JobBOSS² (JobBOSS Squared) Within the CMMC Boundary

Hosting, Shared Responsibility, and the FedRAMP Equivalency Question for the Current Edition

David W. Koran

CyberAB Registered Practitioner Advanced

May 24, 2026

From Where the Server Sits to Who Is Responsible

A companion paper has already addressed the legacy E2 and JobBOSS systems that run on a server in the contractor's own building. This paper addresses the current product, JobBOSS2, and the question changes when the product changes. For a legacy on-premises system, the controlling question is where the data lives and how the contractor protects it, because the contractor owns every layer from the operating system down to the room the server sits in. For the current product, the controlling question becomes who is responsible for what, because JobBOSS2 is frequently hosted by the vendor rather than installed on the contractor's hardware, and a hosted arrangement divides responsibility between the vendor and the contractor rather than placing all of it on a single party.

JobBOSS2 is the product ECI Software Solutions built by bringing the earlier JobBOSS and E2 lines into a single platform, and ECI describes it as a cloud-native ERP for job shops and make-to-order manufacturers. ECI brands the product as JobBOSS with a superscript two, written here as JobBOSS2 for readability and for consistency with how the product is most often searched. It is offered in more than one place. It can be installed on premises on the contractor's own server, it can be hosted by the vendor in a commercial cloud, and it can be hosted by the vendor in a separate government cloud offering built for defense work. Each of those arrangements carries a different answer to the CMMC question, and a contractor that does not know which arrangement it is using cannot answer the question at all.

The regulatory baseline is the same as for the legacy systems. The Cybersecurity Maturity Model Certification program, codified at 32 CFR Part 170 and effective December 16, 2024, requires a contractor that processes, stores, or transmits Controlled Unclassified Information to implement the 110 security requirements of NIST Special Publication 800-171 Revision 2 and to demonstrate that implementation through a Level 2 assessment. What the hosted case adds is a second body of requirements that

govern the use of an external cloud service to hold CUI, and those requirements are where this paper concentrates.

The Determination That Comes First

Before any of the hosting analysis, a contractor has to determine whether the data inside its shop management system is actually CUI, and that determination follows the contract markings and the flow-down terms rather than an assumption. Defense work routinely brings CUI into the shop in the form of technical data, drawings, and specifications tied to the contract, and that data flows into the quotes, job travelers, routings, inspection records, and purchase orders the ERP holds. When the contract data carries the CUI designation, the data inside JobBOSS2 is CUI, and if that data will sit in a vendor-hosted environment, the cloud requirements attach. If the determination is that the data is not CUI, the cloud rule does not apply, and the analysis stops here.

The Three Ways JobBOSS2 Is Deployed

Once the data is confirmed to hold CUI, the next step is to establish which of three arrangements the contractor uses, because each leads to a different requirement. The table below maps the deployments to what governs them.

Deployment, where CUI lives, and what governs it

Deployment	Where CUI lives	What governs it
Installed on premises on the contractor's server	The contractor's own system, on Microsoft SQL Server	The on-premises control work in the companion paper; no external cloud service provider and no FedRAMP obligation
Vendor-hosted, commercial cloud tier	The vendor's commercial environment	Not an appropriate home for CUI unless the specific offering used for it is FedRAMP Moderate authorized or equivalent

Vendor-hosted, government cloud offering	AWS GovCloud or Azure Government	The cloud rule for CUI, FedRAMP Moderate authorization or equivalency, plus the shared-responsibility analysis

The on-premises option returns the contractor to the companion paper. The two hosted options are the subject of this paper, and the distinction between the commercial tier and the government tier matters, because they are not the same environment and do not carry the same protections.

The Cloud Rule for CUI

When a contractor uses an external cloud service to store, process, or transmit CUI, DFARS 252.204-7012 governs the arrangement. The clause requires the contractor to require and ensure that the cloud service meets security requirements equivalent to the FedRAMP Moderate baseline and that it supports the cyber incident reporting, forensic analysis, and media preservation obligations set out in paragraphs (c) through (g) of the clause. The CMMC final rule carries this into the assessment. An external cloud service that handles CUI is within the assessment scope, and the C3PAO evaluates it as part of the Level 2 assessment rather than taking it on faith. With the implementing clause DFARS 252.204-7021 in effect since November 10, 2025, CMMC requirements are now being inserted into applicable Department of Defense solicitations and contracts under the program's phased rollout, rather than waiting on a future date.

There are two ways for a cloud offering to satisfy the rule. The first is authorization on the FedRAMP Marketplace at the Moderate level or higher, which is the simpler and more transparent route, because the contractor can verify the status by checking the Marketplace listing directly. The second is FedRAMP Moderate equivalency, a defined alternative for offerings that have not pursued a full FedRAMP authorization. Equivalency is more demanding than the word suggests, and the next section sets out what it requires, because the distance between a marketing claim and the actual standard is where most contractors are exposed.

What FedRAMP Moderate Equivalency Actually Requires

The Department of Defense defined equivalency in a memorandum dated December 21, 2023, titled Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings. To be considered FedRAMP Moderate equivalent, a cloud service offering must achieve 100 percent compliance with the latest FedRAMP Moderate security control baseline, with no control-related findings and no open plans of action remaining from the assessment, evaluated by a FedRAMP-recognized third-party assessment organization applying standard FedRAMP methodology, including a penetration test. The offering must produce a body of evidence, consisting of the system security plan, the security assessment plan, the security assessment report prepared by the third-party assessor, and the plan of action and milestones, and present that body of evidence to the contractor, with the Defense Industrial Base Cybersecurity Assessment Center able to review it.

The FedRAMP Moderate equivalency standard

Element	What it means
100 percent of the FedRAMP Moderate baseline	Every control implemented, with no exceptions
No open findings or plans of action from the assessment	All POA&M items from the 3PAO assessment must be corrected and validated as closed before equivalency is recognized, unlike a FedRAMP authorization, which can carry open items
Third-party assessment	Performed by a FedRAMP-recognized 3PAO, not a vendor self-attestation
Penetration test	Included within the assessment methodology

Body of evidence	SSP, SAP, SAR, and POA&M, presented to the contractor and available to DIBCAC
Letter of attestation	The 3PAO deliverable a contractor relies on to confirm the result

Operational plans of action that arise later, during the continuous monitoring of an authorized offering, are evaluated separately and do not by themselves defeat equivalency. The prohibition is on leaving assessment findings unresolved as a substitute for compliance at the conclusion of the assessment.

The point the memorandum settled is that running on a FedRAMP-authorized platform is not the same as the offering being equivalent. A vendor can build its product on AWS GovCloud or Azure Government, both of which carry FedRAMP authorization at the infrastructure layer, and the product itself can still fall short of equivalency, because the controls that determine the outcome operate at the application and operational layers the vendor runs on top of that infrastructure. The authorized platform is necessary and not sufficient. The offering itself must be assessed and must attest, and a contractor cannot satisfy the cloud rule by pointing to the platform underneath the offering.

What ECI Publishes, and What It Means

ECI publishes that JobBOSS2 and its M1 product are hosted within AWS GovCloud and Azure Government environments that carry FedRAMP High authorization, that the products are able to handle Controlled Unclassified Information, and that the company is advancing toward FedRAMP Moderate Equivalency for JobBOSS2 and M1. ECI has separately announced that the products were designed to comply with CMMC 2.0 standards following third-party readiness assessments. These are ECI's published statements as of the writing of this paper, and a contractor relying on them should read them precisely.

Read precisely, those statements describe an infrastructure that is FedRAMP authorized and an equivalency effort that is in progress. No public evidence is available that the specific JobBOSS2 or M1 cloud service offering used to store, process, or transmit CUI

has achieved either a FedRAMP Moderate authorization, which would appear on the FedRAMP Marketplace, or a FedRAMP Moderate equivalency confirmed by a third-party assessment organization's letter of attestation. This is worth noting because the achievement is demonstrable and the vendors who reach it generally announce it. A number of providers serving the defense market, including secure collaboration platforms and an enterprise resource planning vendor, have publicly announced FedRAMP Moderate equivalency for their offerings, each citing an assessment by a FedRAMP-recognized third-party organization and a letter of attestation. The published record for JobBOSS2 describes progress toward the standard rather than its completion. A contractor should not treat the descriptive language as proof. It should verify the current status directly with ECI, check the FedRAMP Marketplace, and request the customer responsibility matrix, the letter of attestation, and the body of evidence for the specific offering that will hold its CUI.

Three things are easy to run together, and keeping them apart is what protects the contractor. The FedRAMP authorization of the underlying infrastructure, AWS GovCloud or Azure Government, is a property of the platform the vendor builds upon. A vendor statement that a product is able to handle CUI or is ready for CMMC is a readiness claim about the software rather than a certification of the contractor. And the contractor's own CMMC status is something only the contractor can hold, through its own assessment. None of the three substitutes for the others. The C3PAO conducting the Level 2 assessment will look for the Marketplace authorization or the body of evidence behind an equivalency claim, not for the marketing language, and a contractor that cannot produce one of those for the environment holding its CUI has a finding rather than an inheritance.

The Shared-Responsibility Model and the Customer Responsibility Matrix

Even when a hosted offering meets the cloud rule, the contractor is not relieved of its own obligations. A hosted environment operates on a shared-responsibility model, in

which the vendor implements and operates some controls and the contractor remains responsible for others. The division is written down in a customer responsibility matrix, which maps each requirement to the party that carries it. The controls the vendor carries can be inherited and cited in the contractor's own System Security Plan. The controls assigned to the customer must be implemented and evidenced by the contractor. A hosted ERP does not make the contractor compliant. It carries part of the load and assigns the rest back, and the matrix is the document that records which is which.

The controls that typically remain with the contractor include the management of its own user accounts and access within the application, multifactor authentication for its users where the matrix assigns that to the customer, the handling of CUI once it leaves the hosted environment in reports and exports, the security of the endpoints its people use to reach the service, and the governance and documentation that no vendor can perform on the contractor's behalf. Reading the customer responsibility matrix and implementing the retained portion is the work, and it is the work a contractor most often underestimates when it assumes a hosted product arrives compliant out of the box.

There is also a scope consequence that follows from placing CUI in a hosted environment. Doing so expands the contractor's CUI boundary into that environment, which means the vendor's infrastructure and the people who operate it become part of the assessment consideration, and the contractor relies on the vendor's incident response and on the DFARS 252.204-7012 obligations flowing through the contract. Where the vendor cannot demonstrate that its offering meets the cloud rule, and cannot support the incident reporting and forensic obligations, that inheritance does not hold, and the contractor is left carrying a gap it may not have priced or planned for. The inheritance is only as good as the offering's demonstrated standing and the contract behind it.

One point governs how the entire matrix should be read. The matrix divides the implementation of controls between the vendor and the contractor, but it does not divide accountability for the CUI, and that accountability does not transfer. Under

DFARS 252.204-7012 and the CMMC framework, the contractor remains the party obligated to safeguard the Controlled Unclassified Information and to report a cyber incident within seventy-two hours, regardless of which party operated the control that failed. A breach or a leak that originates in the vendor's cloud, or in a managed service provider operating that environment on the contractor's behalf, is the contractor's reportable incident and the contractor's exposure, even where the matrix placed the failed control on the vendor. The vendor may be contractually liable to the contractor for its own failure, but the government's counterparty is the contractor, not the vendor. The same principle reaches the annual affirmation a contractor makes in the Supplier Performance Risk System. Where that affirmation rests on controls inherited from a vendor whose offering does not in fact meet the standard, the misrepresentation belongs to the contractor, and the False Claims Act exposure attaches to the contractor rather than to the vendor.

The Diligence

A contractor placing CUI in a hosted JobBOSS2 environment should establish a short set of facts in writing rather than by assumption. It should confirm which deployment and which hosting tier it is subscribed to, since the commercial tier and the government tier are different environments. It should obtain the customer responsibility matrix and read what the matrix assigns to the contractor. It should request the evidence that the offering meets the cloud rule, which is either a FedRAMP Marketplace authorization at Moderate or higher, or the third-party assessor's letter of attestation and the body of evidence behind an equivalency claim, and it should verify that evidence rather than accept descriptive language, because the C3PAO will do the same. It should confirm that the contract requires the vendor to meet the equivalency standard and to support the cyber incident reporting, forensic analysis, and media preservation obligations of DFARS 252.204-7012. Where ITAR technical data is involved, it should confirm United States Persons handling and United States data sovereignty, which the government cloud offering is built to address but which should be confirmed for the specific data in question. And where the offering does not yet meet the cloud rule, the contractor should treat a commercial tier as unsuitable for CUI unless the specific offering used for that

tier is FedRAMP Moderate authorized or can produce a valid FedRAMP Moderate equivalency package, planning the data's placement accordingly.

Two further steps follow from the fact that accountability for the CUI stays with the contractor. The first is a residual risk analysis. After the customer responsibility matrix is applied, the contractor should establish where the remaining risk actually sits and confirm that its own cyber liability coverage responds to a loss of CUI that occurs within the vendor's environment rather than only to an incident on the contractor's own network. Many policies are written around the insured's own systems, and a loss inside a hosted ERP can fall into a gap. The vendor's insurance protects the vendor, and its reach to the contractor depends on the indemnification terms in the contract, so the vendor's coverage and those terms should be reviewed as part of the diligence rather than assumed to extend to the contractor. The second step is an incident response assessment tested against the hosted scenario before an incident occurs. The plan should establish who detects an event, who notifies whom, how the contractor obtains from the vendor the forensic data and the preserved media it needs to meet the reporting and preservation obligations in paragraphs (c) through (g) of DFARS 252.204-7012, and whether the vendor is contractually bound to cooperate and to produce that evidence on the timeline the obligations require. An incident response plan that assumes the affected data and the relevant logs sit on the contractor's own network will fail at the moment it is needed, because in a hosted arrangement they sit in the vendor's environment.

The On-Premises Alternative

A contractor can also run JobBOSS2 on its own server rather than in the vendor's cloud. That choice returns the contractor to the model addressed in the companion paper, in which the contractor owns every applicable control across the host, the database, the network, the endpoints, and the exports, on a modern and supported SQL Server stack. The hosted decision and the on-premises decision are genuine alternatives, and the right one depends on the contractor's resources, its willingness to operate the controls itself, and whether a vendor-hosted offering that meets the cloud rule is available to it.

Neither choice is automatically correct. The on-premises path places the whole control burden on the contractor but keeps the data and the boundary within the contractor's direct control. The hosted path can move part of the burden to a vendor, but only when the offering meets the cloud rule and only for the portion the customer responsibility matrix assigns to the vendor. Both can be made defensible, and both can be made indefensible by the same error, which is assuming the work is done when it is not.

A Diagnostic Sequence

The hosted decision can be approached as a sequence. Working through the following questions in order tells a contractor where it stands and what it still has to establish.

Working through a hosted deployment

Question	What it determines
Does the JobBOSS2 environment contain CUI?	If it does not, the cloud rule does not attach. If it does, the rest applies.
Is the product on premises or hosted by the vendor?	On premises follows the companion paper. Hosted follows this analysis.
If hosted, is it the commercial tier or the government tier?	The commercial tier should not be treated as a home for CUI unless the specific offering meets the cloud rule. The government tier may be designed for that use case, but the specific offering must still be verified.
Is the offering FedRAMP Moderate authorized, or equivalent with a 3PAO attestation?	This is the threshold the offering must clear to hold CUI. Authorization of the platform underneath does not satisfy it.
Has the contractor obtained and read the customer responsibility matrix?	It defines what the contractor inherits from the vendor and what it retains.
Are the retained controls implemented and evidenced?	Inheritance covers only the vendor's portion; the rest is the contractor's to prove.

Does the contract carry the DFARS 252.204-7012 obligations to the vendor?	Incident reporting, forensic analysis, and media preservation must flow through to the provider.
If ITAR data is involved, is US Persons handling and US data sovereignty confirmed?	Export-controlled data carries restrictions beyond those for CUI generally.
Do the incident response plan and the cyber liability coverage account for a breach in the vendor's environment?	Accountability for the CUI and the reporting obligation stay with the contractor regardless of which party operated the failed control.

The System Security Plan and the Evidence Behind It

The hosting choice and its consequences are themselves System Security Plan content. The plan describes the deployment, identifies the hosted environment as part of the boundary, records the basis on which the offering meets the cloud rule, whether a FedRAMP Marketplace authorization or an equivalency attestation with its body of evidence, documents the controls inherited from the vendor and the controls retained by the contractor according to the customer responsibility matrix, and carries the evidence that the retained controls operate. A hosted arrangement does not shrink the System Security Plan. It changes what the plan must document and adds the vendor relationship and the inheritance to the things the contractor must be able to prove.

The determination, as with the legacy systems, comes from that body of implementation and evidence rather than from the brand of the product or the word cloud. A hosted JobBOSS2 environment can be a sound home for CUI when the offering meets the cloud rule, the customer responsibility matrix is read and acted upon, and the contractor evidences the portion it retains. It is not a sound home for CUI when the contractor assumes the vendor has handled everything, when the offering sits on a FedRAMP-authorized platform without itself meeting the equivalency standard, or when the data has been placed in a commercial tier for convenience. The difference between the two situations is visible in the evidence, and the assessment looks for it.

The Evidence Package

Because the determination rests on evidence, it helps to know in advance what that evidence consists of for a hosted deployment. The following items are the records a contractor assembles to demonstrate that a hosted JobBOSS2 environment is a defensible home for CUI, and they are, in practice, what a prime contractor or an assessor asks to see.

Evidence for a hosted deployment

Evidence	What it supports
System Security Plan identifying the hosted environment within the boundary	Scope and security planning
Hosting tier and subscription record	Which cloud rule path applies
FedRAMP Marketplace authorization, or the 3PAO letter of attestation and body of evidence	The offering's authority to hold CUI under DFARS 252.204-7012
Customer responsibility matrix	The division of controls between vendor and contractor
Documentation of inherited controls	The controls cited from the vendor in the SSP
Implementation and evidence for retained controls	The controls the contractor owns under the matrix
Identity and multifactor authentication records for the contractor's users	Access control and authentication, the 3.1 and 3.5 families
Export and endpoint handling for the contractor's environment	CUI leaving the hosted environment and the devices reaching it
Contract terms carrying DFARS 252.204-7012 to the vendor	Incident reporting, forensic analysis, and media preservation
Residual risk analysis after the responsibility matrix	Where remaining CUI risk sits once inheritance is applied

Cyber liability coverage review, including the vendor's coverage and indemnification terms	Whether a loss of CUI in the hosted environment is insured
Incident response plan tested against the hosted scenario	Detection, notification, and access to vendor forensic data under DFARS 252.204-7012 (c) through (g)
ITAR United States Persons and data sovereignty confirmation, where applicable	Export control beyond CUI generally

The Pattern Beyond One Product

JobBOSS2 is a worked example of a question every defense manufacturer now faces with hosted software. The same shared-responsibility analysis applies to any external cloud service that holds CUI, whether it is an ERP, a manufacturing execution system, a quality management system, a document or collaboration platform, or a governance, risk, and compliance tool. In every case the questions are the same. Does the offering meet the FedRAMP Moderate authorization or equivalency standard, demonstrated by a Marketplace listing or a third-party attestation and body of evidence. What does the customer responsibility matrix assign to the contractor. And can the contractor implement and evidence the portion it retains. A contractor that learns to ask those questions of one hosted product can ask them of all of them, which is why a paper about one ERP is, in practice, a guide to the hosted-software decision across the whole environment.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced, and the founder of David Koran and Associates. He helps aerospace and defense manufacturers implement CMMC on legacy ERP systems and bring difficult manufacturing environments into compliance. He is the author of The CMMC Decision and can be reached at dkoran@davidkoran.com and (802) 335-2662.

References

Cybersecurity Maturity Model Certification (CMMC) Program, 32 CFR Part 170, Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

Cybersecurity Maturity Model Certification (CMMC) Program, Final Rule, Federal Register, October 15, 2024. https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Acquisition.gov. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, Acquisition.gov. https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-with-the-cybersecurity-maturity-model-certification-level-requirements

Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings, Department of Defense Chief Information Officer, December 21, 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/FedRAMP-EquivalencyCloudServiceProviders.pdf

FedRAMP Marketplace, U.S. General Services Administration. https://marketplace.fedramp.gov/

ITAR-CMMC-Compliant Cloud Solutions for Manufacturers, ECI Software Solutions. https://www.ecisolutions.com/industries/manufacturing/itar-cmmc-compliant-solutions/

ECI Launches JobBOSS2, a New Cloud-Native ERP for Small and Medium Manufacturers, ECI Software Solutions. https://www.ecisolutions.com/news/eci-launches-jobboss2-a-new-cloud-native-erp-for-small-and-medium-manufacturers/

ECI Software Solutions JobBOSS2 and M1 Are Ready for Cybersecurity Maturity Model Certification (CMMC 2.0) Standards, Business Wire, October 17, 2023. https://www.businesswire.com/news/home/20231017502845/en