carahsoft

CMMC 2.0 Backup & Recovery Compliance

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO ValuePoint, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Bacula Systems, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

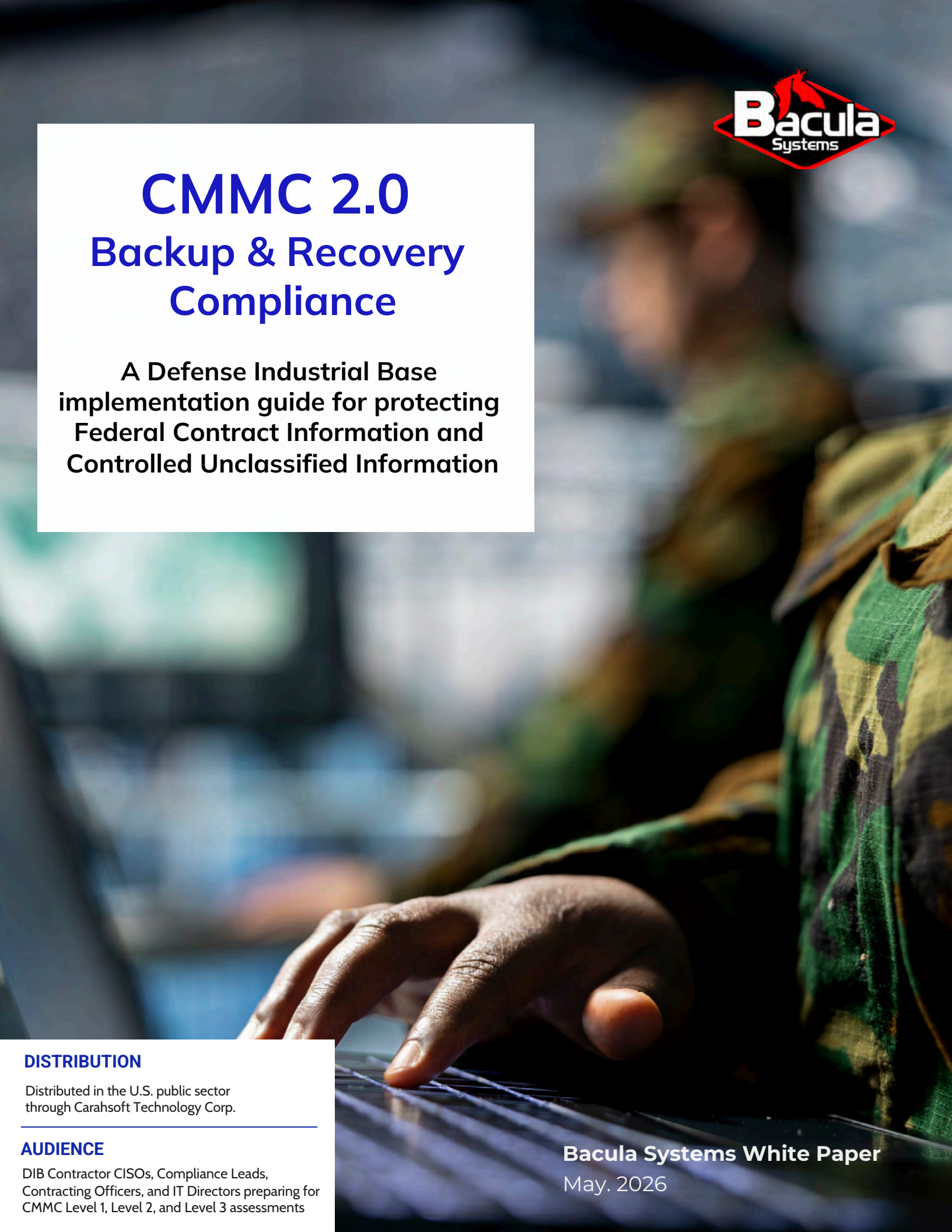
Explore More Resources:
carah.io/BaculaSystemsResources

Join Events & Webinars:
carah.io/BaculaSystemsEvents

Discover Technology Solutions:
carah.io/BaculaSystemsSolutions

Learn About Procurement:
carah.io/BaculaSystemsContracts

Connect With Our Team:
BaculaSystems@carahsoft.com
571-590-4040



CMMC 2.0

Backup & Recovery Compliance

A Defense Industrial Base implementation guide for protecting Federal Contract Information and Controlled Unclassified Information

DISTRIBUTION

Distributed in the U.S. public sector through Carahsoft Technology Corp.

AUDIENCE

DIB Contractor CISOs, Compliance Leads, Contracting Officers, and IT Directors preparing for CMMC Level 1, Level 2, and Level 3 assessments

Bacula Systems White Paper
May. 2026

Table of contents:

Executive Summary

Cybersecurity Maturity Model Certification 2.0 is no longer a prospective compliance program. The DoD Final Rule at 32 CFR Part 170 took effect December 16, 2024, and the DFARS implementation rule at 48 CFR took effect November 10, 2025. Phase 1 of the four-phase rollout is active in solicitations today. Phase 2, beginning November 10, 2026, will require third-party C3PAO certification at Level 2 for the majority of contracts that involve Controlled Unclassified Information.

For defense contractors and subcontractors across the Defense Industrial Base, the practical question has shifted from "will CMMC apply to us?" to "can we produce documented evidence that our backup and recovery architecture satisfies the assessment objectives our C3PAO will examine?" That question lands squarely on backup. CMMC Level 2 incorporates 110 security requirements from NIST SP 800-171 Rev. 2, and a substantial subset of those requirements — particularly across the Contingency Planning, Media Protection, System and Information Integrity, Audit and Accountability, and System and Communications Protection families — are unsolvable without a backup and recovery platform that was designed for them.

This whitepaper maps Bacula Enterprise capabilities directly to the CMMC Level 1, Level 2, and Level 3 requirements that depend on backup. It is structured to give contractor compliance teams a defensible position to take into a C3PAO assessment, and to give contracting officers and IT directors a procurement-ready evaluation framework for selecting a backup platform that will not become a CMMC liability.

Executive Summary (continued)

The Assessment Horizon is Approaching

The practical question for the DIB has shifted from "*will CMMC apply?*" to *"can we produce forensic evidence that our architecture satisfies C3PAO assessment objectives?"*

Three findings from this analysis:

1. Bacula Enterprise satisfies every backup-relevant CMMC Level 2 control without architectural workarounds, custom integrations, or third-party add-on modules.

2. The most common backup-related assessment findings — missing offline copies, lack of recovery testing evidence, inadequate audit logging, and unverifiable encryption — are addressed natively by Bacula's architecture.

3. Bacula's per-core licensing model removes the structural incentive to under-protect CUI in order to control backup software costs, a problem that is widespread among contractors using per-TB or per-VM platforms.

The CMMC 2.0 Landscape

The Two-Rule Structure

The CMMC 2.0 program is governed by two interrelated federal rules. The Program Rule, codified at 32 CFR Part 170, establishes the substantive cybersecurity standards, the three certification levels, the assessment methodology, and the roles of C3PAOs and DIBCAC. It became effective December 16, 2024. The DFARS Acquisition Rule, codified at 48 CFR (amending Parts 204, 212, 217, and 252), establishes the contractual mechanism — DFARS clause 252.204-7021 — that makes CMMC certification a binding award-eligibility condition. The DFARS rule became effective November 10, 2025, marking the first day of the four-phase rollout.

Phase 1 (November 10, 2025 to November 9, 2026) requires Level 1 or Level 2 self-assessment as a condition of award for newly awarded contracts that involve FCI or CUI. DoD retains discretion to require Level 2 C3PAO certification during Phase 1 for higher-sensitivity programs. Phase 2 begins November 10, 2026, at which point Level 2 C3PAO certification becomes the default requirement for contracts involving CUI. Phase 3 begins November 10, 2027 and adds Level 3 DIBCAC assessments for the highest-priority programs. Phase 4 begins November 10, 2028, at which point all applicable DoD contracts — including option exercises on existing awards — must include the appropriate CMMC level as a condition of award.

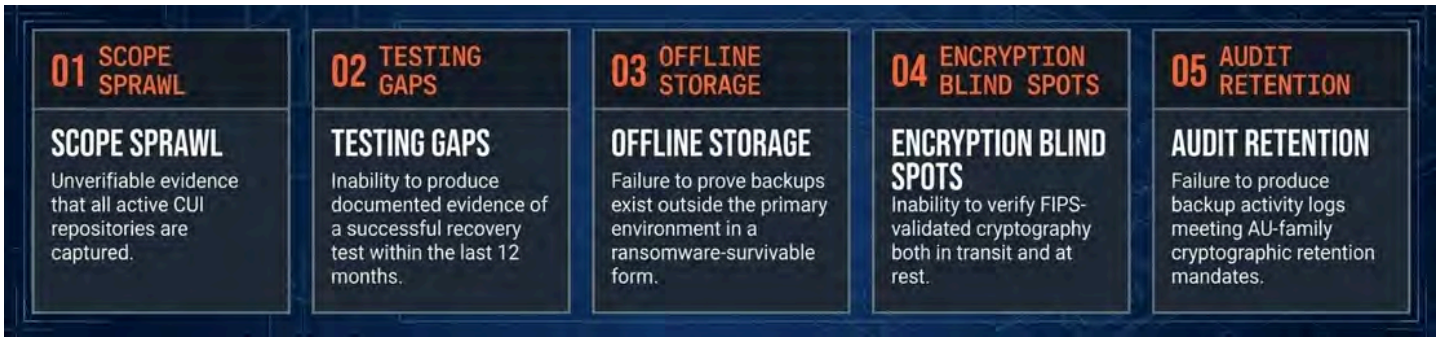
The Three Certification Levels

Level	Information Type	Controls	Assessment
Level 1 — Foundational	Federal Contract Information (FCI) only	15 requirements from FAR 52.204-21	Annual self-assessment with senior leadership affirmation
Level 2 — Advanced	Controlled Unclassified Information (CUI)	110 requirements from NIST SP 800-171 Rev. 2	Triennial C3PAO certification (some self-assessment in Phase 1)
Level 3 — Expert	CUI in highest-priority programs	110 NIST 800-171 R2 requirements plus selected NIST 800-172 enhancements	Triennial DIBCAC government-led assessment

The Subcontractor Flow-Down

CMMC requirements flow down from primes to subcontractors based on the type of information the subcontractor will process, store, or transmit. A subcontractor handling only FCI may be required to achieve Level 1. A subcontractor handling CUI must achieve at minimum Level 2 with the same assessment type the prime is required to hold. A prime contractor with a Level 3 obligation must require its subcontractors handling CUI to hold at least Level 2 C3PAO certification. The prime is contractually obligated to verify subcontractor compliance at the time of award. This flow-down structure means CMMC is not a problem only for primes — every tier of the DIB supply chain is in scope.

The Most Frequent Points of Assessment Failure



Assessors rigorously examine backup infrastructure because it touches every system processing CUI. These gaps are unsolvable through policy - they require an architectural answer.

Why This Whitepaper Focuses on Backup

Of the 110 controls in NIST SP 800-171 Rev. 2, approximately twenty-five are either directly satisfied by, or materially depend on, backup and recovery capability. C3PAO assessors examine these controls with particular rigor because backup is one of the most common areas where contractors discover late-stage compliance gaps.

The most frequent assessment findings relate to backup scope ("are all CUI repositories actually being backed up?"), recovery testing ("can you produce evidence of a successful restoration test in the last twelve months?"), offline storage ("can you demonstrate that backups exist outside the primary environment in a form that survives a ransomware event?"), encryption ("are backups encrypted with FIPS-validated cryptography both in transit and at rest?"), and audit logging ("can you produce backup activity logs that meet AU-family retention requirements?"). Each of these findings is unsolvable through policy alone. They require an architectural answer, and the architectural answer is the backup platform itself.

CMMC Level 1 — Foundational Backup Requirements

Level 1 applies to contractors that process, store, or transmit Federal Contract Information but not Controlled Unclassified Information. The fifteen Level 1 requirements derive from FAR 52.204-21 (now relocated to FAR 52.240-93). Three of the fifteen are directly relevant to backup and recovery.

The Three Backup-Relevant Level 1 Controls

Control	Requirement	Bacula Capability
3.1.1 / AC.L1-3.1.1	Limit information system access to authorized users, processes, or devices.	Role-based access controls; per-job authentication; integration with Active Directory/LDAP; separate roles for backup operators, restore operators, and administrators.
3.1.2 / AC.L1-3.1.2	Limit access to types of transactions and functions authorized users are permitted to execute.	Granular permission model separating backup, restore, configuration, and audit functions; no implicit privilege escalation between roles.
3.13.1 / SC.L1-3.13.1	Monitor, control, and protect organizational communications at external boundaries and internal boundaries.	TLS-encrypted daemon-to-daemon communications; FIPS 140-validated cryptographic modules; configurable network boundary controls between Director, Storage Daemon, and File Daemon tiers.

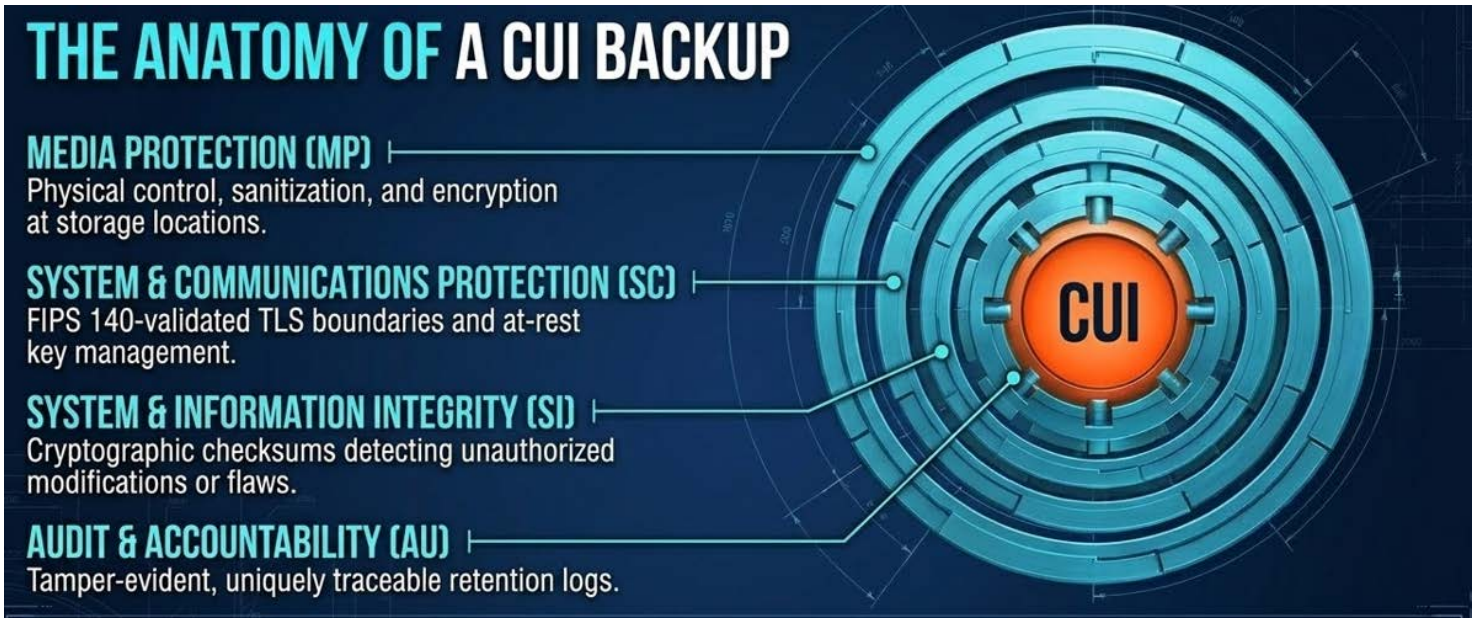
For Level 1 contractors, the backup platform's contribution to compliance is straightforward but not trivial. The platform must enforce access boundaries (3.1.1, 3.1.2), and it must protect the data it moves across those boundaries (3.13.1). Bacula Enterprise satisfies these requirements by default in any standard deployment configuration.

Level 1 does not require backups to be created. It does, however, require that any backups that exist be protected to the same standard as the data they contain. A contractor that operates a backup system that fails to enforce access controls or encrypt FCI in transit creates a Level 1 finding even if backups are not otherwise mandatory.

CMMC Level 2 — The Core Compliance Mapping

Level 2 is where the majority of DIB contractors will operate.

The 110 NIST SP 800-171 Rev. 2 requirements span fourteen control families. Backup and recovery is most heavily concentrated in five of those families: Contingency Planning is not a separate family in NIST SP 800-171 (it appears in the broader 800-53 catalog) but its requirements are distributed across Media Protection (MP), System and Information Integrity (SI), Audit and Accountability (AU), System and Communications Protection (SC), and Recovery (RE). What follows is the mapping that matters most for a C3PAO assessment.



CMMC Level 2 incorporates 110 requirements. Twenty-five of these controls are entirely dependent on how the backup platform executes these four protective layers.

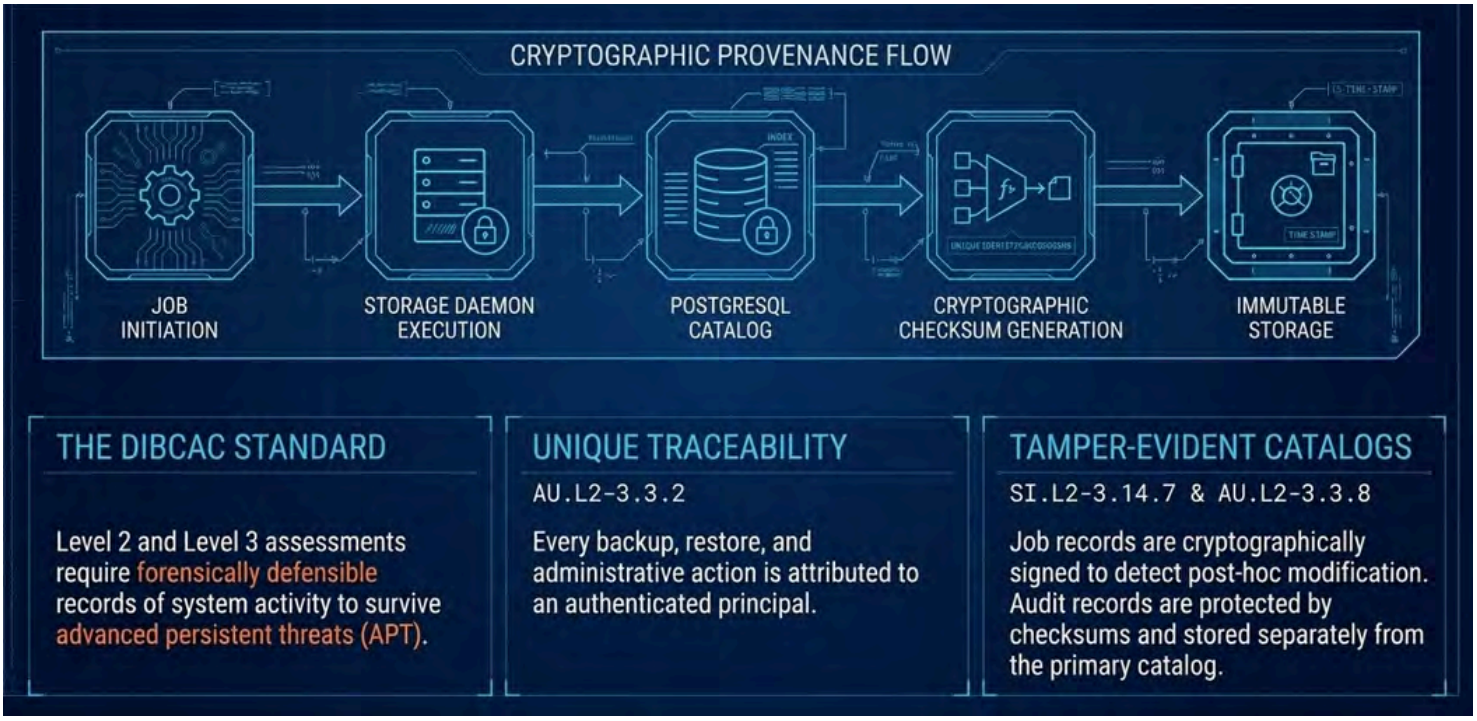
The Critical Backup-Relevant Level 2 Controls

The following controls represent the backup and recovery requirements that C3PAO assessors examine with particular attention. Each entry identifies the NIST 800-171 control, summarizes the assessment objective, and describes how Bacula Enterprise satisfies the control through native architectural capability rather than configuration workaround.

Media Protection (MP) Family: Securing the payload (MP and SC Families)

Control	Requirement Summary	Bacula Capability
3.8.1 / MP.L2-3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Encrypted storage at rest; tape encryption (AES-256); object lock for cloud targets; physical media tracking via Volume catalog with chain-of-custody metadata.
3.8.2 / MP.L2-3.8.2	Limit access to CUI on information system media to authorized users.	Role-based access at Volume and Pool level; cryptographic separation by tenant; key custodianship independent of storage administrator role.
3.8.3 / MP.L2-3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Built-in tape erase/relabel commands with audit trail; cryptographic erasure via key destruction; documented sanitization workflows compliant with NIST SP 800-88.
3.8.6 / MP.L2-3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport.	FIPS 140-validated AES-256 encryption applied at the Storage Daemon before media write; encryption persists across all transport modalities including tape shipment to offsite vaults.
3.8.9 / MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.	Native immutable storage; air-gap-capable architecture (CNSSI 4009-2015 aligned); tamper-evident audit log of all access to backup repositories.

System and Information Integrity (SI) Family



Control	Requirement Summary	Bacula Capability
3.14.1 / SI.L2-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	Verify Jobs detect cross-host file changes that indicate compromise; integration with SIEM platforms for automated flaw notification; cryptographic checksums on every backed-up object.
3.14.6 / SI.L2-3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Per-job logging of source, destination, volume, duration, and outcome; anomaly detection on backup volume and timing patterns; native syslog and SIEM forwarding.
3.14.7 / SI.L2-3.14.7	Identify unauthorized use of organizational systems.	Tamper-evident catalog of every backup and restore operation; authentication required for every job; cryptographic signing of job records to detect catalog tampering.

Audit and Accountability (AU) Family

Control	Requirement Summary	Bacula Capability
3.3.1 / AU.L2-3.3.1	Create and retain system audit logs and records to the extent needed to enable monitoring, analysis, investigation, and reporting of unlawful or unauthorized activity.	Comprehensive job, restore, configuration, and authentication logs; retained per organizational policy; cryptographically protected against post-hoc modification.
3.3.2 / AU.L2-3.3.2	Ensure that the actions of individual system users can be uniquely traced.	Every backup, restore, configuration change, and administrative action attributed to an authenticated principal; service accounts subject to the same audit requirements as human users.
3.3.4 / AU.L2-3.3.4	Alert in the event of an audit logging process failure.	Native alerting on log generation failures; integration with monitoring platforms; configurable escalation paths.
3.3.8 / AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Audit records protected by cryptographic checksum; separate retention storage from primary catalog; immutable storage option for audit trail.

System and Communications Protection (SC) Family

Control	Requirement Summary	Bacula Capability
3.13.8 / SC.L2-3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	FIPS 140-validated TLS for all daemon-to-daemon communications; AES-256 for payload-level encryption; configurable cipher suites and minimum protocol versions.
3.13.10 / SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Integration with enterprise key management systems including KMIP-compliant providers; OpenBao/Vault integration; documented key lifecycle including generation, rotation, and destruction.
3.13.11 / SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Bacula leverages OpenSSL with FIPS 140-validated modules; documented FIPS mode of operation; organizational ability to validate FIPS configuration through configuration audit.
3.13.16 / SC.L2-3.13.16	Protect the confidentiality of CUI at rest.	AES-256 encryption applied at the Storage Daemon; per-volume keys; protection persists regardless of storage medium (disk, tape, object, cloud).

Recovery (Distributed Across Multiple Families)

NIST SP 800-171 Rev. 2 does not contain a dedicated "Contingency Planning" family in the way NIST SP 800-53 does. Recovery requirements are distributed primarily across the AU, SI, MP, and SC families above. However, certain control objectives — particularly the ability to restore systems to a known-good state following a security incident — are examined by C3PAOs as integrated capability questions rather than single-control questions. A contractor that cannot demonstrate restoration capability will receive findings against multiple controls simultaneously. Bacula's bare-metal recovery (LinuxBMR, WinBMR), application-consistent restoration of databases (Oracle, MS SQL, PostgreSQL, MySQL, MongoDB, IRIS), and infrastructure-as-code restore workflows directly address this composite assessment objective.

CMMC Level 3 — Enhanced Requirements for High-Priority Programs

Level 3 is required for contractors handling CUI in DoD's highest-priority programs. The exact program list is determined by DoD on a per-program basis but typically includes weapons systems, space programs, certain communications and intelligence programs, and select critical-technology efforts. Level 3 incorporates all 110 NIST SP 800-171 Rev. 2 requirements and adds a selected subset of NIST SP 800-172 enhanced security requirements designed to defend against advanced persistent threats.

Backup Architecture: Assessment Liability VS. Assessment Enabler

CRITERIA	LEGACY / SAAS BACKUP	CMMC-NATIVE ARCHITECTURE
Management Plane	Cloud/SaaS expanding the assessment scope	Fully contained on-premises operation
Air-Gap Methodology	Logical barriers (S3 Object Lock / API-gated)	Physical isolation **(CNSSI 4009-2015 aligned)**
Licensing Model	Per-TB (Creates financial disincentive to protect CUI)	Per-Core (Removes cost penalties for data growth)
Audit Provenance	Basic application logging	Cryptographically signed, tamper-evident catalogs
POA&M Reality	Heavy POA&Ms required; cannot be closed within 180 days due to structural replacements	Native capability requiring no architectural remediation

Level 3 is assessed by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), not by C3PAOs. DIBCAC assessments are conducted by government personnel and are substantially more rigorous than C3PAO Level 2 assessments. The backup and recovery implications of Level 3 fall into three categories

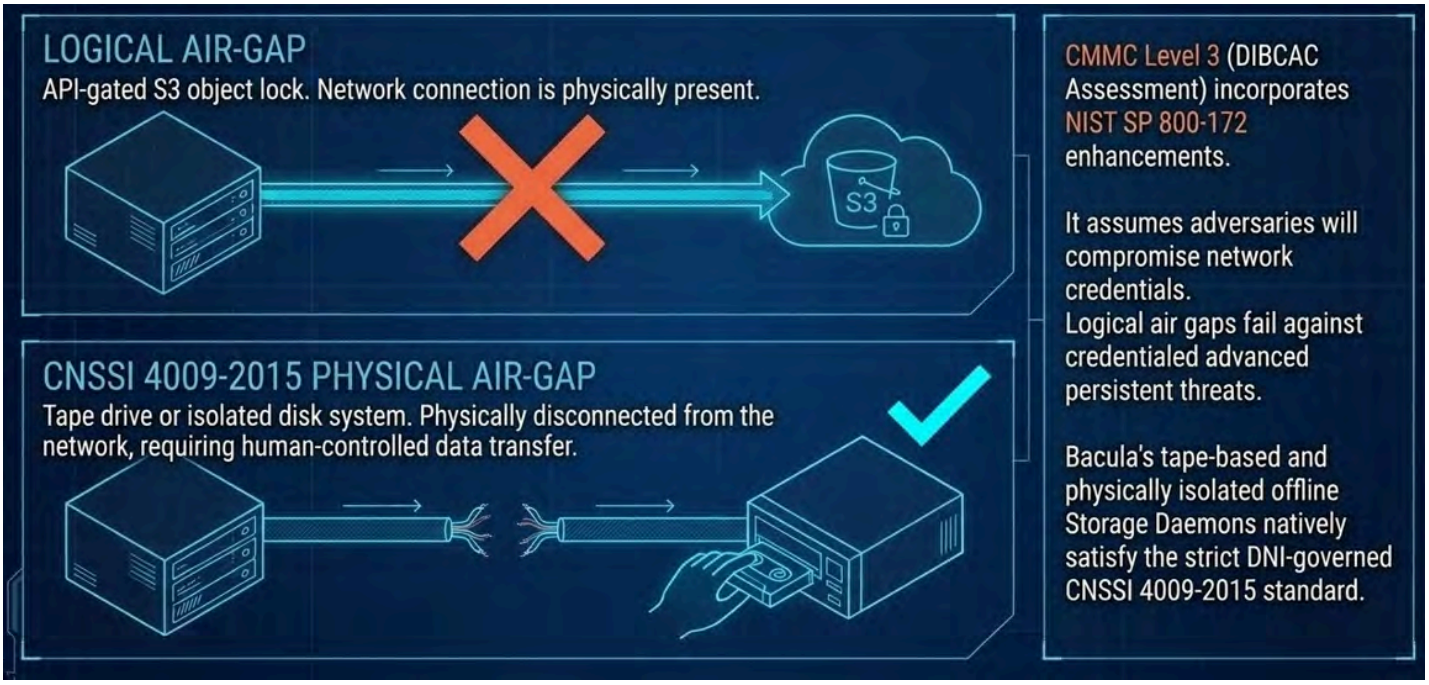
Advanced Persistent Threat Resilience

NIST SP 800-172 emphasizes the assumption that adversaries with significant resources, persistence, and sophistication will attempt to compromise contractor systems. The backup platform must therefore be designed not merely to recover from accidental data loss but to recover from a sophisticated, multi-stage attack that may have included tampering with backup systems themselves. This is where Bacula's architectural separation between Director, Storage Daemon, and File Daemon — combined with cryptographic verification of every backup — provides materially greater protection than appliance-based architectures where the backup management plane and the backup storage are integrated into a single failure domain.

True Air Gap

Level 3 environments are precisely the contractor environments where logical air gap solutions are most likely to be deemed insufficient. The DNI-governed CNSSI 4009-2015 definition of air gap requires both physical separation and human-controlled data transfer. Bacula's tape-based and physically isolated workflows satisfy this definition.

The True Air Gap Divider (Level Three Standard)



S3 Object Lock, immutable cloud buckets, and API-gated repositories — whatever their other merits — do not. Contractors operating at Level 3 should expect DIBCAC to examine air gap claims against the CNSSI 4009 standard rather than against vendor marketing language.

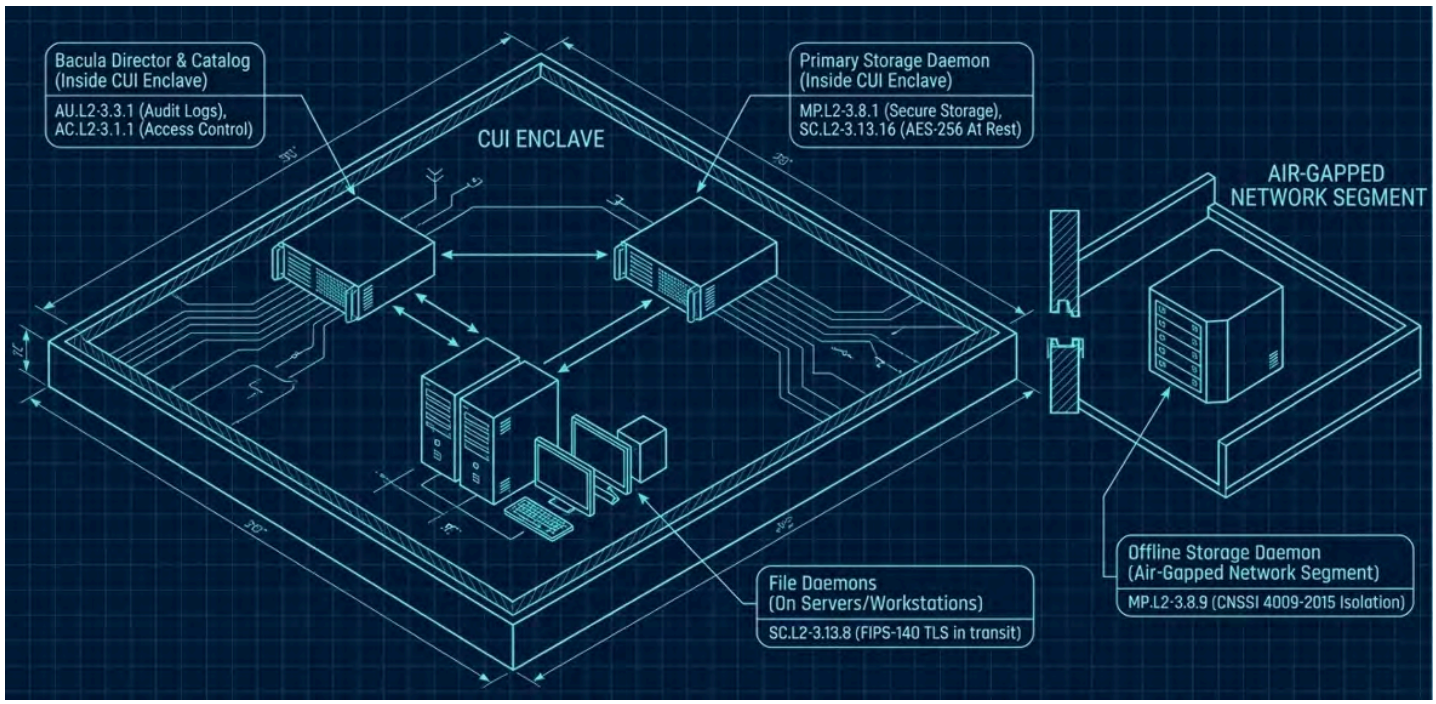
Forensic-Grade Audit and Provenance

Level 3 assessments examine the contractor's ability to produce forensically defensible records of system activity, including backup activity, in the event of a suspected compromise. Bacula's tamper-evident catalog, cryptographically signed job records, and configurable retention windows that exceed NIST 800-171 minimums provide the audit substrate that DIBCAC examiners will look for. A backup platform that does not produce records suitable for use as forensic evidence is, at Level 3, a compliance liability rather than a compliance enabler.

CMMC Reference Architecture

The following reference architecture pattern is suitable for a CMMC Level 2 contractor environment and is upgradeable to Level 3 by adding the air-gap and forensic components described in Section 4. It is offered as a starting point for contractor architects, not as a prescriptive deployment.

Synthesis: The Secure Enclave Blueprint



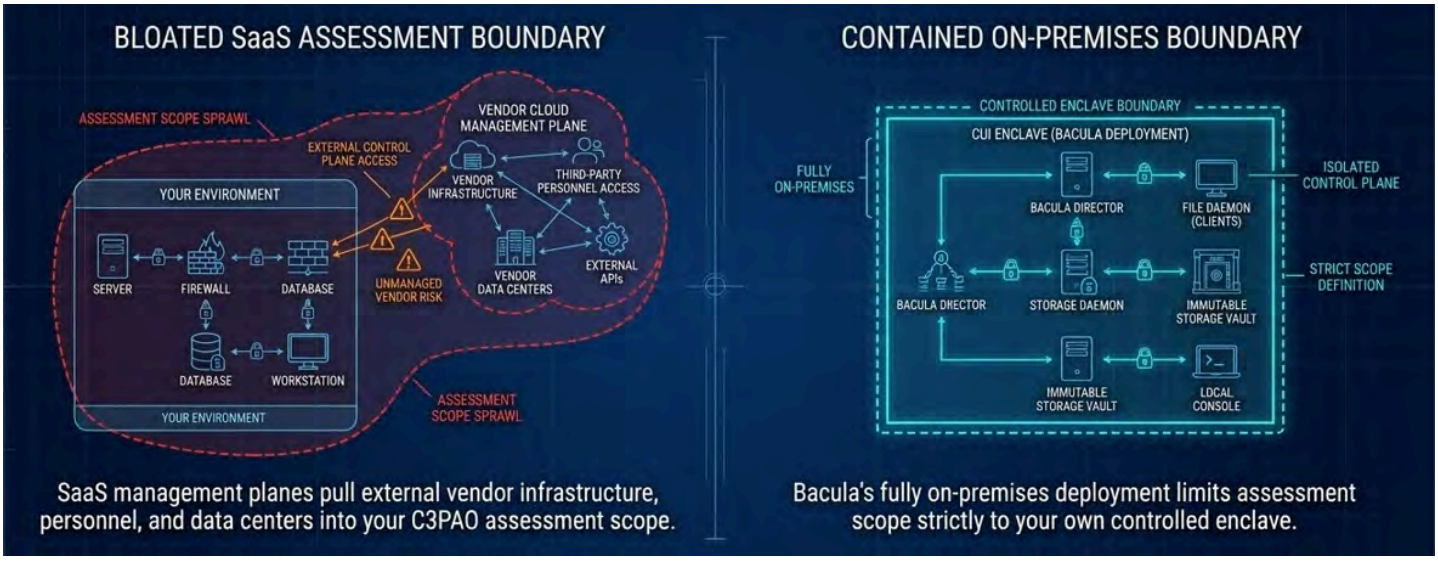
Logical Architecture Components

Component	Function	CMMC Linkage
Bacula Director	Central scheduling, job orchestration, catalog, and audit log generation. Deployed on a hardened Linux host inside the CUI enclave.	AU.L2-3.3.1, AU.L2-3.3.2, SI.L2-3.14.7, AC.L2-3.1.1
Storage Daemon (Primary)	Disk-based backup target inside the CUI enclave. Encrypted volumes; immutable retention configured per organizational RPO/RTO targets.	MP.L2-3.8.1, MP.L2-3.8.6, MP.L2-3.8.9, SC.L2-3.13.16
Storage Daemon (Offline / Air-Gap)	Tape library or physically isolated disk system reachable only via scripted, audited transfer. Satisfies the CNSSI 4009 air-gap definition for Level 3 environments.	MP.L2-3.8.9 (Level 3 enhancement)
File Daemons	Per-host agents on workstations, servers, hypervisor hosts, application platforms (Oracle, MSSQL, etc.), and Kubernetes clusters.	Distributed across MP, SI, AU, SC families
Catalog	PostgreSQL database tracking every backup, every volume, every restore. Cryptographically protected; retained per organizational policy.	AU.L2-3.3.1, AU.L2-3.3.8, SI.L2-3.14.7
Key Management Integration	External KMS (KMIP-compliant) or OpenBao/Vault for cryptographic key custody. Storage administrators do not have direct access to keys.	SC.L2-3.13.10, SC.L2-3.13.11
SIEM Integration	Syslog/CEF forwarding of all Bacula events to the organizational SIEM for correlation with broader security telemetry.	AU.L2-3.3.4, SI.L2-3.14.6

Network Boundary Considerations

CMMC assessors examine network boundaries with particular attention to whether CUI can leak out, and whether attackers can leak in. The Bacula three-tier architecture (Director, Storage Daemon, File Daemon) supports configurable boundary placement that allows the backup platform to participate in a defense-in-depth model rather than create new attack surface.

The ESP Boundary Trap



Under the CMMC final rule, an external service provider without independent certification expands your assessment liability. keep your control plane inside your enclave

In typical contractor deployments, the Director and primary Storage Daemon reside inside the CUI enclave, separated from non-CUI corporate IT by a controlled boundary.

File Daemons are deployed on every host that processes, stores, or transmits CUI. Communication between tiers is TLS-encrypted with FIPS-validated cryptographic modules. The offline/air-gap Storage Daemon, where deployed, is placed on a physically separate network segment with no continuous connectivity to the CUI enclave.

External Service Providers (ESPs) and the Backup Vendor Question

The CMMC Final Rule changed the External Service Provider treatment between proposed and final versions. Under the final rule, ESPs are not required to obtain their own CMMC certification. However, an ESP that does not pursue certification will have its assets included within the scope of its client's C3PAO assessment. This creates a structural incentive for ESPs to pursue certification independently — and creates a structural risk for contractors who select ESPs that do not.

Implications for Backup Vendor Selection

Many contractors operate backup-as-a-service or managed backup arrangements. The ESP rule means that the backup vendor's cloud infrastructure, management plane, and personnel may all fall within scope of the contractor's CMMC assessment. Three vendor characteristics become procurement-critical:

- Whether the vendor's management plane is a cloud SaaS service that requires the contractor's CUI to traverse vendor-controlled infrastructure. Several major backup vendors have migrated their management consoles to SaaS in recent years; this materially expands CMMC assessment scope.
- Whether the vendor pursues an independent compliance posture (FedRAMP authorization, SOC 2 Type II, ISO 27001) that contractors can use to inherit controls.
- Whether the vendor's deployment model permits fully on-premises operation with no required external connectivity, allowing the contractor to keep all CUI-handling components within the contractor's own assessment boundary.

Bacula Enterprise is deployed as on-premises software with no required cloud management plane. The Director, Storage Daemons, and File Daemons can run entirely within the contractor's CUI enclave with no external connectivity except for license validation (which can be performed offline via scheduled key files). This structural property removes the backup vendor from the contractor's CMMC assessment scope to the maximum extent possible — a meaningful reduction in compliance complexity that is not available with SaaS-management backup platforms.

Plan of Action & Milestones (POA&M) Strategy

CMMC permits limited use of POA&Ms to remediate specific, lower-impact controls that are not fully implemented at the time of assessment. Level 1 does not permit any POA&M items. Level 2 permits POA&Ms for selected lower-weighted controls, with full closure required within 180 days. Level 3 has the most restrictive POA&M policy.

Backup-Related Controls and POA&M Eligibility

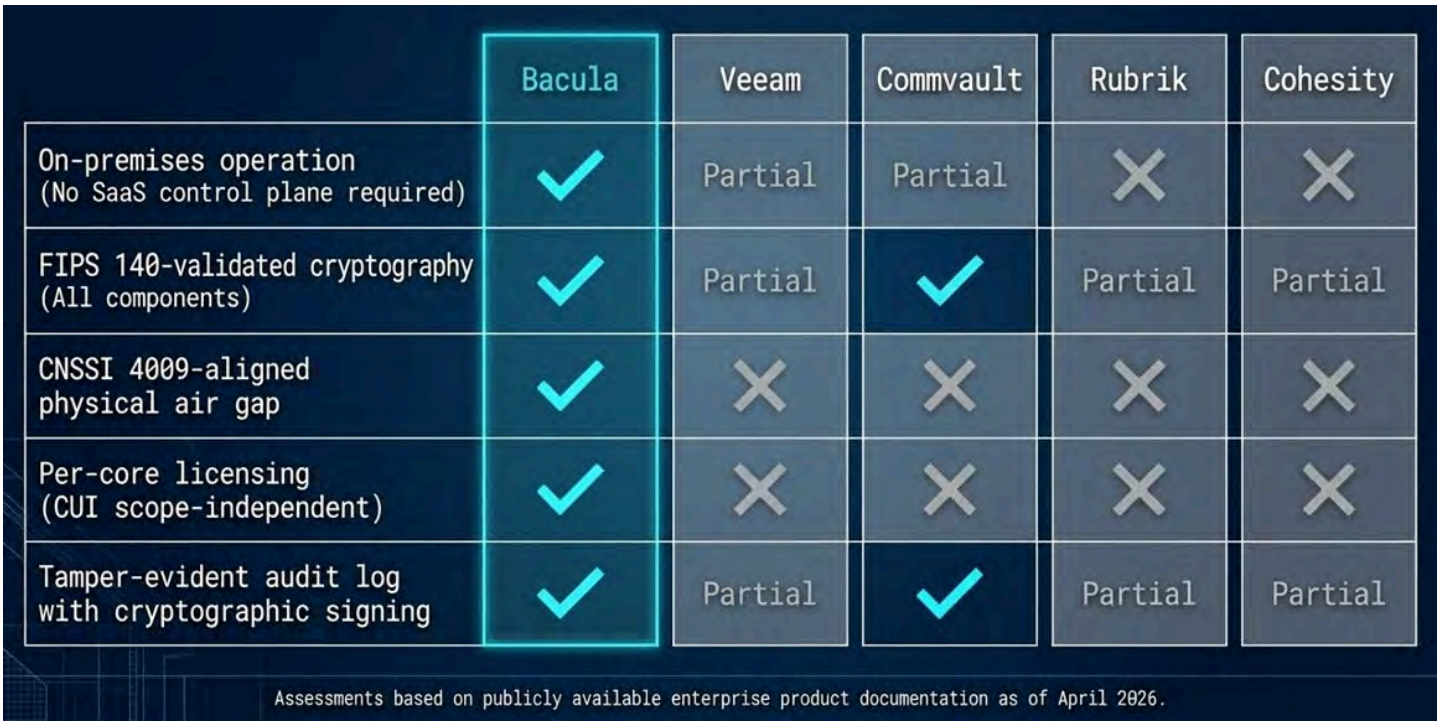
The backup-relevant controls in Section 3 of this whitepaper carry varying assessment weights. SC.L2-3.13.11 (FIPS-validated cryptography) and SC.L2-3.13.16 (CUI confidentiality at rest) are weighted heavily and are typically not eligible for POA&M closure. MP.L2-3.8.6 and MP.L2-3.8.9 (cryptographic protection of media in transport and at backup locations) carry similar weight. Audit and integrity controls in the AU and SI families carry medium weights with case-by-case POA&M eligibility.

In practice, backup-related findings are difficult to close via POA&M because they typically require platform replacement or major architectural change rather than configuration adjustment. The implication for contractors is that backup platform selection must be made before assessment, not after, and the platform must be selected to satisfy the highest-weighted controls natively.

Competitive Capability Comparison

The following comparison summarizes how Bacula Enterprise compares to the leading enterprise backup platforms most commonly encountered in DIB contractor environments, evaluated against CMMC-relevant capabilities. Assessments are based on publicly available product documentation as of April 2026.

The ESP Competitive Reality



The structural differences highlighted in the table on the next page are not minor product positioning differences. They are architectural properties that determine whether a contractor's backup platform contributes to or detracts from CMMC compliance. The combination of on-premises operation, FIPS-validated cryptography, true air gap capability, and per-core licensing — the four properties where Bacula leads consistently — is the combination that produces a defensible position in a C3PAO assessment.

Capability	Bacula	Veeam	Commvault	Rubrik	Cohesity
On-premises operation with no required SaaS management plane	Yes	Partial	Partial	No	No
FIPS 140-validated cryptography across all components	Yes	Partial	Yes	Partial	Partial
CNSSI 4009-aligned air gap (physical isolation, manual transfer)	Yes	No	No	No	No
Per-core licensing (CUI scope-independent)	Yes	No	No	No	No
Tamper-evident audit log with cryptographic signing	Yes	Partial	Yes	Partial	Partial
Linux-native architecture (reduced Windows attack surface)	Yes	No	Partial	Partial	Partial
Fully air-gapped operation with no external dependencies	Yes	No	Partial	No	No
Bare-metal recovery for Linux and Windows endpoints	Yes	Yes	Yes	Partial	Partial

Conclusion and Next Steps

CMMC 2.0 has moved from anticipation to operational reality. Contractors that have not yet begun their compliance preparation are already behind. Contractors that have begun preparation but have not yet validated their backup architecture against the CMMC control objectives are at risk of late-stage findings that are difficult or impossible to remediate via POA&M.

Bacula Enterprise is purpose-built for the architectural properties that CMMC assessment objectives require: on-premises operation that does not expand assessment scope; FIPS-validated cryptography across every component; tamper-evident audit logs that satisfy AU-family requirements without auxiliary tooling; air-gap capability that meets the CNSSI 4009-2015 definition for Level 3 environments; and a per-core licensing model that does not penalize contractors for protecting more of their CUI rather than less.

Recommended Next Steps

1. Map your existing backup deployment against the controls in Section 3 of this whitepaper. Identify any controls where your current platform requires manual procedural workaround rather than native architectural capability.
2. If your backup platform's management console is a SaaS service, conduct an ESP scope analysis to determine whether the vendor's infrastructure will be included in your C3PAO assessment.
3. Review your encryption configuration against SC.L2-3.13.11. Confirm that the cryptographic modules in use are FIPS 140-validated and that your operational mode of the modules is the validated mode.
4. Schedule a documented recovery test against your CUI repositories within the next ninety days. Retain the test results as evidence for assessment.
5. If you operate at or anticipate Level 3, evaluate your backup architecture against the CNSSI 4009-2015 air gap definition. Logical air gap solutions are likely to be insufficient at Level 3.
6. Engage Carahsoft, Bacula's authorized public sector partner, for procurement support and contracting vehicle access including SEWP V, GSA, and DoD-specific vehicles

Bacula Systems is available through Carahsoft Technology Corp. for U.S. public sector procurement, including the Defense Industrial Base. Bacula's existing deployments at Los Alamos National Laboratory, Idaho National Laboratory, and Sandia National Laboratories provide established credibility for the highest-sensitivity DoD and DOE environments.

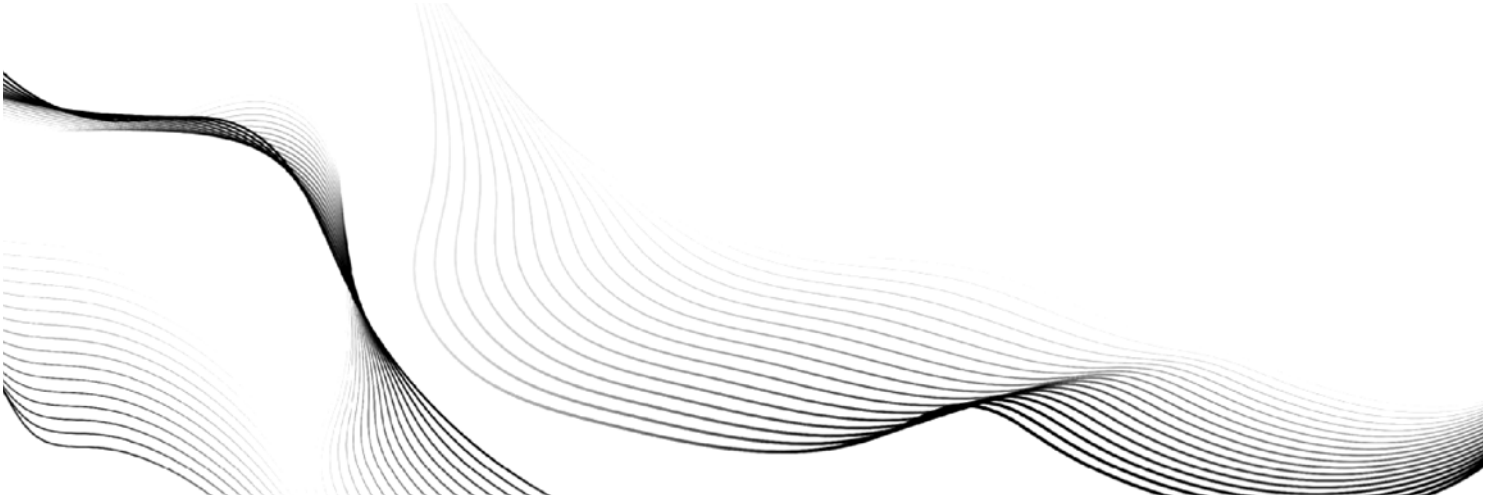
contact@baculasystems.com | www.baculasystems.com

About Bacula Systems

Bacula Systems is an enterprise backup and recovery software company with offices in Europe and the United States. Bacula Enterprise is deployed across HPC national laboratories, critical infrastructure operators, financial institutions, healthcare organizations and defense agencies worldwide.

Bacula's Linux-native, director-driven architecture, per-core licensing model, and security-first design mean it is highly suited for organizations that treat security, OT compliance, and native architecture as a mandate. It is specifically designed to handle extremely large, complex, and high-performance data environments while maintaining exceptional levels of security and flexibility. Its scalable, modular architecture integrates seamlessly with HPC systems, regulated environments, hybrid cloud infrastructures and diverse data types common in genomics, drug discovery and scientific research.

Don't let backup constraints limit your security. Contact Bacula today and discover how its comprehensive data protection can accelerate your path to higher security levels.



Document Version: 2.0
Publication Date: April 2026

www.baculasystems.com