

Bacula Systems DoW Solution Brief

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



Department of War Solution Brief

Bacula Systems DoW Solution Brief

Secure, Compliant and Scalable Data Backup & Recovery for the
U.S. Department of War — Across All Mission Domains

AUTHOR

Bacula Systems

TECHNOLOGY

Critical Data Backup and Restore, Data Resilience and
Disaster Recovery

DATE

April 4 2026

LEARN MORE



TABLE OF CONTENTS

Introduction	3
DoW Mission Environment	3
Why Bacula Systems?	3
Operational Impact	3
Mission Domain Coverage	4
Cross-Domain Backup & Recovery	4
Key Capabilities	5
Security & Ransomware Resilience	5
Compliance Enablement	5
Cross-Domain Scalability	5
Air-Gap & Data Sovereignty	5
Cost Predictability	6
Deployment Flexibility (CONUS / OCONUS)	6
Compliance Alignment	6
CMMC & NIST SP 800-171 Mapping	6
Additional Frameworks	6
Bacula Enterprise's Strict Compliance Alignment	7
Bacula vs. Alternatives	8
Bacula Enterprise's Clear Differentiation	8
Conclusion	9

Introduction



DoW Mission Environment

The U.S. Department of War (DoW)¹ operates one of the most diverse and demanding IT estates in the world — spanning classified and unclassified networks, supercomputing centers, tactical edge deployments, enterprise business systems, sovereign and commercial cloud, virtualized and containerized workloads, and operational technology supporting weapon systems and base infrastructure. Each of these domains has distinct data protection requirements, but all share a common imperative: uncompromising security, strict compliance alignment, architectural flexibility, and rapid recovery to maintain mission readiness.

Adversary targeting of DoW data has expanded from classified intelligence to logistics, personnel, research, AI training corpora, and the mission software supply chain. Ransomware, insider threat, and supply-chain compromise are now persistent risks across every domain — and recoverable, tamper-proof backups have become a foundational element of cyber resilience.

WHY BACULA SYSTEMS?

Bacula Enterprise delivers immutable backups, true air-gapped storage, FIPS 140-validated encryption, advanced incremental and synthetic backup levels, and centralized policy control across all DoW mission domains — from petabyte-scale HPC to forward-deployed tactical units — under a single, scriptable, open-architecture platform with no per-terabyte licensing tax.

OPERATIONAL IMPACT

- Reduced downtime from cyber incidents and ransomware across CONUS and OCONUS operations
- Audit-ready posture for CMMC 2.0, NIST SP 800-171, NIST SP 800-53, and DISA STIG requirements
- Long-term cost efficiency for petabyte-scale, multi-domain deployments
- Significantly increased mission resilience for classified, tactical, and enterprise workloads
- Sovereignty assurance through Swiss-headquartered engineering and open, inspectable architecture

¹ Per Executive Order 14347 (Sep 5, 2025), "Department of War" and "Secretary of War" are authorized secondary titles used in non-statutory contexts. The Department's legal name remains the Department of Defense (DoD) until Congress acts. References to "DoW" in this brief follow the Department's public branding; statutory and contractual references retain "DoD."

Mission Domain Coverage



DoW data protection is a portfolio of related problems with shared compliance, security, and resilience requirements. Bacula Enterprise addresses all of them with a single architecture, single licensing model, and single operational toolset — reducing tool sprawl, simplifying certification & accreditation (C&A), and consolidating the supply chain.

Cross-Domain Backup & Recovery

Mission Domain	Representative Workloads	Bacula Enterprise Coverage
HPC & AI/ML	DoD Supercomputing Resource Centers, AI training clusters, modeling & simulation, R&D environments	Parallel streams; GPFS, Lustre, BeeGFS native; GUF1 integration; framework-aware (PyTorch, JAX, MLflow)
Classified Networks	SIPRNet, JWICS, special-access program enclaves	True air-gap (CNSSI 4009-2015); offline tape & immutable object; cross-domain transfer-friendly
Tactical / Edge	OCONUS forward operating sites, expeditionary kits, DDIL (Disconnected, Degraded, Intermittent, Limited)	Lightweight Linux footprint; disconnected operation; deduplicated replication when reconnected
Enterprise IT	NIPRNet business systems, Active Directory, Exchange, SQL/Oracle, file & collaboration	54+ application plugins; agent-based and agentless options; granular restore
Cloud (Sovereign & Commercial)	DoD IL2–IL6, JWCC providers (AWS, Azure, Google, Oracle), cloud-native workloads	Object-storage immutability; multi-cloud orchestration; FedRAMP-aligned deployments
Virtualization	VMware, KVM/libvirt, Hyper-V, Proxmox, Nutanix AHV	Image-level and file-level recovery; VMware migration support; hypervisor-agnostic
Containers & DevSecOps	Kubernetes, OpenShift, Platform One / Iron Bank pipelines	Persistent-volume protection; namespace-aware policy; CI/CD-friendly APIs
Operational Technology	Base utility SCADA, weapon-system support infrastructure, ICS/OT historians	IEC 62443-aligned; read-only and offline target support; long-retention tape
Mainframe & Legacy	IBM z/OS, IBM Power (AIX, IBM i), Solaris, HP-UX	Native agents for legacy platforms; sub-capacity-friendly licensing; tape-first workflows

Key Capabilities



Bacula Enterprise provides a comprehensive feature set engineered for the stringent requirements of DoW environments — across security, compliance, scalability, sovereignty, cost, and deployment flexibility.

1. Security & Ransomware Resilience

Immutable backups, air-gapped and encrypted storage for classified and CUI workloads, role-based access control (RBAC) with multi-factor authentication, FIPS 140-validated cryptography for data in transit and at rest, and tamper-evident audit logs aligned with the September 2026 FIPS 140-3 transition.

2. Compliance Enablement (CMMC, NIST, DISA STIG)

Tamper-proof audit logs, centralized policy control, encrypted transfers, secure REST API, and DISA STIG-aligned Linux deployment patterns. Direct mapping to NIST SP 800-171 (CMMC 2.0 Level 2), NIST SP 800-53 Moderate/High, and DoD Impact Levels IL2 through IL6.

3. Cross-Domain Scalability

Parallel backup streams for HPC clusters, native support for GPFS, Lustre, BeeGFS, and standard POSIX filesystems, broad OS coverage (Linux, Unix, Windows, macOS, mainframe, IBM Power), and orchestration across distributed DoW sites — from a tactical kit to a Tier-1 supercomputing facility.

4. Air-Gap & Data Sovereignty

True air-gap aligned with CNSSI 4009-2015 (not just network isolation), offline tape libraries, immutable object storage, and Swiss-headquartered, open-architecture engineering — providing inspectable code paths and a supply chain free of foreign adversary influence.

5. Cost Predictability

Per-core / per-agent licensing — no per-terabyte capacity tax. OPEX scales with infrastructure size, not data growth. Bacula works with any storage hardware, tape system, or DoW-approved cloud, eliminating vendor lock-in and preserving Government Furnished Equipment (GFE) investments.

6. Deployment Flexibility (CONUS / OCONUS)

Runs on hardened Linux distributions used across DoW (RHEL, Rocky, Ubuntu Pro for Government), supports fully disconnected (DDIL) tactical environments, and federates centralized control with local autonomy — critical for forward-deployed and contested communications scenarios.

Compliance Alignment

CMMC 2.0 / NIST SP 800-171 Mapping

Bacula Enterprise capabilities map directly to the NIST SP 800-171 Rev 2 control set that underpins CMMC 2.0 Level 2 — the baseline assessors and C3PAOs use today. The mapping below highlights backup-relevant controls; Bacula's broader feature set supports additional NIST families when integrated with site SIEM, IAM, and configuration management tooling.

Forward path: NIST SP 800-171 Rev 3 (97 controls, finalized May 2024) is the expected future baseline for CMMC, with industry consensus on a 2027–2028 transition window. Bacula's feature set already aligns with Rev 3 control language and DoD-published Organization-Defined Parameters (ODPs) for log retention, encryption, and recovery.

Additional Frameworks & DoW Standards

- NIST SP 800-53 Rev 5 — Moderate and High baselines for federal information systems
- DoD Cloud Computing SRG — Impact Levels IL2 through IL6, including JWCC-aligned deployments
- FedRAMP High — for cloud-hosted Bacula deployments via authorized providers
- DISA STIGs — Linux STIG-aligned hardening guidance for Director, Storage and File Daemon hosts
- CNSSI 4009-2015 — true air-gap definition for classified and high-assurance workloads
- IEC 62443 — for OT/ICS environments at DoW installations and weapon system support infrastructure
- FIPS 140-3 — cryptographic module standard (FIPS 140-2 sunsets to Historical List on Sep 21, 2026)

Bacula Enterprise's Strict Compliance Alignment

NIST SP 800-171 Rev 2 Control (CMMC 2.0 Level 2)	Bacula Systems Capability
3.3.1 / 3.3.2 – Audit logging & accountability	Tamper-evident, immutable audit logs with centralized reporting
3.4.1 / 3.4.2 – Configuration baselines & enforcement	Centralized policy control; templated, version-controlled job definitions
3.6.1 / 3.6.2 – Incident handling & recovery	Fast, large-scale, granular restores; documented RTO/RPO
3.8.7 – Removable media controls	Encrypted, RBAC-controlled tape and removable media handling
3.8.9 – Backup of CUI	Encrypted backup of CUI with role-based recovery (core control)
3.13.8 – Cryptographic protection in transit	TLS-protected transfers using FIPS 140-validated modules
3.13.11 / 3.13.16 – FIPS-validated cryptography & confidentiality at rest	FIPS 140-validated encryption for stored backups; AES-256

Bacula vs. Alternatives



DoW programs increasingly evaluate backup vendors not just on feature parity but on licensing economics, supply-chain risk, and architectural openness. Bacula Enterprise significantly differentiates on each axis.

Bacula Enterprise's Clear Differentiation

Consideration	Bacula Enterprise	Typical Capacity-Priced Alternatives
Licensing model	Per-core / per-agent. Cost scales with infrastructure, not data growth.	Per-TB capacity licensing. Cost grows with every petabyte added.
Architecture openness	Open, scriptable, modular. Inspectable code paths; standards-based protocols.	Proprietary appliances or closed control planes. Vendor lock-in risk.
HPC scale	Native parallel streams; GPFS, Lustre, BeeGFS support; petabyte-proven.	Limited or no HPC filesystem support; struggles past low petabytes.
Air-gap posture	True air-gap aligned with CNSSI 4009-2015 (offline tape, immutable object).	Often “immutable” via cloud-only locks; not equivalent to true air-gap.
Sovereignty	No foreign-adversary supply chain exposure.	U.S. or mixed-jurisdiction ownership; varies by vendor.
DoW reference base	NASA, LANL, Idaho National Laboratory, Sandia, US Air Force, US Navy, Lockheed Martin, Northrup Grumman.	Generally enterprise-IT-centric; thin HPC and classified references.

CONCLUSION

SUMMARY OF OPERATIONAL IMPACT

Bacula Systems delivers significant operational impact across the full DoW data estate — from petabyte-scale supercomputing centers to tactical edge deployments — by reducing downtime from cyber incidents, ensuring an audit-ready posture for CMMC 2.0 and NIST requirements, providing extreme long-term cost efficiency through per-core licensing, and increasing mission resilience in both CONUS and OCONUS operations.

With an open-architecture foundation, true air-gap aligned with CNSSI 4009-2015, FIPS 140-validated cryptography, and reference deployments at LANL, Idaho National Laboratory, Sandia, NASA, and US Air Force/US Navy, Bacula is purpose-built for the scale, security, and sovereignty demands of the modern Department of War.

CONTACT & MORE INFORMATION

For more information, technical specifications, classified-environment deployment patterns, or DoW reference case studies, please contact Bacula Systems. We are ready to support your mission-critical data protection needs across every domain — from the data center to the tactical edge.



+1 800 256 0192



sales@baculasystems.com