

Securing IT

CMMC Ready Cyber
Compliance Solutions



Infrastructure as a Service
(IaaS) Born Compliant CMMC
Accredited Architecture

CMMC Levels 3, 4 and 5

Safe, Secure

- Email
- CUI File Sharing

Role-based

- Backups
- Endpoint Security
- Incident Response

Accreditation ready CMMC
Assessment Package

IT Cybersecurity Solutions pre-integrated, with turn-key “born compliant” solutions for your business. IaaS managed solutions tailored for your CMMC and NIST 800-171 risk level

Pre-integrated, hardened email and file sharing systems for full NIST 800-171 and CMMC Levels 3-5 compliance, available TODAY with turn-key security and pre-written compliance documentation.

SECURE EMAIL

- Built on ultra-stable, fault-tolerant high-availability private cloud Linux servers, managed by Aramint in the US by US citizens for compliance with ITAR / CUI / CDI / PII data
- DDoS-resistant cutting edge pre-filtered anti-phishing email using proven MailRoute® technology
- Migration assistance from O365®, in-house Exchange®, or Gmail® servers
- Full support for S/MIME and integrated 2FA (deployable with pre-integrated FIPS 140-2 2FA tokens)
- Insider threat protection, including threat hunting, command-and-control identification, and patient-zero analysis based on behavioral analysis for required incident reporting and counter-intelligence collaboration.
- Laptop lockdown services including advanced anti-virus and profile management with local+cloud domain controllers

SECURE FILE SHARING AND COLLABORATION

- Private cloud role-based file sharing, with system-level encryption, password- or PKI-based SSO access already in-place
- Designed for limited access to CUI/CDI files, with mobile access pre-limited based on file metadata
- Multi-user simultaneous, collaboration editing of files
- Windows clients for automatic folder synchronization into our highly-secure private cloud
- Automatic archiving of documentation versions and version control
- Bare metal backups of all laptops and servers, providing virtual laptop re-creation and major incident recovery
- All hosting is in a US-based private cloud, on dedicated servers with segmented storage and multiple guards and firewalls fully meeting NIST 800-171 and CMMC Level 5 standards



EMAIL SECURITY

Pre-filtered email with secure 2FA logins, fully NIST 800-171 and CMMC compliant with accrediting documentation. Automatic intelligent threat response, isolating potentially compromised clients and protecting the rest of your network and workforce, while complying with optimal NIST threat-response and threat-hunting profiles.



SECURE DOCUMENT MANAGEMENT

Role-based, encrypted file storage fully compliant with NIST 800-171 and CMMC levels 3-5. Logging and alerts on attack events, with rapid response to ensure your data is protected.



2 FACTOR AUTHENTICATION

Quick-start 2FA setup via pre-configured with FIPS 140-2 tokens and documented PKI domain controllers. Additional full-service setup of locally-administrated Certificate Authority by your IT staff, with OCSP validation and support for US DoD ECA x.509 PKI certificates

FOR MORE INFORMATION CONTACT US
888-720-1150 or sales@aramintcyber.com
www.aramintcyber.com

aramint
Cyber Compliance