carahsoft

Bacula Systems U.S. IC 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

Intelligence Community Solution Brief

Bacula Systems U.S. IC Solution Brief

Secure, Sovereign, and Scalable Backup & Recovery for the U.S. Intelligence Community — Across the Full Mission

AUTHOR

Bacula Systems

TECHNOLOGY

Critical Data Backup and Restore, Data Resilience and Disaster Recovery

DATE

April 4 2026

LEARN MORE

TABLE OF CONTENTS

Introduction

IC Mission Environment

The U.S. Intelligence Community (IC) — the eighteen elements directed by the Office of the Director of National Intelligence (ODNI) — operates the most security-sensitive IT estate in the federal government. Mission systems span Top Secret/SCI networks (JWICS), classified collection and analysis platforms, high-performance computing for cryptanalysis and signals processing, AI/ML on classified corpora, the Commercial Cloud Enterprise (C2E), cross-domain solutions, and the SCIF infrastructure that physically houses them. Each system carries strict compliance, sovereignty, and cyber resilience requirements under ICD 503 and the National Security Systems framework.

Adversary targeting of IC data has expanded from collection sources and methods to the supply chain behind every system that processes them. The January 2026 ODNI cybersecurity modernization announcement underscored the imperative for tamper-proof, recoverable, sovereign data protection across the full IC mission portfolio — at SCI, Secret, and unclassified levels.

WHY BACULA SYSTEMS?

Bacula Enterprise delivers immutable backups, true air-gapped storage aligned with CNSSI 4009-2015, FIPS 140-validated encryption, advanced incremental and synthetic backup levels, and centralized policy control across all IC mission domains — from SCIF-resident classified workloads to C2E cloud deployments — under a single, scriptable, open-architecture platform engineered in Switzerland and free of foreign-adversary supply chain exposure.

OPERATIONAL IMPACT

- Reduced downtime from cyber incidents and ransomware across SCI, Secret, and unclassified domains
- Audit-ready posture for ICD 503, NIST SP 800-53, and CNSSI 1253 categorization
- Long-term cost efficiency for petabyte-scale classified analytic and HPC environments
- Significantly increased mission resilience for collection, analysis, and dissemination systems
- Sovereignty assurance through Swiss-headquartered engineering and inspectable architecture

Mission Domain Coverage

IC data protection is a portfolio of related problems with shared compliance, sovereignty, and resilience requirements. Bacula Enterprise addresses all of them with a single architecture, single licensing model, and single operational toolset — reducing tool sprawl, simplifying ICD 503 certification & accreditation, and consolidating the supply chain.

Cross-Domain Backup & Recovery

Mission Domain	Representative Workloads	Bacula Enterprise Coverage
JWICS / TS-SCI	Top Secret/SCI mission systems, SCIF-resident analytic platforms, special access programs (SAP)	True air-gap (CNSSI 4009-2015); offline tape & immutable object; SCIF-deployable Linux footprint
Classified HPC & Cryptanalysis	Signals processing, modeling & simulation, classified AI/ML training on collected corpora	Parallel streams; GPFS, Lustre, BeeGFS native; framework-aware (PyTorch, JAX)
Mission Analytic Platforms	All-source analysis tools, link analysis, geospatial (NGA-style), entity resolution, knowledge graphs	Database-aware plugins; petabyte-scale; granular point-in-time recovery
Commercial Cloud Enterprise (C2E)	AWS, Microsoft, Google, Oracle, IBM at IC classification levels; cloud-native mission apps	Object-storage immutability; multi-cloud orchestration; cross-CSP portability
Cross-Domain Solutions (CDS)	Data transfer between SCI, Secret, and unclassified enclaves; one-way guards	Standards-based protocols; CDS-friendly file transfer; integrity-verified replication
Counterintelligence & Insider Threat	User activity monitoring repositories, audit archives, forensic data lakes	Tamper-evident retention; immutable audit storage; long-retention tape & object
Enterprise IT (NIPRNet & IC ITE)	Unclassified business systems, IC ITE shared services, AD/Exchange/SQL/file	54+ application plugins; agent-based and agentless; granular restore
Edge & Forward Deployments	Forward-deployed collection platforms, OCONUS field stations, DDIL operations	Lightweight Linux footprint; disconnected operation; deduplicated replication when reconnected
Operational Technology	SCIF infrastructure controls, building security, classified facility utility systems	IEC 62443-aligned; read-only and offline target support; long-retention tape

Key Capabilities

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

1. Security & Ransomware Resilience

Immutable backups, air-gapped and encrypted storage for SCI and SAP 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

Compliance Enablement (ICD 503, NIST SP 800-53, CNSSI 1253)

Tamper-proof audit logs, centralized policy control, encrypted transfers, secure REST API, and DISA STIG-aligned Linux deployment patterns. Direct mapping to NIST SP 800-53 Rev 5 control families (CP, AU, SC, SI), CNSSI 1253 categorization for National Security Systems, and ICD 503 RMF artifact requirements

Cross-Domain Scalability

Parallel backup streams for classified 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 IC sites — from a forward field station to a Tier-1 SCIF-resident supercomputing facility

4. Air-Gap & 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, CNSSP 11-aligned supply chain integrity, and zero foreign-adversary dependency

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 IC-approved cloud (including all C2E providers), eliminating vendor lock-in and preserving Government Furnished Equipment (GFE) investments.

6. Deployment Flexibility (CONUS / OCONUS)

Runs on hardened Linux distributions (RHEL, Rocky, Ubuntu Pro for Government), supports fully disconnected (DDIL) and contested-communications environments, and federates centralized control with local autonomy — critical for forward-deployed collection platforms and OCONUS field stations.

Compliance Alignment

ICD 503 / NIST SP 800-53 Mapping

IC systems are categorized under CNSSI 1253 and accredited under ICD 503 using the NIST SP 800-53 Rev 5 control catalog tailored for National Security Systems. Bacula Enterprise capabilities map directly to the backup-, audit-, and integrity-relevant control families. The mapping below highlights the controls Bacula most directly enables; the broader feature set supports additional families when integrated with site SIEM, ICAM, and configuration management tooling.

Bacula's architecture is engineered to satisfy CP-9 "System Backup" as a primary capability rather than a bolted-on feature — including the CP-9 enhancements most often invoked at the Moderate and High categorization baselines: cryptographic protection (CP-9(8)), separate storage (CP-9(1)), and protection from unauthorized modification (CP-9(5)) via immutable storage.

Bacula Enterprise's Strict Compliance Alignment

NIST SP 800-53 Rev 5 Control (per DOE Order 205.1B)	Bacula Systems Capability
CP-9 — System backup	Encrypted, scheduled, verified backups of mission and audit data (core control)
CP-10 — System recovery & reconstitution	Fast, large-scale, granular restores; documented RTO/RPO; bare-metal recovery
AU-2 / AU-3 / AU-9 — Audit events, content & protection	Tamper-evident, immutable audit logs with centralized reporting
CM-3 — Configuration change control	Centralized policy control; templated, version-controlled job definitions
IR-4 — Incident handling	Recovery integration with incident response; isolated restore environments
MP-6 — Media sanitization	Encrypted, RBAC-controlled tape and removable media handling
SC-8 / SC-13 — Transmission confidentiality & cryptographic protection	TLS-protected transfers using FIPS 140-validated modules
SC-28 — Protection of information at rest	FIPS 140-validated encryption for stored backups; AES-256
SI-7 — Software, firmware & information integrity	Immutable storage targets and integrity verification on restore

Additional Frameworks & IC Standards

- **ICD 503** — Information Technology Systems Security Risk Management, Certification and Accreditation
- **ICD 705** — Sensitive Compartmented Information Facilities (SCIF) — Bacula deployable inside SCIF boundaries
- **CNSSI 1253** — Security Categorization and Control Selection for National Security Systems
- **CNSSI 4009-2015** — National Information Assurance Glossary (true air-gap definition)
- **CNSSP 11** — National Policy Governing the Acquisition of IA Products (sovereignty considerations)
- **NIST SP 800-37 Rev 2** — Risk Management Framework, applied to NSS via CNSSI 1253
- **FIPS 140-3** — cryptographic module standard (FIPS 140-2 sunsets to Historical List on Sep 21, 2026) Available via Carahsoft, Bacula Systems' exclusive Intelligence Community channel partner6)

Bacula vs. Alternatives

IC procurement evaluates backup vendors on supply-chain sovereignty, architectural openness, and licensing economics at petabyte scale — not just feature parity. Bacula Enterprise differentiates significantly on each axis

Bacula Enterprise's Clear Differentiation

Consideration	Bacula Enterprise	Typical Capacity-Priced Alternatives
Sovereignty	No foreign-adversary supply chain exposure. CNSSP 11 friendly.	U.S. or mixed-jurisdiction ownership; opaque global supply chains.
Architecture openness	Open, scriptable, modular. Inspectable code paths; standards-based protocols.	Proprietary appliances or closed control planes. Limited inspectability.
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.
Classified HPC scale	Native parallel streams; GPFS, Lustre, BeeGFS support; petabyte-proven.	Limited or no HPC filesystem support; struggles past low petabytes.
Licensing model	Per-core / per-agent. Cost scales with infrastructure, not data growth.	Per-TB capacity licensing. Cost grows with every petabyte added.
IC-component reference base	DOE national laboratories (LANL, INL, Sandia), NASA, Us Army, Us Navy, Lockheed Martin, Northrup Grumman.	Generally enterprise-IT-centric; thin classified and HPC references.
Tape & HSM integration	First-class tape; integrates with HPSS, Versity, Spectra Logic, IBM, Quantum.	Tape often deprioritized in favor of vendor cloud lock-in.

CONCLUSION

SUMMARY OF OPERATIONAL IMPACT

Bacula Systems delivers significant operational impact across the full Intelligence Community mission — from SCIF-resident classified analytic platforms to forward-deployed collection sites — by reducing downtime from cyber incidents, ensuring an audit-ready posture for ICD 503 and NIST SP 800-53 requirements, providing extreme long-term cost efficiency through per-core licensing, and increasing mission resilience across SCI, Secret, and unclassified domains.

With an open-architecture foundation, true air-gap aligned with CNSSI 4009-2015, FIPS 140-validated cryptography, exclusive IC channel availability through Carahsoft, and reference deployments at LANL, Idaho National Laboratory, and Sandia, Bacula is purpose-built for the scale, security, and sovereignty demands of the modern Intelligence Community.

CONTACT & MORE INFORMATION

For more information, technical specifications, classified-environment deployment patterns, or IC-component reference engagements, please contact Bacula Systems or your Carahsoft account team. We are ready to support your mission-critical data protection needs across every IC domain — from the SCIF to the field station.

+1 800 256 0192 sales@baculasystems.com