

# Bacula Systems DoE 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](https://carahsoft.com)



Explore More Resources:  
[carah.io/BaculaSystemsResources](https://carah.io/BaculaSystemsResources)



Join Events & Webinars:  
[carah.io/BaculaSystemsEvents](https://carah.io/BaculaSystemsEvents)



Discover Technology Solutions:  
[carah.io/BaculaSystemsSolutions](https://carah.io/BaculaSystemsSolutions)



Learn About Procurement:  
[carah.io/BaculaSystemsContracts](https://carah.io/BaculaSystemsContracts)



Connect With Our Team:  
[BaculaSystems@carahsoft.com](mailto:BaculaSystems@carahsoft.com)  
571-590-4040



Department of Energy Solution Brief

# Bacula Systems DoE Solution Brief

Secure, Compliant, and Exascale-Ready Backup & Recovery for the  
U.S. Department of Energy — From the National Labs to the Grid

## AUTHOR

Bacula Systems

---

## TECHNOLOGY

Critical Data Backup and Restore, Data Resilience and  
Disaster Recovery

---

## DATE

April 4 2026

---

LEARN MORE



# TABLE OF CONTENTS

---

|                                                 |          |
|-------------------------------------------------|----------|
| <b>Introduction</b>                             | <b>3</b> |
| DoE Mission Environment                         | 3        |
| Why Bacula Systems?                             | 3        |
| Operational Impact                              | 3        |
| <b>Mission Domain Coverage</b>                  | <b>4</b> |
| Cross-Domain Backup & Recovery                  | 4        |
| <b>Key Capabilities</b>                         | <b>5</b> |
| Security & Ransomware Resilience                | 5        |
| Compliance Enablement                           | 5        |
| Cross-Domain Scalability                        | 5        |
| Air-Gap & Data Sovereignty                      | 5        |
| Cost Predictability                             | 6        |
| Deployment Flexibility (Lab to Grid)            | 6        |
| <b>Compliance Alignment</b>                     | <b>6</b> |
| DOE Order 205.1B / NIST SP 800-53 Mapping       | 6        |
| Additional Authorities                          | 7        |
| Bacula Enterprise's Strict Compliance Alignment | 7        |
| <b>Bacula vs. Alternatives</b>                  | <b>8</b> |
| DoE Reference Customers                         | 8        |
| <b>Conclusion</b>                               | <b>9</b> |

---

---

# Introduction

---



## DoE Mission Environment

The U.S. Department of Energy (DoE) operates the largest portfolio of federal scientific computing in the world — including three of the planet’s most powerful supercomputers (Frontier at ORNL, Aurora at ANL, and El Capitan at LLNL) — alongside nuclear weapons design under the National Nuclear Security Administration (NNSA), basic and applied energy research across the Office of Science laboratories, long-tail environmental management archives, naval nuclear propulsion, and grid-scale operational technology at the Power Marketing Administrations. Each mission carries distinct data protection, compliance, and retention requirements — but all share a common imperative: uncompromising security, extreme scale, and preservation of irreplaceable scientific and national security data.

DoE’s recently announced Genesis Mission — the AI-for-Science initiative spanning the national lab complex — further raises the stakes on data protection. Foundation model checkpoints, training corpora, and experimental datasets now demand the same recoverability guarantees long required of NNSA classified workloads, but at orders-of-magnitude greater scale and throughput.

---

## WHY BACULA SYSTEMS?

Bacula Enterprise delivers immutable backups, true air-gapped storage, FIPS 140-validated encryption, and centralized policy control across the full DoE mission portfolio — from exascale HPC and AI training infrastructure to NNSA classified enclaves, light-source data archives, environmental management retention, and Power Marketing Administration OT — under a single open-architecture platform with no per-terabyte licensing tax. Bacula is already deployed at LANL, Idaho National Laboratory, and Sandia.

## OPERATIONAL IMPACT

- Recovery economics that scale to exascale data growth without per-TB licensing penalties
- Audit-ready posture for DOE Order 205.1B, NIST SP 800-53, and NNSA classified-system requirements
- Long-term retention efficiency for environmental management, scientific archive, and regulatory data
- Ransomware resilience for unclassified, CUI, and classified DoE workloads alike
- Sovereignty assurance through Swiss-headquartered engineering and inspectable architecture

# Mission Domain Coverage



DoE data protection spans more domains, more scale, and more retention regimes than any other federal department. Bacula Enterprise addresses all of them with a single architecture, single licensing model, and single operational toolset — reducing tool sprawl, simplifying lab-by-lab Authority to Operate (ATO) processes, and consolidating the supply chain across the seventeen national laboratories and DoE field sites.

## Cross-Domain Backup & Recovery

| Mission Domain                  | Representative Workloads                                                                                 | Bacula Enterprise Coverage                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Exascale & Leadership HPC       | Frontier (ORNL), Aurora (ANL), El Capitan (LLNL), Perlmutter (NERSC), Polaris (ANL)                      | Parallel streams; native GPFS, Lustre, BeeGFS; GUFI integration (LANL provenance); HPCAccelerator |
| NNSA Classified                 | Nuclear weapons design, stockpile stewardship, RD/FRD/UCNI workloads at LANL, LLNL, Sandia, Y-12, Pantex | True air-gap (CNSSI 4009-2015); offline tape & immutable object; SAP-friendly deployment          |
| Office of Science Computing     | ASCR facilities, NERSC, ALCF, OLCF; open-science research data, simulation outputs                       | Petabyte-scale orchestration; long-term archive integration; HSM and tape-tier integration        |
| AI / ML for Science (Genesis)   | Foundation model training, scientific ML, model checkpoints, training corpora preservation               | Framework-aware (PyTorch, JAX, MLflow, Kubeflow); Megatron/DeepSpeed checkpoint protection        |
| Light Sources & User Facilities | APS (ANL), NSLS-II (BNL), LCLS (SLAC), ALS (LBNL); high-throughput experimental data                     | Streaming ingest; high-throughput backup; immutable archive for irreplaceable beam-time data      |
| Environmental Management        | Hanford, Savannah River, Oak Ridge cleanup; multi-decade regulatory and waste-form retention             | Long-retention tape; cryptographically verified provenance; cost-efficient cold-tier storage      |
| Power Marketing Administrations | BPA, WAPA, SWPA, SEPA grid OT; SCADA, EMS, market systems; NERC CIP-regulated assets                     | IEC 62443-aligned; NERC CIP retention support; offline target & long-retention tape               |
| Naval Reactors                  | Submarine and carrier propulsion design data, classified engineering archives                            | True air-gap; granular long-term restore; controlled access via RBAC + MFA                        |
| Enterprise IT & EIA             | Energy Information Administration, headquarters business systems, lab business IT                        | 54+ application plugins; agent-based and agentless options; granular restore                      |

# Key Capabilities



Bacula Enterprise provides a comprehensive feature set engineered for the stringent requirements of DoE environments — across security, compliance, exascale scalability, sovereignty, cost, and the full deployment spectrum from leadership computing facility to substation.

## 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 (DOE 205.1B, NIST, NERC CIP))

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 (DoE federal baseline), NIST SP 800-171 for contractor CUI environments, CNSSI 1253 for NNSA classified systems, and NERC CIP for Power Marketing Administration OT.

## 3. Exascale & Cross-Domain Scalability

Parallel backup streams engineered for leadership-class HPC, native support for GPFS, Lustre, and BeeGFS, GUFI integration (Grand Unified File Index, originated at LANL) for filesystem intelligence at scale, and framework-aware protection of AI training infrastructure (PyTorch, JAX, MLflow, Kubeflow, DeepSpeed, Megatron-LM).

## 4. Air-Gap & Data Sovereignty

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

## 5. Cost Predictability

Per-core / per-agent licensing — no per-terabyte capacity tax. OPEX scales with infrastructure size, not data growth — a critical economic property as DoE moves from petascale to exascale to multi-exascale data estates. Bacula works with any storage hardware, tape system, or DoE-approved cloud, preserving lab investments in HPSS, Versity, Spectra Logic, and existing tape infrastructure.

## 6. Deployment Flexibility (Lab to Grid)

Runs on hardened Linux distributions used across DoE labs (RHEL, Rocky, SUSE), supports fully disconnected environments, and federates centralized control with local lab autonomy — preserving the operational independence each lab and field site requires while standardizing the underlying platform.

---

# Compliance Alignment

---



## DOE Order 205.1B / NIST SP 800-53 Mapping

DoE federal systems are governed by DOE Order 205.1B (Department of Energy Cyber Security Program), which tailors NIST SP 800-53 Rev 5 to the DoE mission. Contractor systems handling Controlled Unclassified Information additionally apply NIST SP 800-171 Rev 2. NNSA classified systems are categorized under CNSSI 1253. Bacula Enterprise capabilities map directly to the backup-, audit-, and integrity-relevant control families across all three regimes.

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 that govern DoE national security and CUI systems: 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 & DoE Standards

- DOE Order 205.1B – Department of Energy Cyber Security Program
- DOE Order 471.6 – Information Security Manual (classified information protection)
- DOE Order 470.4B – Safeguards and Security Program
- NIST SP 800-37 Rev 2 – Risk Management Framework
- NIST SP 800-171 Rev 2 – protection of CUI in contractor (M&O) environments
- CNSSI 1253 – categorization for NNSA and other DoE National Security Systems
- CNSSI 4009-2015 – true air-gap definition for classified workloads
- NERC CIP – for Power Marketing Administration grid OT environments
- FIPS 140-3 – cryptographic module standard (FIPS 140-2 sunsets to Historical List on Sep 21, 2026)



# Bacula vs. Alternatives



DoE procurement evaluates backup vendors at a scale and across a span of mission types unmatched in the federal government. Bacula Enterprise differentiates significantly on the axes that matter most to DoE labs and field sites.

## Bacula Enterprise's Clear Differentiation

| Consideration            | Bacula Enterprise                                                             | Typical Capacity-Priced Alternatives                               |
|--------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Exascale economics       | Per-core / per-agent. Cost flat as data grows from PB to EB.                  | Per-TB licensing. Cost scales linearly with the data tsunami.      |
| HPC filesystem support   | Native GPFS, Lustre, BeeGFS; GUF-aware; HPCAccelerator.                       | Limited or no parallel filesystem support; struggles past low PB.  |
| DoE deployment footprint | Live at LANL, Idaho National Laboratory, and Sandia.                          | Few backup vendors carry production references at NNSA-scale labs. |
| Architecture openness    | Open, scriptable, modular. Inspectable code paths.                            | Proprietary appliances or closed control planes.                   |
| Air-gap posture          | True air-gap aligned with CNSSI 4009-2015 (offline tape, immutable object).   | Often “immutable” via cloud-only locks; not equivalent.            |
| Sovereignty              | Swiss-headquartered. No foreign-adversary supply chain exposure.              | U.S. or mixed-jurisdiction ownership; opaque global supply chains. |
| Tape & HSM integration   | First-class tape; integrates with HPSS, Versity, Spectra Logic, IBM, Quantum. | Tape often deprioritized in favor of vendor cloud lock-in.         |

## DoE Reference Customers

- Los Alamos National Laboratory (LANL) — NNSA nuclear weapons design, classified HPC
- Idaho National Laboratory (INL) — nuclear energy research and national security HPC
- Sandia National Laboratories — NNSA nuclear deterrent stockpile stewardship and classified HPC
- NASA — large-scale scientific computing and mission-critical engineering data

# CONCLUSION

## SUMMARY OF OPERATIONAL IMPACT

Bacula Systems delivers significant operational impact across the full DoE mission portfolio — from exascale leadership computing facilities to NNSA classified enclaves to Power Marketing Administration grid OT — by reducing downtime from cyber incidents, ensuring an audit-ready posture for DOE Order 205.1B and NIST SP 800-53 requirements, providing the only licensing economics that scale linearly with infrastructure rather than data growth, and increasing mission resilience across unclassified, CUI, and classified domains.

With an open-architecture foundation, true air-gap aligned with CNSSI 4009-2015, FIPS 140-validated cryptography, native exascale HPC capability, and existing production deployments at LANL, Idaho National Laboratory, and Sandia, Bacula is purpose-built for the scale, security, and sovereignty demands of the modern Department of Energy.

## CONTACT & MORE INFORMATION

For more information, technical specifications, exascale deployment patterns, NNSA classified-environment guidance, or DoE lab reference engagements, please contact Bacula Systems. We are ready to support your mission-critical data protection needs across every DoE domain — from leadership-class HPC to the substation.



+1 800 256 0192



[sales@baculasystems.com](mailto:sales@baculasystems.com)