

An Air Gap You Can Prove

Isolated Recovery for
Federal, Defense and
Critical Infrastructure

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/baculasystems



Learn About Procurement:
carah.io/BaculaSystemsContracts



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



Bacula Enterprise Air-Gapped Edition

An Air Gap You Can Prove

Isolated recovery for federal, defense and critical infrastructure

Air-Gapped Edition

Bacula Enterprise · 2026



BACULA SYSTEMS

Enterprise data protection · Swiss-headquartered · open-source core

WHAT THIS DOCUMENT IS

The governing definition of an air gap, decomposed into requirements a customer or an assessor can test, and an honest account of where Bacula meets them today. It is not a feature list. A significant part of this market sells immutable cloud storage as an air gap; against the definition it is not one, and a claim that cannot survive testing is worse than no claim at all.

01**Why this conversation, and why now**

The term air gap is used loosely, and it has a governing definition. CNSSI 4009-2022, adopted from IETF RFC 4949 version 2 and carried in the NIST glossary, defines it as an interface between two systems at which they are not connected physically and any logical connection is not automated. Two clauses, about a single interface. Not an architecture, not a facility, not a security program. Where a claim is tested — in an assessment, in a contract dispute, after an incident — that is the text it is tested against.

Meeting it has become a contract condition rather than a design preference. CMMC entered the Federal Acquisition Regulation on 10 November 2025 and is phasing into Department of Defense contracts, carrying the NIST SP 800-171 control set for controlled unclassified information. NIST SP 800-53 CP-9 and CP-10 remain the federal baseline for backup and for system recovery and reconstitution. The DOE and NNSA complex flows equivalent requirements down to its contractors. In each case someone is now asking a question about recovery that most estates cannot answer.

What a federal or defense buyer is now obliged to do

The definition is the standard. These are the regimes that make meeting it a contract condition.

CNSSI 4009-2022 The definition	Adopted from IETF RFC 4949 version 2 and carried in the NIST glossary. Two clauses about a single interface: not connected physically, and any logical connection not automated. This is the standard a claim is tested against.
CMMC 48 CFR rule effective Nov 2025	Phasing into DoD contracts across four phases. Built on the NIST SP 800-171 control set for CUI, including the protection of backup data at storage locations.
NIST SP 800-53 Federal baseline	CP-9 information system backup and CP-10 system recovery and reconstitution. The controls an authorizing official examines, and the ones continuous monitoring reports against.
DOE and NNSA Laboratory complex	Flowed-down contractor requirements documents, operational technology scope, and estates where disconnection is the normal operating state rather than an exception.
ICS and OT Critical infrastructure	Environments already segmented from enterprise networks, where the recovery path is frequently the one route back in and the one nobody has tested.

Each of them asks whether the data comes back. None is satisfied by a copy nobody has tried to restore.

02**What an air gap actually requires**

Two of the five requirements below are definitional and three are evidentiary, and the distinction is worth keeping clear. A1 and A2 are the definition itself: no physical path at the interface outside a transfer event, and any transfer that does occur happening only because a person caused it. E1, E2 and E3 are not part of the definition — they are what a customer, an assessor or a court would need in order to believe A1 and A2. Conflating the two is how this conversation usually goes wrong.

The definition, decomposed into testable requirements

Two clauses define the gap. Three more are what an assessor needs in order to believe them.

A1 No physical path exists at the interface outside a transfer event	Definitional
A2 Any transfer across the interface occurs only under human control	Definitional
E1 The disconnected state can be demonstrated by someone other than the operator	Evidentiary
E2 Every transfer event is recorded: who authorized it, when it opened and closed, what crossed	Evidentiary
E3 The state cannot be changed by the system being protected against	Evidentiary

E3 is where most products fail. If the backup software, or a credential it holds, can re-establish the path, the gap is not under anyone else's control — and the correct term is enforced isolation, not an air gap.

E3 is where most products fail, and where the honest boundary sits. A robotic tape library is the clearest case. Media inside a library that the backup software can command a robot to mount is not air-gapped: no human action is required, and a physical path can be established on demand. The same media in an export slot, removed by a person, is air-gapped. The gap begins where the software's reach ends, which is why the question to ask of any implementation is not how strong the protection is but who can undo it.

2.1 A property of one interface, not of a system

The definition concerns a single interface between two systems, not every interface in an estate. A backup server with network interfaces is not disqualified. What matters is the interface across which the protected copy is reached, and whether a signal could traverse it at all. That is an observable physical state, confirmable by looking at the equipment, which is precisely why the definition is written the way it is: it is meant to be verifiable without trusting anyone's configuration.

Nor does the definition require permanent disconnection. It describes the state of an interface during the period in question, not a condition that must hold forever. An interface that is closed, opened under human control for a transfer, and closed again satisfies both clauses throughout, provided nothing automated can open it.

WHAT IT IS

03

Bacula Enterprise Air-Gapped Edition

An edition of Bacula Enterprise for organizations that have to meet the definition and to show that they meet it. The platform underneath is the same one every other Bacula deployment runs; the edition is the packaging, the compliance mapping and the evidence, not a separate codebase or a fork carrying its own defect history.

Property	What it means in an air-gapped deployment
Tape write, export and removal	Mature and long-standing, with export lists, barcode tracking and pool definitions. The unambiguous case: no physical path, and a transfer that requires a person. The definition is met here today, without qualification.
Removable disk as a target	Supported today and equivalent to tape in definitional terms. Different handling economics, the same standing against both clauses.
Own volume format on any target	Recovery requires the software and the media, not a particular storage product, a vendor appliance, or a cloud account that has to still exist and still be reachable.

Property	What it means in an air-gapped deployment
No outbound connectivity	No component requires an outbound connection to operate — no license call-home and no entitlement check. Not required by the definition, but it settles the obvious question about what the software reaches when nobody is watching.
Catalog and configuration protected with the data	What makes the isolated copy independently usable. A copy that cannot be read without the system that wrote it is not a recovery position.
Key custody with the customer	Keys are customer-held. No key management vendor is named, required or integrated as a dependency.
Open-source core	The core is open source and auditable, which matters where an assessor is entitled to establish what the software can and cannot reach.

04

What the definition does not require

What the definition requires, and what gets imported into it

Most of the complexity in this area is people adding requirements the definition does not contain.

In the definition	Imported, and not required
No physical path across the interface outside a transfer event, and any transfer happening only because a person caused it. Two clauses about one interface, both verifiable by inspection rather than by trusting a configuration.	Permanent disconnection. A SCIF. Encryption. Immutability or write-once media. Data diodes. Purpose-built hardware. No network interfaces anywhere in the system. All valuable; none of it decides whether a gap exists.

An air gap is narrow, not impractical. Discarding the imported requirements is most of the simplification available.

Most of the complexity in this area is people adding requirements the definition does not contain, and then concluding that an air gap is impractical. It is not impractical. It is narrow. A SCIF and physical security controls come from other standards governing classified environments. Encryption is valuable, required elsewhere, and irrelevant to whether a gap exists. Immutability and write-once media address a different threat. Data diodes do not create an air gap at all — strictly they create a controlled one-way path, which is a different thing with different properties. None of it decides the question.

The practical consequence is that an air gap is available to most organizations today, using equipment they already own, without a construction project or a purpose-built appliance. What is usually missing is not the gap. It is the record that the gap was there.

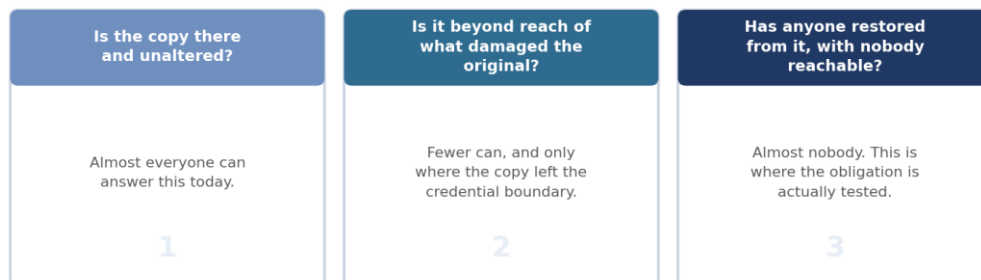
Implementation	Against the definition
Tape, exported and physically removed by a person	MET. No physical path, and transfer requires a human. This is what the definition describes.
Removable disk, disconnected and removed	MET. Equivalent to tape in definitional terms.
Storage system disconnected by link control outside the backup software	MET, where the control genuinely lies outside the software's reach. Where it does not, see the row below.
Storage system whose link the backup software can re-enable	NOT MET. This is enforced isolation, not an air gap. The distinction matters, and we state it rather than blur it.
Tape in a robotic library the software can command	NOT MET. A physical path can be established on command, with no human action.

Implementation	Against the definition
Immutable object storage with object lock	NOT MET. Permanently connected and logically automated. Valuable against a different threat; not an air gap under either clause.
THE ARGUMENT	

05

What an assessor actually tests

What an assessor asks, and who can answer



A dated record of a recovery performed by your own engineers, with every supplier unreachable, is the artifact the third question needs.

An authorizing official examining CP-9 and CP-10, a CMMC assessor working the NIST SP 800-171 controls, and a laboratory reviewing a flowed-down requirement all have the same three questions available. Does a copy exist. Is it beyond the reach of whatever damaged the original. Has anyone ever restored from it. Most of the market can answer the first two.

A copy nobody has attempted to restore is not a recovery capability, it is an assumption. What satisfies an assessor — and what satisfies a program office, which is the harder audience — is a dated record of a recovery actually performed, against a stated scope, with the time it took written down and the failures named. That record is the deliverable almost no vendor in this category produces.

5.1 The witnessed recovery test

A short, bounded engagement with a specific shape. It disturbs nothing in the estate, requires no architectural decision, and produces a written result whether it passes or fails.

- ▶ Scope agreed and written down before the test, and the result recorded against that scope.
- ▶ Your own personnel perform the recovery. We observe and record; we do not drive.
- ▶ No supplier reachable during the test, including us.
- ▶ Recovery time and recovery point measured against the objectives you have stated, not against ideal conditions.
- ▶ A failed test produces a report and an itemized list of what prevented recovery. Remediation is a separate scope and a separate conversation.

As a commercial instrument this is unusually effective, because it costs a day or two, tells an organization something uncomfortable it did not previously know, and converts into an architecture conversation on its own evidence rather than on a vendor's assertion. The resulting record is the artifact an assessor asks for and the one almost nobody holds.

06

The commercial model

Element	Position
No capacity pricing	Bacula does not charge for protected capacity in any form — no front-end terabyte, no storage-based metering. This is a standing commitment, and it holds for tape and removable media as it does for everything else.
Levels, editions and tiers	Three separate things. The Level is the platform feature set — Core, Advanced or Premium. The Edition is the market package, Air-Gapped for this market or Sovereign for Europe. The Tier is the subscription tier on the price list, with isolated recovery added against it rather than as a fourth axis.
Services	Commissioning, witnessed recovery tests and an annual attestation. The attestation is recurring rather than a one-off project, and is priced that way.
Purchasing vehicle	Where an agreement or a federal vehicle already exists it becomes the purchasing vehicle. Where one does not, a direct subscription against the level and tier you choose is the whole of it — no framework to negotiate first, and no minimum commitment.

07

Where to start

#	Step	Who
1	A technical session on the architecture and, as importantly, where it does not fit.	Both, one hour
2	Identify the interface that has to hold, and the estate behind it.	You
3	Run one witnessed recovery test against that estate.	Both
4	Agree the commercial shape — level, tier and the services scope.	Both
5	Record the result and the gaps, whichever way the test goes.	Both

The third step is the one that decides this. If a witnessed test produces a result you did not expect, the rest of the conversation writes itself. If it passes cleanly, you hold a dated record worth showing to any assessor or program office that asks, and we have learned something about our own product. Both outcomes are worth the day they cost, which is the reason we would rather start there than with a presentation.