fed, ScienceLogic, Kaseya and AWS GovCloud Secret Server UIs. This instance of Duo MFA is not for customers to deploy for MFA access to their internal systems.	No known limitations to functionality.

What do Red River Engineers need to know to operate our CMMC MSP environment?

1. CMMC Training Requirement

Complete the CMMC training about the compliance requirements of the environment. While it's not a "how do I operate this environment," it outlines compliance responsibilities and is a mandatory Government requirement to complete.

2. Complete Customer Required Training

Any customer specific CMMC training and/or requirements that our Managed Services staff must complete before accessing the environments for management. These customers may have yet to develop training, but over time Red River can help prepare as we gather information on what's needed.

3. Access CMMC Customer Environments

Access to a customer network, applications, infrastructure, public cloud, and SaaS applications must be performed from the provided AWS Workspace desktops to ensure the customers' data, files, etc., do not end up on our corporate systems or laptops. Remoting to customer systems or access to UIs for their O365 instances, Azure, and AWS should all happen from the provided AWS Workspaces desktops. Remoting via Kaseya will be available. ConnectWise & Bomgar Remote tools are not in the CMMC build and will not be used to access CMMC customer systems.

4. Access to CMMC-Gov MSP Tools

Access to the management tools in the environment must be performed from the AWS Workspace desktops, including the Kaseya, ScienceLogic, Secret Server, and Service Now UIs. It also includes access to the in-boundary system servers to ensure the information does not leave the environment and ends up on our corporate laptops, Team Sites, SharePoint sites, etc.

5. Customer Onboarding / Document Handling

Red River will consult with customers to determine proper handling of customer SOPs, credentials, diagrams (Visio), and other customer-provided documentation. They may consider all company data sensitive and wish to handle it as CUI/CDI. We have a GCC High O365 tenant to enable Managed Services or Onboarding teams to store and manage customer-provided data. Guidelines needed for the protection of customer CUI data may involve further discussions and clarification. It will be the customer that has to determine where their CUI data is and managed.

6. Tool Usage within CMMC Customer Environments

Careful consideration will be taken if/when additional applications that are not in the current CMMC platform need to be added. Only after an impact assessment, a design review with the compliance team and proper change management, will tools be added. SaaS applications that do not meet CMMC/DFARS requirements will not be used. Additionally, the customer must review and approve the use of locally installed tools to capture data. These requirements may require higher LOE for CMMC customer engagements; however, this may not be avoidable and will reflect higher customer costs to run in an environment that meets CMMC / DFARS requirements.

Red River

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, cybersecurity, infrastructure, collaboration and cloud solutions.

Learn more at **redriver.com**