The Rack Report | Q1 2026

Your inside look at what's powering tomorrow's data centers.

Perkins Coie

Legal and Regulatory Considerations for Data Center Development on Federal Land

by Kelly Doran, Laura Morton, Greg Vogel, Jessica Lockhart, and Madison Plummer

Building a data center on federal land introduces obligations and oversight mechanisms that often differ significantly from private sector development. On federal land, the federal government may retain ownership, regulatory authority, and inspection rights, which means that projects must often follow federal real estate, environmental, security, and compliance requirements throughout construction and operations.

Federal agencies may use several types of instruments to make land available for data center development. One common tool is the enhanced use lease (EUL), which allows agencies such as the Department of the Army to lease nonexcess property for long-term commercial development. Recent Army EUL solicitations indicate that these agreements can authorize developers to finance, construct, and operate data centers on military installations for terms up to 50 years. For example, an Army EUL at Fort Hood (now Fort Cavazos), Fort Bragg (now Fort Liberty), Fort Bliss, and Dugway Proving Ground illustrate typical federal requirements. Developers must conduct environmental reviews under the National Environmental Policy Act (NEPA), complete Environmental Condition of Property (ECP) reports, and comply with all applicable federal, state, and local laws throughout development and operations. These federal leases also provide agency inspection rights and require the developer to restore the land at the end of the lease term. These requirements differ from private sector ground leases, where inspection and restoration obligations are typically more limited.

Other agencies may also use traditional long-term leases, which rely on existing leasing authorities and allow them to select developers through competitive processes. In addition, energy-related property authorities may be used where a project provides onsite power or supports federal energy infrastructure goals, an approach encouraged by federal directives identifying priority federal sites for large-scale data center development, co-located with certain energy sources, including geothermal and nuclear energy. For example, the U.S. Department of Energy (DOE) has accelerated efforts to transform sections of its federal land portfolio into strategic hubs for AI-enabled data centers and advanced energy infrastructure by issuing four solicitations for data centers to be sited on DOE laboratory lands—Idaho National Laboratory, Paducah Gas Diffusion Plant, Oak Ridge National Laboratory, and the Savannah River Site.

But political priorities to site projects on these national laboratory lands do not mean data centers will be up and running as quickly as may be desired or projected. Multilayered, technology- and project-specific federal and state statutory and regulatory requirements still apply to constructing both data centers and the generation sources that power them on federal lands. Leases must be negotiated pursuant to DOE jurisdiction under the Atomic Energy Act (AEA) and the DOE Organization Act, which provide DOE with the authority to sell, lease, grant, and dispose of real property originally acquired in connection with AEA purposes. Like DOD, DOE must make decisions on the availability of the property following evaluations of mission need, land use plans, environmental conditions/status, potential environmental impacts, and the interests of the local community and tribes. Ultimately, when balanced against protection of the environment, water resources, cultural resources, and the interests of surrounding communities and tribes, developing on federal lands might be more difficult and time-consuming than necessary for the rapid growth of data centers and their power sources.

The federal government may also enter a direct contract to use the data center as an end customer. In these cases, the federal contract is governed by procurement regulations, such as the Federal Acquisition Regulation (FAR) and agency supplements like the Defense Acquisition Regulation Supplement (DFARS). Typical federal contracts include requirements related to information and physical security controls, such as the Cybersecurity Maturity Model Certification (CMMC), incident reporting, data handling, audit rights, and ongoing compliance with federal standards.

© 2026 Perkins Coie LLP

These traditional, FAR-based procurement contracts—as well as other common federal contract vehicles like grants, cooperative agreements, Other Transaction (OT) agreements, and Cooperative Research and Development Agreements (CRADAs)—may be used in whole or in part to build out a federal data center or aspects of a data center for federal use.

Federal contracts and agreements contain federal requirements that can create a broader risk environment for developers. Work performed on federal land or under federal agreements often involves detailed documentation, regulatory filings, and compliance certifications that the government relies on to monitor performance. For example, these agreements require representations that address a broad range of issues, such as certifying an entity's size status, prohibiting human trafficking, and safeguarding sensitive information. If information provided to the government is incomplete or inaccurate, developers may face increased scrutiny or enforcement action under federal fraud and compliance statutes, such as liability under the False Claims Act and suspension or debarment from federal contracting. This risk has become more pronounced following the U.S. Department of Justice's creation of the National Fraud Enforcement Division, which is focused on strengthening oversight of activities connected to federal program.

© 2026 Perkins Coie LLP