



OPEN
Compute Project



GEICO'S OCP ADOPTION

A BLUEPRINT FOR ENTERPRISE INFRASTRUCTURE TRANSFORMATION

Authors:

[Jason Holpuch, GEICO](#)
[John Hilt IV, P.E., GEICO](#)
[Ryan Chow, GEICO](#)
[Sahid Jaffa, GEICO](#)

Contributors

[Rebecca Weekly, GEICO](#)
[Steve Helvie, Open Compute Project](#)

Executive Summary

This Open Compute Project (OCP) white paper addresses the adoption of OCP infrastructure at enterprise scale through the experience of GEICO. It is intended for the everyday enterprise, from small to large, whose core business is not information technology but who depends on it as a critical enabler. Unlike hyperscalers, Original Equipment Manufacturers (OEMs), Original Design Manufacturers (ODMs), or cloud service providers, these enterprises operate in industries such as financial services, healthcare, retail, and manufacturing. GEICO's journey demonstrates that the adoption of OCP designs is both possible and beneficial for organizations seeking hyperscale-grade efficiency, flexibility, and cost advantages without being hyperscalers or engaging in hardware or infrastructure manufacturing.

GEICO initiated its OCP program in 2023 to gain greater control over infrastructure, reduce costs, and accelerate innovation. The company also aligned the program with OCP's five tenets of Openness, Efficiency, Impact, Scale, and Sustainability. Since then, GEICO has deployed two new colocation facilities with more than 1,000 OCP servers based on Open Rack version 3 (ORv3) rack architecture, integrating Data center Secure Control Module (DC-SCM), Open Compute Project network interface card (OCP-NIC) 3.0, and Modular Hardware System (MHS) designs. These deployments establish the foundation for GEICO's long-term objective to repatriate at least 50 percent of cloud workloads by 2029.

The adoption of infrastructure based on OCP designs has provided flexibility and control beyond what was possible with public cloud or Original Equipment Manufacturer (OEM) systems. GEICO can now design configurations to match enterprise needs, consolidate compute and storage on a common hardware platform, and operate a private cloud capable of hosting diverse workloads. This flexibility is matched by measurable cost benefits: GEICO has reduced unit costs by more than 50% per compute core and more than 60% per gigabyte of storage compared to both OEM hardware and public cloud¹.

The challenges were significant. GEICO pursued an aggressive timeline moving from inception to production in less than 24 months, driven by expiring OEM contracts, rising cloud costs and innovation-driven workload demands. Global supply chain pressures from the artificial intelligence (AI) boom affected component lead times and forced repeated bill of materials (BOM) adjustments. Fleet and firmware management emerged as critical gaps requiring new processes and expertise. Compatibility issues also surfaced, as many traditional devices such as top-of-rack and management switches were not designed for ORv3 racks and required IEC 60320 C13/C14 outlets, with C19/C20 where higher power is needed. To resolve this, GEICO collaborated with partners to develop the GEICO Power System (GPS)ⁱ, a hybrid ORv3 power system, now listed by Underwriters Laboratories (UL), that provides IEC 60320 C13/C14 and C19/C20 outlets so traditional AC-powered networking gear can coexist with OCP-native systems."

The key lesson for other enterprises is that OCP hardware design adoption is not purely a procurement exercise. It is both an architectural shift and a cultural transformation. Success requires executive sponsorship, careful partner selection, and specialized skills. Enterprises should plan for at least a 24-month cycle from program inception through evaluation, Engineering Validation Testing (EVT), Design Validation Testing (DVT), Production Validation Testing (PVT), and production.

This white paper presents GEICO's blueprint for the adoption of OCP-based designs. It captures motivations, design choices, and lessons learned from deploying OCP-recognized hardware in an enterprise setting. Most

¹ Realizations and scenarios are unique and specific to GEICO. Others may be very different.

This not a representation of any industry benchmark or standard.



importantly, it provides guidance for other enterprises that want to leverage OCP standards to lower costs, gain transparency, and take ownership of their technology future.

Call to Action

Everyday enterprises seek the flexibility, control, and cost advantages of OCP designs. They typically lack hyperscale procurement volume and large firmware engineering teams. The OCP community, ODMs, integrators, and component and software vendors should address the following priorities:

1. Supply and SKUs

Establish low to moderate volume programs with predictable pricing and lead times for orders of 50 to 500 units. Publish 12-to-18-month bill of materials (BOM), stability windows and clear end of life (EOL) and end of support (EOS) roadmaps. Provide evaluation bundles and pre-cabled first-rack pilot kits.

2. ORv3 racks, power, and networking

Standardize hybrid ORv3 power options that provide IEC 60320 C13/C14, with C19/C20 where required, so traditional AC-powered ToR and management switches can operate in ORv3 racks during transition. Offer certified integration kits with UL listings and reference wiring guides. Expand ORv3-compatible network options and certified adapters to support mixed deployments and incremental transitions. Publish rack integration and colocation delivery playbooks. Note that ORv3 is most practical for greenfield builds, since most colocation providers do not support it off the shelf. In existing colocation facilities with EIA-310 19-inch racks, enterprises may find it simpler to retain 19-inch for general-purpose compute and adopt ORv3 selectively for high-power accelerated designs, where OEM/ODM suppliers provide a wide range of options.

3. Firmware and lifecycle

Deliver enterprise-ready distributions of OpenBMC with long-term support branches, signed images, a software bill of materials (SBOM), and security update SLAs. Provide Distributed Management Task Force (DMTF) Redfish conformance profiles and reference pipelines for BIOS and BMC updates with automated rollout and rollback. Provide pre-validated baselines per platform, with documented interoperability across NIC, storage, and power firmware.

4. New Product Introduction (NPI) and Qualification

Provide packaged NPI kits with EVT, DVT, and PVT plans, acceptance criteria, golden images, and telemetry collectors matched to platform maturity. Include thermal and reliability guidance for dense rack configurations, including networking components.

5. Inventory, fleet operations, and security

Offer accelerators for establishing a system of record, including import templates and auto-discovery plugins. Publish reference jobs for secure firmware operations, image signing, staged rollouts, UEFI Secure Boot, and end-to-end chain-of-trust patterns suitable for regulated industries.

6. Support model and ecosystem alignment

Bridge the gap between OEM and ODM offerings with a single-escalation, multi-vendor SLA that spans server hardware, components, firmware, and management software. Back SLAs with NDAs and collaboration agreements that define artifact access, validation scope, and joint triage. The OCP community should standardize cross-vendor validation and badge enterprise-ready, pre-integrated and validated solutions from OEM/ODM suppliers, which deliver more value to enterprises than another MHS revision.

These actions will lower barriers to entry and make hyperscale-grade efficiency, flexibility, and cost outcomes attainable for the everyday enterprise.

Table of Contents

Executive Summary	1
Call to Action	2
Introduction.....	6
Compliance with Open Compute Project Tenets	7
Openness	7
Efficiency	7
Impact.....	7
Scale.....	8
Sustainability	8
Strategic Imperative: Why GEICO Transitioned to OCP	8
Lessons from Public Cloud at Scale	8
Limitations of Traditional OEM Paths.....	8
Financial Rationale and Time to Value	9
Selection, Evaluation, and Design Fit for Enterprise	9
Enterprise server hardware configurations and best practices	10
Enterprise server (L6), component, and chassis (L10) best practices	10
Enterprise server rack configuration and data center best practices	11
Enterprise Server Hardware New Product Integration (NPI)	11
NPI Objectives.....	11
NPI Phases	11
Implementation guidance	12
From OEM to Open: Building an ODM-based Supply Chain.....	12
OEM to ODM: Support, staffing, and integration implications	12
OEM to ODM: Supply chain, logistics, and operational readiness	13
Lead times and BOM stability.....	13
Component lifecycle	14
Spares and RMA	14
Forecasting and capacity planning	14
Contracts and trade compliance	14
Logistics and delivery.....	15
Integration in mixed environments.....	15

Support and staffing	16
Fleet Management Challenges and Mitigations.....	16
Hardware Integration and Firmware Lifecycle	17
OpenStack Bare Metal Integration	17
NetBox as the System of Record for Inventory	18
Firmware Update Management	18
Recommendations for enterprise adoption:.....	18
Hardware Platform Security and Root of Trust	19
Conclusion	19
Glossary	21
References	24
License	26
Appendix A	27



Introduction

Enterprises are reassessing infrastructure strategies to balance cost, flexibility, and speed of innovation. Public cloud adoption has delivered rapid scale, yet many organizations now face rising run-rate costs, uneven transparency, and limited control over design choices. Traditional Original Equipment Manufacturer (OEM) platforms address some needs, but fixed configurations, long lead times, and limited openness often constrain enterprise objectives. This white paper documents how GEICO adopted Open Compute Project (OCP) designs to build a private cloud foundation that is cost efficient, flexible, and under enterprise control.

GEICO began this program in 2023 after a decade of significant expansion in public cloud consumption. By 2021, GEICO operated across multiple cloud service providers, and by 2023 total public cloud spend exceeded 300 million dollars annually, with a substantial concentration on a single provider. Prior OEM approaches required stitching together multiple partner solutions to reach desired outcomes. These factors prompted a strategic shift toward open hardware, open interfaces, and standardization through OCP.

GEICO selected Open Rack version 3 (ORv3) as the rack standard and incorporated the Data center Secure Control Module (DC-SCM) and Open Compute Project network interface Card 3.0 (OCP-NIC). The OCP modular hardware system (MHS) approach allows compute and storage servers to share a common base platform. Technical choices emphasized high core count processors, lower platform power, and Peripheral Component Interconnect Express (PCIe) 5.0 support. The management plane integrates the Distributed Management Task Force Redfish interface with baseboard management software stack BMC to enable automation and consistent lifecycle operations.

Initial deployments established two new colocation facilities with more than 1,000 OCP servers. These installations form the foundation for GEICO's objective to repatriate at least fifty percent of cloud workloads by 2028. Early results confirm material unit cost improvements. GEICO realized more than 50% reduction in cost per compute coreⁱⁱ and more than 60% reduction in cost per gigabyte of storageⁱⁱⁱ when compared to prior OEM systems and equivalent services from cloud providers. OCP designs have also provided the flexibility to deploy a diverse set of workloads on a consistent hardware foundation that supports private cloud operations.

The journey surfaced practical constraints that are common in enterprise settings. Time-to-production was targeted at less than twenty-four months due to expiring contracts and operational timelines. Component supply was affected by increased demand for artificial intelligence hardware, which influenced lead times and required adjustments to the bill of materials. Fleet and firmware lifecycle management required new processes, tooling, and skills. Compatibility gaps existed between ORv3 power architectures and traditional AC-powered devices such as top-of-rack and management switches that use IEC 60320 C13/C14 connectors, with C19/C20 where higher power is required. GEICO collaborated with partners to design and contribute a hybrid ORv3 power solution, listed by Underwriters Laboratories (UL), that enables mixed deployments within the same rack.

This white paper is written for the everyday enterprise, from small to large, whose primary business is not infrastructure manufacturing. It provides a blueprint that connects strategy to execution with enterprise-focused recommendations. The blueprint addresses chassis design and selection, including when to use pre-existing platforms versus custom designs. It covers firmware and fleet management issues, mitigations, and practical recommendations. It outlines logistics and shipping considerations. It highlights tax and tariff implications that



affect total cost and procurement planning. It explains manufacturing and compliance requirements that influence schedules and risk. It presents methods for mitigating compatibility issues and enabling EIA-310 19-inch equipment to operate within ORv3 racks, including hybrid ORv3 power with IEC 60320 C13/C14 outlets and C19/C20 where required, along with approved mounting and cable-management practices. It provides a structured comparison of OEM and Original Design Manufacturer (ODM) approaches to guide sourcing and support decisions.

The remainder of the document develops these topics in depth and provides actionable guidance for implementation.

Compliance with Open Compute Project Tenets

A full explanation of the OCP core tenets can be seen [here](#)

Openness

GEICO adopts open specifications and interfaces to ensure interoperability and firmware transparency. The designed stack uses DMTF Redfish across platforms based on ORv3, DC-SCM, and OCP NIC 3.0. GEICO has openly shared its adoption lessons and contributed a UL-listed hybrid ORv3 power solution that enables EIA-310 19-inch equipment to operate within ORv3 racks through IEC 60320 C13/C14 outlets, with C19/C20 where higher power is required. The program is executed with multiple solution providers to assemble an enterprise-scale OCP environment.

Efficiency

GEICO's OCP adoption of OCP technologies delivers material cost and energy gains. Early results show more than 50% lower cost per compute core and more than 60% lower cost per gigabyte of storage compared to OEM systems and public cloud. ORv3 improves power delivery efficiency through rack-level DC distribution and increases usable rack density, which reduces space and cooling requirements. A MHS with PCIe 5.0 support extends platform life, reduces spares, and improves total cost of ownership.

Impact

GEICO demonstrates that OCP designs are viable at enterprise scale. Production deployments in two colocation facilities with more than 1,000 servers are operating today, with a growth target of 3,000 servers over the next few years. GEICO works with ODMs to stabilize SKUs, define predictable BOM windows, and align qualification practices to enterprise timelines. The hybrid ORv3 power solution, UL-listed, enables EIA-310 19-inch equipment to operate in ORv3 racks via IEC 60320 C13/C14 and C19/C20 outlets during transition. GEICO shares lessons and pain points with the community so peers can adopt more quickly, and suppliers can take corrective actions that reduce barriers to entry.



Scale

GEICO's OCP design is modular and repeatable so it can start small and expand predictably. ORv3, MHS, DC-SCM, and OCP NIC 3.0 provide a uniform base that supports compute and storage on common components. A single pilot rack can be deployed first, then scaled rack by rack using consistent SKUs and BOM windows. Remote management uses Redfish, with staged update processes for controlled rollouts and rollbacks. Growth follows an NPI path with EVT, DVT, and PVT so new configurations are added with minimal disruption.

Sustainability

GEICO's OCP adoption emphasizes transparency, circularity, and measurable improvement. ORv3 increases energy efficiency through rack-level DC power and higher usable density, reducing space and cooling requirements. The hybrid ORv3 power approach enables reuse of EIA-310 19-inch equipment through IEC 60320 C13/C14 and C19/C20 outlets, limiting waste during migration. Standardized components, planned BOM stability, and PCIe 5.0 support extend platform life and promote repair and reuse.

Strategic Imperative: Why GEICO Transitioned to OCP

GEICO's transition to Open Compute Project (OCP) designs was a strategic response to increasing infrastructure demand, rising run-rate costs, and the need for greater control over design and operations. The objective is to support artificial intelligence and machine learning (AI/ML), analytics and core insurance modernization on a platform with predictable economics, transparent lifecycle management, and flexibility to adapt.

Lessons from Public Cloud at Scale

For more than a decade, GEICO has operated enterprise-scale workloads in public clouds. This experience delivered agility, rapid scale, infrastructure diversity, and faster delivery of products and services. At sustained scale, side effects became material for certain workload classes. Legacy and proprietary systems that require significant re-architecture, redesign, or replatforming were costly to operate in a pure consumption model. Hardware and service catalogs are limited to what a provider offers, which constrains choices of chipsets, graphics processing units, storage media, and network features, and some capabilities carry premium pricing. In practice, public clouds are not infinitely scalable; GEICO has encountered capacity constraints, service deprecations, and regional or quota limits that required significant unplanned work to meet business demand. Not all workloads are a best fit for public clouds. OCP hardware designs, paired with an Original Design Manufacturer (ODM) sourcing model, provide a foundation for an enterprise private cloud that can rehost selected public cloud workloads while preserving the ability to use cloud services where they fit best.

Limitations of Traditional OEM Paths

Traditional OEM platforms are effective for narrow, well-understood workloads, but their proprietary control planes and lifecycle managers favor single-vendor unification and restrict heterogeneous operations. When infrastructure spans multiple OEMs, operations fragment across separate tools and release cadences, producing duplicated processes, inconsistent interfaces, parallel automation pipelines, and divergent inventory and telemetry models. Complexity and cost rise due to overlapping licenses and subscriptions, multiple support programs and contracts, product-specific training, and security teams tracking distinct firmware advisories and



remediation steps. OEMs do provide mature documentation, integrated tooling, and consistent field reliability that are of value to enterprises. However, these benefits often force a regression to the lowest common denominator across a mixed fleet, and the associated price premiums are not always justified for certain workload mix and scale.

Qualification slows because hardware options, dependency chains, and release timing differ by vendor, which drives a bias toward the smallest common denominator rather than the optimal configuration per workload. These constraints informed GEICO's move to OCP designs and open interfaces that support a uniform operational model across vendors, reinforced by stable SKUs, defined BOM windows, and an enterprise-aligned NPI process.

Financial Rationale and Time to Value

GEICO's decision was grounded in comparative quotations and total cost of ownership (TCO) analysis, not only post-deployment outcomes. Side-by-side quotes from OEM offerings, public cloud services, and OCP platforms sourced through ODMs were normalized to unit economics and modeled over a multiyear horizon. The analysis included server acquisition, rack power and cooling, colocation space, lifecycle operations, support, software licensing impacts, and depreciation. Sensitivity tests were applied for utilization, energy price, and component refresh.

The modeled results showed that OCP with an ODM supply model delivered materially lower unit cost. Projected cost per compute core and cost per gigabyte of storage were more favorable than both OEM quotes and public cloud pricing for steady, enterprise workloads. Contributing factors included ORv3 rack-level DC power efficiency, higher usable rack density that reduced space and cooling charges, simplified sparing from an MHS base, and avoidance of bundled features not required for GEICO's workload profiles. Lead-time and availability data from suppliers were incorporated to assess time to first capacity. Standard building blocks and a defined NPI path with EVT, DVT, and PVT reduced qualification effort, which improved time to value relative to traditional procurement cycles.

Selection, Evaluation, and Design Fit for Enterprise

GEICO assessed Open Compute Project (OCP) building blocks and platform options using enterprise requirements for compute, storage, and bill of materials (BOM) capabilities that needed to mirror prior OEM designs and public cloud offerings. In an ODM context, matching these baselines was straightforward: select processor families and socket counts, choose chassis form factors, size memory and storage, and specify network interface options. Stitching these components together to meet capacity targets was the easy part.

When evaluating new platform designs, enterprises should prioritize solutions that are OCP Accepted™ or OCP Inspired™. These designations signal adherence to open standards, validated interoperability, and alignment with community-driven specifications critical factors for de-risking procurement and lifecycle management in modern supply chains.

Beyond capacity and feature matching, enterprises should factor in supplier availability and support coverage, integration complexity with existing tooling, the scope of New Product Introduction (NPI) testing, thermal, power, and serviceability constraints, site readiness for power and networking, and lifecycle commitments such as long-term support, signed images, and BOM stability.



Below are some of the OCP components and fleet management solutions GEICO evaluated ranked by ease of enterprise adoption.

- **OCP-NIC 3.0.** Widely available from OEM/ODM vendors and major NIC manufacturers. Standardizes the network interface, reduces driver and tooling variance, and integrates cleanly when validated against target operating systems and orchestration platforms.
- **Modular Hardware System (MHS).** Establishes a common L6 base for multiple roles so compute and storage share the same motherboard, backplanes, and service parts. This reduces variant count, simplifies spares, and concentrates qualification scope. Confirm PCIe 5.0 lanes, backplane options, and chassis service clearances for the intended workloads.
- **Datacenter Secure Control Module (DC-SCM).** Separates the control plane from the host to improve serviceability and lifecycle control. Verify module availability across the program horizon and align vendor roadmaps and security features with enterprise policy. Form factor versions are not interchangeable. GEICO encountered a limitation where Secure Boot requirements necessitated DC-SCM 2.0 after an initial 1.0 selection. Validate security and firmware requirements against the DC-SCM version early and account for redesign or re-qualification if a version change is required.
- **2OU three-node compute form factor.** Available through ODMs and effective for maximizing compute density per rack. Validate thermal headroom, airflow direction, rail and tool compatibility, and field service procedures under worst-case drive and NIC populations.
- **Open Rack version 3 (ORv3) with distributed power shelves.** Available via ODMs and distribution. Plan rack-level redundancy strategy and any battery backup unit decisions. Most network gear is not ORv3 native; mixed racks often require a hybrid ORv3 power approach that provides IEC 60320 C13/C14 outlets, with C19/C20 where required, using listed integration kits and approved mounting to host EIA-310 19-inch devices during transition.
- **Management firmware and lifecycle.** Require DMTF Redfish conformance, signed images, SBOM, and long-term support commitments per platform. Enterprise adoption frequently depends on access to artifacts under NDA, pre-validated baselines, and reference update pipelines that support staged rollout and rollback across BIOS, BMC, NIC, storage, and power firmware.

Enterprise server hardware configurations and best practices

Within hyperscale environments it is common to support many SKUs per workload class. Most enterprises benefit from the opposite approach. Constrain platform variants and design for repeatability across motherboard (L6), server chassis (L10), and rack configuration (L11). Define a small set of target workload profiles such as general compute, storage, database, and accelerated. Map each profile to a limited number of qualified configurations with a documented bill of materials and uniform acceptance criteria. This reduces qualification time, simplifies spares and operations, and keeps lifecycle management predictable

Enterprise server (L6), component, and chassis (L10) best practices

Align on a single CPU family and one L6 that can serve multiple roles. Standardize components across SKUs, including DRAM speed and size, boot devices, data drive type and capacity, and NIC options. Where feasible, reuse a single L10 chassis for both compute and storage, or introduce a carefully sized HCI SKU to cover mixed roles.



Validate thermal margin and serviceability at worst-case drive and NIC populations. Confirm airflow direction, rail compatibility, and tool access, and publish field-replaceable unit kits for common repairs. Maintain a short list of golden configurations with pinned firmware and documented acceptance tests so new deliveries are commissioned the same way every time. This alignment reduces spare part diversity, shortens mean time to repair, and lowers operational risk across the hardware lifecycle.

Where Modular Hardware System (MHS) is available, design the platform so a single L6 can be retained while CPUs and carrier cards are swapped in a later step. This provides a path to future processors without gating the initial launch. Validate mechanical fit, power delivery, and thermal headroom for the anticipated next generation during the first qualification so the later upgrade is a controlled change rather than a redesign.

Enterprise server rack configuration and data center best practices

Moving to the rack configuration (L11), enterprises are often constrained by available power, air cooling capacity, network topology, and the size of failure domains within a smaller data center footprint. Document per-rack power and cooling capabilities for each site to set maximum L11 configurations by hardware class. Allow L11 requirements to inform the data center network architecture, including top-of-rack versus end-of-row placement and acceptable oversubscription. Define the failure domain for each class so incidents and maintenance remain within the intended blast radius. These constraints may lead to lower rack density or a controlled mix of hardware classes within the same rack to align actual load with facility limits. This is a compromise on total cost of ownership that fits the needs of smaller enterprise deployments.

Use the OCP Ready Data Center criteria as a reference for facility readiness and operations. Align site standards and commissioning checklists to those criteria so power distribution, cooling envelopes, safety, service clearances, and monitoring are evaluated consistently across locations. Incorporate these checks into rack acceptance to ensure that L11 designs meet both performance objectives and cost targets before scale-out.

Enterprise Server Hardware New Product Integration (NPI)

Onboarding an ODM server platform at GEICO required a formal NPI process. This process is common in hyperscale environments and is appropriate for enterprises that need predictable quality, clear acceptance gates, and traceable artifacts before production.

NPI Objectives

- Validate server component and system performance outside the production environment.
- Reproduce, debug, and resolve hardware and firmware issues prior to deployment.
- Establish phase gates that control progression and shipments between NPI stages.

NPI Phases

- **Engineering Validation Testing (EVT)** Server and node level testing.
- **Design Validation Testing (DVT):** Rack level testing that exercises integration, networking, power, cooling, and operational workflows.
- **Production Validation Testing (PVT):** Production workload and end-to-end integration testing in conditions that mirror the target environment.



Table 1: OEM/ODM HW maturity and NPI scope

OEM/ODM Hardware Platform Maturity	Enterprise NPI Scope
OEM Server Platform	PVT qualification
ODM Mass Production Server Platform	DVT and PVT qualification
ODM New Server Platform (new electrical, mechanical or firmware)	EVT, DVT, and PVT qualification

For GEICO's first ODM deployment, building and executing this framework was both a challenge and a learning opportunity. Best practice is to set explicit expectations on platform maturity at contract signature, since the OEM or ODM choice affects staffing, test coverage, BOM stability windows, and ordering lead times at each gate. The same choice influences the overall NPI schedule by determining the depth of validation required before production release.

Implementation guidance

- Define written entry and exit criteria for EVT, DVT, and PVT and tie them to shipment releases.
- Require phase deliverables: golden images with checksums, test plans and results, discrepancy logs with corrective actions, and verified rollback procedures.
- Assign defect ownership across ODM, integrator, and component vendors and maintain a single escalation path with documented SLAs.
- Control changes using BOM stability windows and recorded engineering change orders.
- Retain all NPI artifacts with the platform baseline for audit, spares planning, and future refresh cycles.

From OEM to Open: Building an ODM-based Supply Chain

OEM to ODM: Support, staffing, and integration implications

The enterprise experience differs between OEM and ODM sourcing. An OEM provides a single commercial channel for server and component support, repairs, and firmware updates. Offerings are pre-packaged with defined service tiers, tools, and documentation, and the OEM carries responsibility for integration and interoperability within its portfolio. This model aligns with typical enterprise staffing that focuses on L11 and L12 integration, provisioning, and operations.

An ODM model gives the enterprise control of BOM, qualification scope, and release cadence, but it expands the span of control. Most organizations will need to plan for additional roles that are not required in a classic OEM



relationship, including low-level hardware engineers familiar with hardware description language, firmware engineers for BIOS and BMC integration, burn-in and qualification engineers for EVT, DVT, and PVT, and test automation engineers who build repeatable pipelines for inventory, telemetry, and updates. Some capability can be sourced through an integrator or contracted from the ODM, but ownership of results remains with the enterprise.

Enterprises can obtain L11 rack integration and L12 site readiness through an ODM program, but this requires front-loaded planning, investment, and joint integration testing with the ODM and any integrator. The enterprise must still provide in-house expertise for power and thermal engineering, firmware and lifecycle management, commissioning procedures, and operational runbooks, or contract for these skills with clear acceptance criteria. ODM collaboration concentrates control in the enterprise and does not remove accountability for integration, validation, and ongoing support.

When adopting an ODM model, establish the following workstreams with clear ownership:

- Direct vendor support channels with component suppliers to expedite root cause and resolution.
- Roadmap reviews to inform future component selection and refresh timing.
- Firmware release note reviews to drive qualification plans and promotion rings.
- EOL and EOS visibility integrated with spares planning and replacement qualifications.

Align contracts and SLAs with operational reality. Execute NDAs and collaboration agreements with the ODM, integrator, and component vendors that define artifact access, acceptance criteria, escalation paths, and RMA responsibilities.

Important for New Adopters

OCP and ODMs are not synonymous terms. Integrating OCP designs does not require an ODM or custom builds. Several OEMs already incorporate OCP components such as OCP NIC 3.0 and DC-SCM. The sourcing decision should be driven by business requirements, stage of OCP adoption, current engineering capacity, available time for NPI, and the cost–benefit for target workloads. One can also take a hybrid approach: sourcing high volume designs in an ODM fashion and buying off-the-shelf for low volume solutions. This hybrid adds some complexity in fleet management given OEM proprietary solutions, but the tradeoffs may be worthwhile (or even negotiable).

OEM to ODM: Supply chain, logistics, and operational readiness

Moving from OEM consumption to an ODM program increases control over design, bill of materials, and cadence. It also shifts planning, qualification, and support responsibilities to the enterprise and its partners. Treat this as an operational pivot that requires firm governance, explicit contracts, and coordinated execution across suppliers, integrators, and internal teams.

Lead times and BOM stability

AI demand and external events can tighten supply for CPUs, memory, SSDs, NICs, and accelerators. Component substitutions require requalification and can invalidate firmware baselines and spares plans.

- Maintain a rolling 12-to-18-month forecast with safety stock for long-lead field-replaceable units.



- Freeze the BOM for each NPI phase and record engineering change orders with impact analysis before any change.
- Before large or iterative orders, confirm that the qualified BOM is available for the full order tranche to avoid creating mixed fleets.

Component lifecycle

NICs, GPUs, and SSDs may reach end of life or end of support in 2 to 3 years while servers are expected to remain useful for 5 or more.

- Verify lifecycle horizons during NPI and require written EOL and EOS notifications with last-time-buy options that cover the intended service life of the server.
- Prequalify compatible replacements and document the promotion process with test plans, acceptance criteria, and rollback procedures.

Spares and RMA

Mean-time-to-resolution depends on access to parts and clear rules of engagement.

- Establish on-site supply lockers or negotiate consigned spares sized to failure rates, RMA turnaround, and site transit times.
- Define RMA and DOA terms explicitly, including what constitutes DOA versus early-life failure, required evidence, advance-replacement rules, depot versus on-site service, and target resolution times.
- Specify inbound and outbound freight ownership, packaging and labeling requirements, and fees for unreturned parts.

Forecasting and capacity planning

Avoid late bottlenecks in power and mechanical accessories.

- Pre-allocate capacity for power shelves, rectifiers, rails, and cabling that commonly constrain deployments.
- Model demand surges from AI initiatives and disruptions from export controls, sanctions, or regional conflicts.

Contracts and trade compliance

ODM sourcing demands rigorous commercial clarity, legal preparedness, and ongoing governance. Enterprises assume direct responsibility for vendor oversight, contract enforcement, and regulatory alignment functions traditionally abstracted by OEMs.

- **Specify Incoterms and handoff points.** Define International Commercial Terms (Incoterms), title transfer, risk ownership, inspection periods, and delivery thresholds. Clearly indicate when liability shifts from the ODM or integrator to the enterprise and ensure this aligns with the selected Incoterms rule.
- **Define completed delivery per site.** Specify what constitutes delivery acceptance, whether at the loading dock, staged and powered hardware, or fully racked, cabled, and commissioned with documented acceptance testing.
- **Clarify shipping responsibilities.**



- Identify whether the ODM is responsible for shipping from the international factory to the enterprise's local assembly or final data center site.
- Clearly define who owns last-mile logistics and freight costs at each transition point.
- **Establish cancellation and breach terms.**
 - Include clauses for order cancellation, timelines, refund eligibility, or credit handling.
 - Since ODM builds are often custom and non-transferable, negotiate terms that cover enterprise protections in case of ODM breach or missed delivery milestones.
 - Use language similar to existing terms from reviewed contracts to ensure enforceability.
- **Centralize trade compliance artifacts.**
 - Confirm that the ODM and all suppliers are not listed on any sanctioned or restricted-party lists.
 - Require final assembly and testing to occur in geographies compliant with enterprise policies and applicable regulations.
 - Standardize documentation for Harmonized Tariff Schedule (HTS) codes and Export Control Classification Numbers (ECCN).
 - Record country of origin per line item and perform restricted-party screening.
 - Collect certificates of conformity and track UL listings, where applicable.

Logistics and delivery

- All integrated systems require engineered handling and acceptance, regardless of form factor or rack standard. Clearly defined responsibilities, transit expectations, and acceptance protocols are critical to avoiding delays, damage, or disputes.
- Define packaging specifications, including shock and tilt indicators, humidity and temperature tolerances, and burn-in requirements prior to shipment.
- Clarify shipping terms upfront. Determine whether the ODM is responsible for shipping directly to the enterprise data center or to a local assembly site.
- Explicitly state which party is responsible for international freight costs, import duties, taxes, and customs clearance.
- Clearly define the point of delivery: whether the system is considered delivered when it arrives at the loading dock, is racked and stacked, or after site acceptance tests are completed.
- Establish who holds liability during each leg of transit and when risk of loss formally transfers from the ODM to the enterprise.
- At the point of acceptance, scan and record serial numbers, compare them to the approved BOM, capture photo evidence, perform torque and continuity checks, and complete a signed commissioning record.
- Plan for extended transit timelines and ensure delivery site readiness, including space allocation, power, and mechanical clearance for unloading and staging.

Integration in mixed environments

Infrastructure transitions often require co-existence between Open Rack (ORv3) and traditional EIA-310 rack-mounted equipment. Many legacy or network devices are not ORv3-native, and heterogeneous environments must be planned with clear integration and support strategies.



- Publish L11 integration playbooks. Provide detailed procedures for site readiness, rack integration, power shelf wiring, grounding, airflow alignment, cable management, and commissioning. Include clear criteria for acceptance at each stage and document handoffs between facilities, engineering, and operations teams.
- Prepare for hybrid rack deployments.
- Where ORv3 is adopted, use hybrid ORv3 power configurations that support IEC 60320 C13/C14 and C19/C20 outlets.
- Follow validated mounting and airflow practices to ensure safe operation of traditional 19-inch EIA-310 equipment within ORv3 racks.
- Define power budgeting, airflow direction, and access clearance to accommodate mixed-role hardware.
- Support traditional EIA rack environments.
 - Maintain readiness to host traditional equipment in standard EIA-310 racks, especially for devices that are incompatible with ORv3 form factors or power delivery.
 - Ensure rack elevation planning and site power provisioning support both legacy and transitional footprints.
- Coordinate transition planning.
 - Assess which devices are ORv3-compatible and which require traditional rack environments.
 - Create a deployment matrix that maps equipment types to rack standards, ensuring no mismatch between delivery and site readiness.

Support and staffing

Support and staffing models change under ODM. Enterprises gain control of BOM and cadence, but ownership and involvement expand.

Plan for low-level hardware engineers with hardware description language (HDL) familiarity, firmware engineers for BIOS and BMC, burn-in and qualification engineers for EVT, DVT, and PVT, and test automation engineers for inventory, telemetry, and update pipelines.

If using an integrator or ODM services, set acceptance criteria, deliverable artifacts, and service level agreements (SLAs) in writing, and establish a single escalation path that spans the ODM, the integrator, and key component vendors.

Fleet Management Challenges and Mitigations

Transitioning from traditional OEM systems to ODM-based open hardware platforms requires a fundamental shift in how enterprises approach infrastructure lifecycle management. This shift brings greater control and flexibility but also introduces new operational responsibilities that must be addressed through deliberate engineering, process maturity, and integration readiness.

GEICO's adoption of OCP hardware and ODM-sourced platforms surfaced several operational gaps and challenges that required deep investment in tooling, processes, and internal expertise. These lessons offer valuable guidance for other enterprises planning similar transformations.



Hardware Integration and Firmware Lifecycle

ODM platforms often expose lower-level interfaces and less abstracted management layers compared to traditional OEM systems. GEICO had to modernize its internal tools to support Redfish-based management and build firmware lifecycle automation from the ground up.

Adopting ODM-sourced platforms required significant rework of internal fleet management systems and observability pipelines. Unlike traditional OEM solutions that abstract hardware complexity, ODM platforms demand deeper engineering integration and operational ownership.

Key recommendations informed by GEICO's experience include:

- **Prepare for vendor-specific Redfish implementations:** Enterprises should assess and adapt telemetry and fleet observability pipelines to support heterogeneous Redfish schemas. GEICO had to modify internal tooling to interpret and normalize Redfish data across multiple ODM platforms.
- **Design provisioning systems for firmware variability:** Unlike OEMs, ODM firmware maturity can vary. Enterprises should design provisioning workflows to tolerate differences in BMC features, IPMI behavior, and firmware stability. GEICO adjusted its automation pipelines to address these inconsistencies and ensure platform reliability.
- **Implement secure firmware lifecycle pipelines:** Enterprises must own the validation and version control of BIOS and BMC firmware. This includes defining rollback strategies, integrating firmware checks into CI/CD pipelines, and establishing an internal process for trusted firmware updates.
- **Establish structured qualification and validation frameworks:** Each ODM platform should be subjected to standalone and integrated qualification tests. These tests should validate management interfaces, platform behavior under load, and compatibility with enterprise service stacks. GEICO created such a framework to avoid production disruptions and to standardize ODM onboarding.

OpenStack Bare Metal Integration

OpenStack is widely used as a control plane for bare metal provisioning. However, its reliance on standards-based hardware management can pose integration challenges with ODM platforms, particularly when BMC firmware lacks full support for Redfish or exhibits inconsistent behavior. GEICO utilizes OpenStack as the core provisioning and lifecycle platform for bare metal infrastructure. Integrating ODM platforms into OpenStack revealed a range of technical gaps:

- **Test Redfish support against Ironio and other OpenStack services:** GEICO encountered gaps in Redfish schema support across ODM BMCs, which impacted node provisioning and management. Enterprises should evaluate Redfish endpoints in lab environments prior to production deployment.
- **Benchmark BMC reliability under operational workloads:** BMC stability can vary between ODM vendors. Enterprises should develop repeatable test harnesses to validate power control, telemetry access, and firmware updates under simulated production conditions.
- **Identify thermal and power anomalies during burn-in:** Networking devices, particularly NICs and switchgear, may exhibit unexpected thermal or power characteristics when integrated with new ODM platforms.



Enterprises should collaborate with ODMs to adjust firmware and hardware configurations early in the qualification process.

GEICO's expanded qualification matrix ensured that hardware behavior was validated not just in isolation, but in conjunction with OpenStack and its operational requirements. This approach is recommended for any enterprise adopting an open-source control plane with ODM hardware.

NetBox as the System of Record for Inventory

A centralized, vendor-agnostic inventory system is critical to managing modern infrastructure. Enterprises relying on OEM-specific tooling may find that they lack the visibility, automation, and auditability required for scaling ODM-based environments.

To centralize asset management and align with internal compliance requirements, GEICO transitioned to NetBox as its authoritative system of record to address these limitations.

Key practices include:

- Standardize inventory management across all vendors: Enterprises should select an open-source or extensible DCIM tool and treat it as the system of record for all infrastructure assets. GEICO selected NetBox and integrated it into core provisioning and compliance workflows.
- Automate brownfield imports and greenfield tracking: Migration of legacy asset data must be followed by workflows that enforce real-time tracking of greenfield devices. GEICO developed ingestion, mutation, and decommissioning processes to ensure data accuracy and integrity.
- Work with ODMs to define asset metadata standards: ODMs should provide structured asset files that include serial numbers, MAC addresses, firmware versions, and component-level details. Enterprises can use this metadata to validate inventory and streamline operational automation.

By elevating NetBox to the authoritative source of truth, GEICO improved visibility, reduced configuration drift, and enabled policy-driven enforcement across its infrastructure lifecycle. Other enterprises can replicate this model to improve asset governance and reduce reliance on vendor-specific systems.

Firmware Update Management

ODM platforms often lack integrated tooling for firmware updates, requiring enterprises to assume direct responsibility for update orchestration. GEICO historically relied on commercial off-the-shelf (COTS) server management platforms and manual web interfaces to manage firmware versions. This approach proved insufficient at scale, especially as GEICO began operating ODM hardware with inconsistent tooling and limited vendor-side automation.

Recommendations for enterprise adoption:

- Establish automated firmware update pipelines using Redfish APIs, out-of-band management tools, or vendor-provided SDKs where available.
- Integrate firmware management into CI/CD workflows, ensuring updates can be validated in pre-production environments before deployment.



- Track platform firmware baselines across staging, burn-in, and production environments to detect drift and enforce consistency.
- Define rollback and recovery procedures to support version reversion in the event of update failure or performance regressions.

Enterprises adopting ODM platforms must proactively design firmware update processes to ensure platform stability, reduce operational friction, and improve auditability.

Hardware Platform Security and Root of Trust

In traditional OEM environments, platform security responsibilities often reside with the vendor. When transitioning to ODM hardware, GEICO found it lacked internal baselines for secure boot, firmware validation, and root-of-trust enforcement. The organization had to develop these capabilities in-house, beginning with UEFI Secure Boot policies and advancing toward a formalized chain of trust across hardware and software components.

Key recommendations:

- Implement UEFI Secure Boot and ensure operating system images are cryptographically signed, with proper key management and attestation workflows.
- Define firmware signing and validation pipelines, including automated testing of BMC and BIOS integrity during provisioning and updates.
- Establish a root-of-trust model aligned with ODM platform capabilities, incorporating cryptographic identity, key signing, and secure provisioning into the hardware lifecycle.
- Collaborate with ODMs and component vendors to verify support for security features such as TPM integration, hardware-based attestation, and immutable boot loaders.

Conclusion

The adoption of OCP hardware presents enterprises with a compelling opportunity to achieve hyperscale-grade cost efficiency, platform flexibility, and infrastructure transparency, without needing to build systems in-house. GEICO's journey demonstrated that OCP designs, when backed by disciplined planning and execution, can deliver significant unit cost reductions of when compared to traditional OEM systems and public cloud compute and storage services. These savings are enabled by modular architecture, rack-level design efficiencies, and the ability to tailor hardware to specific workload requirements rather than relying on fixed OEM bundles.

OCP components such as OCP NIC 3.0, DC-SCM, MHS, and OpenBMC firmware provide enterprises with powerful tools to improve serviceability, firmware lifecycle management, and interface standardization. However, adopting open hardware is more than a technical decision. It is an operational and cultural transformation that demands maturity across procurement, planning, legal, and engineering disciplines. Enterprises must be prepared to navigate contract governance, supply chain coordination, inspection and acceptance processes, and compliance requirements. This includes specifying commercial terms such as Incoterms, defining points of title and risk transfer, enforcing RMA and DOA remedies, and ensuring supplier adherence critical enterprise requirement and certain governing regulations.



Staffing and internal readiness must also be addressed. Traditional OEM systems arrive fully integrated and vendor-supported, but ODM adoption transfers much of the integration and lifecycle ownership to the enterprise. Depending on the implementation model chosen, enterprises may need internal or partner support for low-level hardware engineering, firmware validation, qualification testing, burn-in processes, and automation tooling. It typically takes 18 to 24 months from program inception to the deployment of production systems. Building the internal capabilities in parallel with hardware qualifications is critical to success. It is critical for Enterprise not to cancel existing contracts with OEMs and proprietary service providers until they have clear PVT results.

It is important to clarify that enterprises do not need to adopt ORv3 racks or pursue ODM-only systems to benefit from OCP technologies. Many OCP components can be used with traditional common redundant power supply (CRPS) systems and 19-inch EIA-compliant servers. Several OEMs already offer pre-qualified servers that include OCP technologies in their bill of materials. This gives enterprises a broad range of adoption paths, including:

- Pre-qualified OEM systems with embedded OCP recognized (OCP Accepted™ and OCP Inspired™ components)
- ODM custom builds that align tightly with internal workload and site requirements
- Hybrid deployments that integrate OCP components into existing infrastructure

While public cloud services remain a strong fit for highly elastic or managed workloads, they are not optimal for every scenario. Steady-state, latency-sensitive, or cost-sensitive applications are often better hosted on-premises. OCP-based systems provide a platform for these workloads with increased transparency, reduced unit cost, and long-term flexibility.

GEICO remains committed to using OCP and ODM platforms for high-volume infrastructure due to the efficiency, agility, and transparency gained. We continue to explore OCP designs for AI/ML systems and edge deployments. The community involvement and support we received was invaluable in our process, and we are excited to contribute back with active feedback to the OCP ecosystem to inform future design iterations for enterprises to consume OCP designs. For enterprises evaluating open hardware, the key takeaway is that success depends on treating OCP adoption as a strategic enterprise initiative. The most successful outcomes emerge when infrastructure, procurement, finance, legal, and engineering teams align early and build capability intentionally to support and scale this transformation.



Glossary

AC (Alternating Current)

An electric current that reverses direction periodically. Used in most standard electrical outlets and relevant when planning data center power configurations.

BMC (Baseboard Management Controller)

A specialized microcontroller embedded on the motherboard of a server. It enables out-of-band management, including remote power control and monitoring of hardware health, independent of the server's operating system.

BIOS (Basic Input/Output System)

Firmware used to perform hardware initialization during the booting process. It provides runtime services for operating systems and programs and is an essential part of the secure boot chain.

BOM (Bill of Materials)

A comprehensive list of components, parts, and assemblies required to build a product. In the context of servers, it refers to the detailed configuration of hardware components.

DC (Direct Current)

A type of electrical current used in certain power delivery systems in data centers, such as those supporting Open Rack infrastructure. Offers improved power efficiency compared to AC in some environments.

DC-SCM (Datacenter Secure Control Module)

An OCP specification that defines a modular, pluggable control module interface for server management functions like BMC, BIOS, and TPM, enhancing security and serviceability.

DOA (Dead on Arrival)

Refers to hardware that fails to operate upon delivery. Enterprises should define handling and replacement processes for DOA systems in supplier contracts.

DVT (Design Validation Test)

A testing phase during hardware development that validates whether a system meets design specifications and requirements before mass production.

EIA-310 Rack

A traditional 19-inch server rack format defined by the Electronic Industries Alliance (EIA). Still widely used in enterprise data centers.

FOSS (Free and Open Source Software)

Software with source code that anyone can inspect, modify, and enhance. Many OCP technologies rely on or are delivered as FOSS, such as OpenBMC and firmware signing tools.

IEC 60320 (C13/C14, C19/C20)

Standard power connector types defined by the International Electrotechnical Commission. Used to support hybrid power delivery when deploying non-ORv3 equipment in ORv3 racks.

Incoterms (International Commercial Terms)

Globally recognized trade terms defining responsibilities between buyers and sellers for the delivery of goods. Important for clarifying logistics and liability in ODM and OEM contracts.

IPMI (Intelligent Platform Management Interface)

A legacy standard for out-of-band management of computer systems. Often replaced by Redfish in modern deployments but still relevant in older or lower-end BMCs.

L6, L10, L11, L12 (Integration Levels)

Terms defining levels of hardware and software integration readiness:

- **L6:** Component-level integration (e.g., individual boards or subsystems)
- **L10:** Fully assembled system without final site-level configuration
- **L11:** Rack-level integration, including networking, power, and cable management
- **L12:** Site-level integration including final configuration, burn-in testing, and handoff for production readiness

MHS (Modular Hardware System)

An OCP standard for designing flexible, modular servers and storage components, allowing for easier upgrades and customization.

NIC (Network Interface Card)

A hardware component that connects a server to a network. OCP NIC 3.0 is an open standard for high-performance, hot-swappable NICs.

NPI (New Product Introduction)

The process of bringing a new product into production, including validation, testing, qualification, and coordination between engineering, procurement, and logistics.

ODM (Original Design Manufacturer)

A company that designs and manufactures a product according to another company's specifications. ODMs offer cost-effective, customizable platforms often used in OCP deployments.

OEM (Original Equipment Manufacturer)

A company that produces hardware that may include components from other vendors. OEMs typically offer integrated systems with full support contracts.

OCP (Open Compute Project)

A collaborative community focused on redesigning hardware technology to efficiently support growing infrastructure demands. Includes open standards for servers, storage, racks, power, and more.

OpenBMC

An open-source firmware stack for BMCs, providing standardized management capabilities for hardware platforms.



ORv3 (Open Rack v3)

An OCP rack standard that uses a 21-inch-wide chassis with centralized power shelves and higher power efficiency compared to traditional racks.

Redfish

A modern, RESTful API standard for hardware management developed by DMTF. It replaces IPMI and is widely used in OCP and ODM platforms for system provisioning, monitoring, and firmware updates.

RMA (Return Merchandise Authorization)

A process for returning defective products to a supplier for repair or replacement. Should be clearly defined in ODM/OEM agreements.

RoT (Root of Trust)

A foundational element in a security architecture that ensures the integrity of the boot process and cryptographic operations. Often supported through secure boot and signed firmware.

SDLC (Software Development Lifecycle)

A structured process for planning, creating, testing, and deploying software. Relevant in firmware lifecycle automation and infrastructure-as-code practices.

SKU (Stock Keeping Unit)

A unique identifier for each distinct product and service that can be purchased. Used to track hardware configurations and compatibility.

TPM (Trusted Platform Module)

A secure crypto-processor used for hardware-based security functions such as secure boot and encryption key storage.

UEFI (Unified Extensible Firmware Interface)

A modern firmware interface that initializes hardware during system boot. It supports secure boot and is replacing traditional BIOS in modern systems.



References

[2024 OCP Global Summit](#) – GEICO Keynote: [Video](#) | [Slides](#)

[OCP-NIC](#)

[DC-SCM](#)

[MHS](#)

[OCP Ready](#)

[Netbox](#)

[ORV3](#)



License

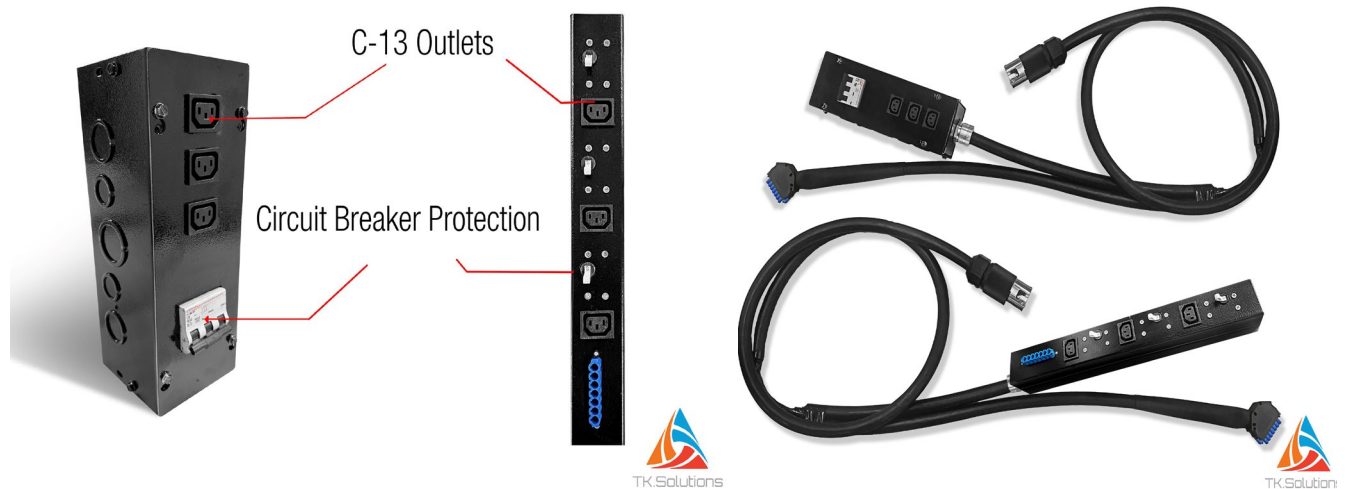
OCP encourages participants to share their proposals, specifications and designs with the community. This is to promote openness and encourage continuous and open feedback. It is important to remember that by providing feedback for any such documents, whether in written or verbal form, that the contributor or the contributor's organization grants OCP and its members irrevocable right to use this feedback for any purpose without any further obligation.

It is acknowledged that any such documentation and any ancillary materials that are provided to OCP in connection with this document, including without limitation any white papers, articles, photographs, studies, diagrams, contact information (together, "Materials") are made available under the Creative Commons Attribution-ShareAlike 4.0 International License found here: <https://creativecommons.org/licenses/by-sa/4.0/>, or any later version, and without limiting the foregoing, OCP may make the Materials available under such terms.

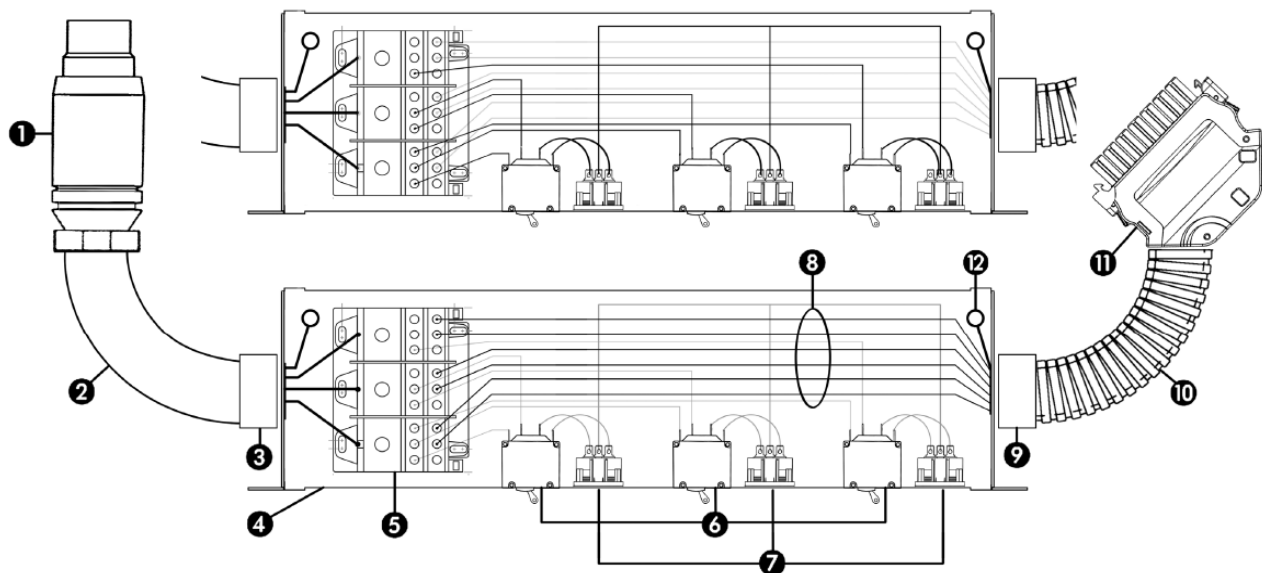
As a contributor to this document, all members represent that they have the authority to grant the rights and licenses herein. They further represent and warrant that the Materials do not and will not violate the copyrights or misappropriate the trade secret rights of any third party, including without limitation rights in intellectual property. The contributor(s) also represent that, to the extent the Materials include materials protected by copyright or trade secret rights that are owned or created by any third-party, they have obtained permission for its use consistent with the foregoing. They will provide OCP evidence of such permission upon OCP's request. This document and any "Materials" are published on the respective project's wiki page and are open to the public in accordance with OCP's Bylaws and IP Policy. This can be found at <http://www.opencompute.org/participate/legal-documents/>. If you have any questions please contact OCP.

Appendix A

i GPS (ORV3 C-13 Power Outlet Box) Specifications and Diagrams



ORV3/C-13 Power Box



- | | |
|-----------------------------|-------------------------------|
| 1- Hubbell CS8365C | 7- Qualtek C-13 716W-X2/02 |
| 2- 8/4 W Rated Cable | 8- 10 gauge MTW |
| 3- American Fitting CG100K | 9- 3/4 BLACK I FLEX Connector |
| 4- Custom Enclosure | 10- 3/4 Black I FLEX |
| 5- ALTECH 38075 | 11-OCP ORV3 Connector |
| 6- Heinmann JA2S-Y156-12P15 | 12-Ground Terminal |

DRAWN Domenick DiMasi	DATE 10/1/2025	Cage Electric & Products Co.	
CHECKED Joe DeSando	10/1/2025	90 Riverdale Rd. Riverdale N.J. 07457	
OK Anthony DeSando	10/1/2025	TITLE ORV3/C-13 Power Box	
APPROVED Joe DeSando	10/1/2025	SIZE A	REV A
Note: THE INFORMATION CONTAINED IN THIS DOCUMENT IS PRELIMINARY TO THE DESIGN AND CONSTRUCTION OF THE PROJECT. IT IS NOT TO BE USED FOR CONSTRUCTION OR FOR ANY OTHER PURPOSE WITHOUT THE WRITTEN APPROVAL OF THE DESIGNER. THE USER SHALL BE RESPONSIBLE FOR OBTAINING ALL NECESSARY PERMITS AND FOR THE PROTECTION OF THE PROJECT. THE USER SHALL BE RESPONSIBLE FOR THE PROTECTION OF THE PROJECT. THE USER SHALL BE RESPONSIBLE FOR THE PROTECTION OF THE PROJECT.		SCALE N/A	SHEET 1 OF 1

-
- ii Unit cost per core was normalized across processor generations and did not credit instructions per cycle (IPC) gains or other generational performance improvements. Even under this conservative method, GEICO realized more than fifty percent lower cost per compute core and more than sixty percent lower cost per gigabyte of storage versus prior OEM systems and comparable public cloud services.
- iii Storage unit cost per GB was normalized as follows: for public cloud, averaged across SSD and HDD offerings; for on-premises, across the all-flash SAN configurations in production during the baseline period. Usable capacity (post RAID/erasure coding, endurance reservation, and spares) was used. No credit was taken for performance differences, latency, data-reduction effects (compression/deduplication), or power/density. This method is conservative toward public cloud pricing; the reported >60% lower unit cost for storage remains under these assumptions.

