BEHIND THE WALLS OF A DIGITAL PALACE: UNDERSTANDING, BUYING, OPERATING, AND FINANCING DATA CENTERS

SUSAN J. BOOTH is a partner at Holland & Knight. She is a Los Angeles real estate attorney with a national practice focused primarily on purchase, sale, and capital market transactions involving data centers, hotels, office buildings, multifamily developments, shopping centers, industrial parks, senior-living centers and mixed-use projects. Susan represents domestic and international commercial banks, pension funds, private equity funds, debt funds, real estate investment trusts (REITs) and family offices and has closed more than $1 billion in transactions in each of the past several years.

Susan's extensive capital markets experience includes both commercial mortgage-backed security (CMBS) and portfolio loans (acquisition, development, construction, revolving, bridge, term, permanent, mezzanine, EB-5, and Sharia compliant), syndication and participation arrangements, joint venture agreements and mortgage loan portfolio sales/acquisitions. Even in the best of times, a portion of her practice is dedicated to assisting mortgage and mezzanine lenders, equity players, and borrowers in developing and implementing strategies to resolve the issues arising from non-performing real estate assets. She has written and spoken extensively on loan workouts, options for handling troubled real estate assets, considerations in foreclosure, and navigating through California's anti-deficiency laws.

Susan has almost three decades of experience representing clients in the acquisition and financing (as both lender and borrower) of data centers. She spent many years on the Director's Committee of Holland & Knight and also spent more than a decade as the head of the firm's West Coast Real Estate Group.

The author thanks the following people for their valuable contributions to this article: Alexis Ford Kernot, Vice President and General Counsel at Digital Realty Trust; Mark Govan, Director at Global Compute Infrastructure; Christian Grossman and Jake Lebovic, both summer associates at Holland & Knight LLP; and Rod Clement, Partner at Bradley.

INTRODUCTION[1]

There are people who believe that zombies will take over the world one day. Today, however, digital information rules the world. In the United States and many other industrialized nations, almost all non-verbal communications (as well as notes and transcriptions of verbal communications) are now stored, transmitted, and processed in a digital format. Data centers are the palace in which that digital information resides.

A data center is a highly specialized, secure facility designed to provide a safe, dependable, and controlled environment for the fast, reliable, and uninterrupted storage, processing, management, and transmission of digital data. Data from a source located outside of the data center is transmitted to and from the data center building through a fiber optic cable (a "fiber"),[2] which is a specific type of conduit that transmits data in the form of light pulses over long distances. Within the data center, data may be stored and/or processed before being transmitted to other users, storers, or processors located at the same or another data center.

From the outside, a data center looks like a nondescript industrial building or an office building with darkened windows. On the inside, it is filled with an extensive array of computing and networking infrastructure, including cables, racks, servers, storage systems, networking equipment, power sources, and coolers. The often-chaotic arrangement of cables and wires within a data center masks the sophistication of the underlying network architecture and the complexity of the computing equipment housed therein.

Data centers are designed to accomplish three primary objectives.[3] The first of these objectives is to minimize the time that it takes to store, transmit, and process the digital information to, from, and inside of the data center. Within the industry, this concept is referred to as "latency" and is measured by the time it takes the computing equipment to respond to a user's request. The longer it takes for the data to be transmitted, the higher the latency. Even the slightest of delays, measured in small fractions of a second, may be long enough to render information valueless (e.g., to a stock trader who needs real-time information).[4] Time delays also reduce productivity and efficiency because users must wait for the information to be uploaded before they can act upon it. Those readers who are old enough to recall accessing the internet through a telephone line can attest to the greater productivity that is achieved through today's much faster ethernet and wireless connections.

The second principal objective of a data center is to enable digital data to be transmitted and processed seamlessly, without any kind of interruption. To achieve this continuity, many data centers employ backup arrangements for one or more of their critical systems, such as electrical power, network distribution, connectivity, data storage, fire suppression, and security. Data centers are evaluated by the number and strength of their backup systems, referred to within the data center industry as "redundancy."[5]

The third principal objective of a data center is to provide a secure facility to ensure that the confidentiality and integrity of the data is maintained. This security is not only highly desirable but also mandatory in many instances. Numerous companies must comply with strict data protection and privacy regulations applicable to their respective industries (e.g., Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS)).[6]

To ensure the security of a data center facility, a combination of physical and electronic measures is instituted to restrict access to the data center. Some data centers conduct extensive background checks and use biometric measurements for admittance. The data is also protected electronically through encryption, firewalls, monitoring, and other preventative security systems.[7] In single-tenant facilities, if the information is particularly sensitive, a data center tenant may prohibit access by non-approved personnel even in an emergency. In the most restrictive data center leases, a property owner may not be allowed to access certain areas of the tenant's space except in specified and limited types of emergencies.

Data centers house massive amounts of computing equipment and computing infrastructure which operate continuously and require a constant (and cool) temperature to avoid overheating, which has the potential to disrupt computing operations. Besides latency and redundancy, a key data center measurement is its information technology (IT) load. The IT load measures the total electrical power demand of the IT equipment and systems within the data center, as distinguished from other electrical components within the data center, such as lights and cooling equipment.[8] A data center developer needs to know the average expected IT load and the maximum IT load of the facility in order to design and construct the facility's architecture and infrastructure (e.g., cooling elements and overall power) that would most efficiently and satisfactorily support the IT load.[9]

Measuring the IT load does not stop once the data center has been completed. A data center operator[10] will continuously monitor the IT load to ensure that the cooling system and other infrastructure is providing the necessary support to the computing system. This continued monitoring helps ensure that the vast resources within the data center are allocated in a way that maximizes the efficiency and reliability of the data center.[11]

The electrical power required for the IT load and the supporting infrastructure make data centers more ravenous consumers of electricity than other real estate product types. For example, a typical office building will use an average of 13.6 watts of power per square foot,[12] but a data center will rarely

use fewer than 100 watts of power per square foot. Many data centers will use several hundred watts of power per square foot.[13]

Data centers are often categorized based upon the maximum level of power that they are able to provide. A data center deployment located in a shared facility may consume just a few kilowatts (KW) of power.[14] In contrast, a large data center deployment may use tens or hundreds of megawatts (MW) of power.[15] Regardless of the size of a data center, effective management of the electrical power is crucial to a data center's successful operations.

Data center demand has increased continuously and exponentially since the start of the industry.[16] This demand swelled during the Covid-19 pandemic because of the number of people working from home, which heightened the technological and connectivity requirements of many businesses.[17] It has not slowed even though many people have returned to work because of the IoT (Internet of Things [i.e., growth of products that store and process digital data, such as Apple watches and Nest thermostats])[18] as well as the growth of artificial intelligence,[19] which requires considerable computing power to handle increasingly complex tasks.[20]

Bridging the delta between data center demand and data center supply poses a formidable challenge. Beyond the costs and complexities of designing a data center, a fundamental requirement for a data center's successful operation is reliable and high-quality electrical power. Currently, utility companies throughout the United States need to create additional infrastructure to increase the amount of electrical power that they can make available to users.[21] As a result, data center developers are exploring alternatives, including ways to make their data centers greener and more energy efficient.[22] Some developers are even trying to develop their own source of own electricity.[23]

TYPES OF DATA CENTER USES

Data centers are often highly customized and tailored to meet the unique requirements of their actual or targeted users. This customization results in a wide array of uses, both within a single data center and among data centers. Many data centers will have auxiliary office space and storage space, but this space is usually small relative to the computing operations' area. The most common types of data centers (based upon the operations within a data center) are discussed below.

Enterprise Data Center

An enterprise data center is operated by a company for its own use to support its internal computing infrastructure and operations. A user may own the building, or it may lease the building (or a portion thereof).

In many respects, an enterprise data center in which a user occupies all (or a substantial part) of the data center resembles a traditional real estate product because the landlord leases space to the tenant, and the tenant is responsible for the operations within its space. In the context of a data center, the basic lease structure is that a landlord will provide the space and agree to make available to the tenant a specified level of electrical power. A landlord may also bring the fiber connection to an inside wall of the data center building. Beyond a specified end point within the landlord-provided infrastructure, a tenant would be responsible for almost everything else, including designing its own internal systems and networks, connecting to the fiber, bringing in its own equipment and managing its operations.

The owners and tenants of enterprise data centers are typically organizations that require significant amounts of customized computing infrastructure to support the vast quantity of data that they need to store, process and transmit. Sometimes these users also have heightened security concerns because of the sensitivity of their data. The foregoing user demands may be accommodated best in an enterprise data center.

Companies like Google, Microsoft Azure, and Amazon Web Services operate multiple enterprise data centers throughout the country. Some they own, and others they lease.[24] Healthcare companies, financial institutions, utility companies, large universities,

and the federal government are examples of other types of organizations that frequently occupy enterprise data centers.[25]

Colocation Data Center

A colocation data center, sometimes referred to as a retail data center, houses servers and networking equipment for many different organizations in a shared setting. Each organization would have the right to use a specified area of space, which may be as small as a single 19-inch rack (i.e., shelf), within the data center. Each organization would provide its own computing equipment, which would be placed in a separate (i.e., segregated from the equipment of other users) locked cabinet, cage, or suite and would have responsibility for ensuring the integrity of its own data. In turn, a data center owner would agree to make available to a user: (i) a specified amount of power; and (ii) a variety of technical support and equipment maintenance services at an additional cost. There are standard services that will be available at most colocation data centers, but the menu of service options will vary among data centers depending upon a data center owner's business model and the needs of the data center's users.

Colocation data centers are attractive to users because their infrastructure is scalable. This means that a data center's components (e.g., the physical space, IT load, electrical power, cooling equipment, and network capacity) may be adjusted to accommodate changes in the data center's overall computing workload without causing a major disruption to a user's operations. Also, as a user's demand increases, the user would have the option of requesting additional services from the data center operator to assist the user in meeting the increased demand.

Many colocation centers also contain a physical location (or multiple locations) within the data center, commonly known as a meet-me room (MMR) or a point of presence (POP) room,[26] in which various users, network providers, and others can connect directly to each other. This direct connection facilitates the exchange of digital information by shortening the transmission time among the connected entities.

All things being equal, it will cost a user more to be in a colocation data center with an MMR than to be in one without an MMR. As a result, small- and medium-sized organizations that do not need the additional connectivity provided by an MMR often occupy colocation data centers without an MMR.

Data centers with MMRs tend to attract not just larger organizations, but also growing organizations that require scalable computing infrastructure (with an MMR being just one component of scalability), and companies that want to access data centers in multiple locations (e.g., e-commerce companies, financial institutions, media companies, and technology companies).

Colocation facilities resemble hotels in certain respects. Like a hotel guest occupying a small space in the hotel and using the hotel's amenities, a colocation user places its computing equipment in a cabinet or cage, located in a larger shared area within the data center building, and uses the "amenities" (i.e., services) that the data center owner would provide.

A user in a colocation facility typically enters into either a colocation agreement (colo agreement) or a Master Services Agreement or Master Terms and Conditions (each, an MSA) with the data center owner. All of these agreements establish the rights and obligations of the parties with respect to the use of space within the data center, the use of the electrical power, and the provision of services at the data center. Typically, a colo agreement and an MSA create a license rather than the legal interest in real estate which would be created by a lease. One of the reasons for this is, like a hotel, the arrangement is less about the physical space and more about the services that are offered. Also, since it is much easier to terminate a license following a default by the licensee than it is to terminate a lease, the license arrangement is attractive to data center owners.

Colo agreements are used more often when the relationship between a data center owner and a

user exists at a single data center whereas MSAs are used more often when the relationship between the parties (including their affiliates) exists at multiple data centers.

A colo agreement sets forth the terms under which a data center owner would: (i) grant a user a non-transferrable license to occupy a designated space within the data center (e.g., a rack, a cabinet[s], or a cage); and (ii) agree to provide the user with basic services (e.g., cooling services). A data center owner might also agree to make a specified level of electrical power available to a user. A data center user would be responsible for providing its own computing equipment.

Additionally, under a colo agreement, a data center owner would agree to make additional services accessible to a user at an additional cost, such as connecting to another user in an MMR, connecting to telecommunications providers, and obtaining installation and maintenance assistance with a user's equipment (but not at a level that would give a data center owner access to any of a user's data). Per the terms of a colo agreement, each time a user requests additional services, an order form would be incorporated into the colo agreement. The order form, which should be signed by the user, would contain the details on the specific services requested by the user and the costs thereof.

An MSA resembles a colo agreement in that a data center owner would: (i) grant a user a non-transferrable license to occupy certain space within the facility; (ii) agree to make available to the user a specified level of electrical power; and (iii) provide basic services to the user. An MSA is more expansive than a colo agreement because it governs the entire business relationship between the parties and may cover multiple data centers, frequently through execution of a short document that incorporates the MSA by reference and identifies building-specific matters (e.g., the property address and maximum available power). An MSA may also use a rider or addendum to cover multiple jurisdictions, not just within the United States but internationally as well. It is worth noting that there are material variations among jurisdictions with respect to the laws governing data centers and, as a result, to the agreements executed thereunder.

As with a colo agreement, a user under an MSA would have the right to request additional services through an order form. The order form would govern specific elements of those services (e.g., the cost, term, power usage, etc.) and be incorporated into the MSA by reference. Some data center owners offer more extensive services under an MSA than they make available under their standard colo agreement.

Cloud Data Centers

Cloud data centers are data centers where one or more cloud service providers (e.g., Amazon Web Services, Google Cloud Platform, and IBM Cloud) house and utilize their computing infrastructure and provide computing resources to third parties through the internet. These data centers tend to be in centralized locations so that the cloud service provider's network and resources are physically closer to the third parties who use its service.[27]

One of the key characteristics of a cloud data center is scalability. A cloud service provider's equipment and network capacity may be increased or decreased depending upon the then-current demand for its services. This flexibility ensures that a cloud service provider (and ultimately a consumer) is not overpaying for unneeded resources and also ensures that the ultimate user is able to access the information in the cloud quickly.

Another important characteristic of a cloud data center is that most, if not all, of its critical systems have redundancy (i.e., backup systems), which reduces the risk of a disruption in operations. All data centers seek to achieve reliability and continuity of operations, but it is particularly important for cloud data centers.

If a colocation data center operates like a hotel, a cloud data center (as between the cloud service provider and its third-party users) operates like a restaurant. A cloud service provider furnishes various

computing resources to its third-party users. As in a restaurant, these third-party users are presented with a menu of options that allows them to select their desired services while relying upon the infrastructure and expertise of the cloud service provider to fulfill their demands. Also, as in a restaurant, the computing resources of a cloud service provider are adjustable based upon its needs.

An MSA is typically the document that governs the relationship between a data center owner and a cloud service provider. Since cloud service providers tend to be large IT companies that exist in multiple data centers, it is easier for the parties to negotiate an MSA agreement once and then expand the scope of the MSA to cover any new data centers added in the future.

Edge Data Centers

Edge data centers are smaller data centers located close to the end user. They are designed to process information locally rather than through centralized data centers. They also tend to prioritize low latency.[28] Despite their smaller size, reliability is important, so they often have redundant backup systems.

Originally, edge data centers were found primarily in rural locations that did not have access to the facilities and equipment used by larger data centers in heavily populated areas. More recently, demand for low latency has driven edge data centers to suburban areas that are closer to their end users.[29]

Edge data centers are used by organizations that benefit from being closer to their respective end users. These organizations may include utility companies, telemedicine providers, and autonomous transportation companies,[30] all of which benefit from the ability to process large amounts of data quickly and locally.

Depending upon the purpose for which the edge data center is being used, the agreement between a data center owner and user could take the form of a lease, colo agreement, or MSA.

Hyperscale Data Centers

A hyperscale data center is distinguished from other types of data centers by its size and electrical power rather than by the nature of its use. Any of the above-referenced data centers could be a hyperscale data center, and cloud data centers frequently are. Hyperscale data centers are designed to accommodate the processing, storage, and transmission of enormous amounts of data. For example, artificial intelligence processing and IoT processing often take place in a hyperscale data center because of the substantial amount of power that is required for each.[31]

By providing substantially more power than other data centers, hyperscale data centers allow a user to deploy considerably more computing equipment than a traditional data center would accommodate. It is not unusual to find more than 100,000 racks, servers, and storage systems within a hyperscale data center.[32] For this reason, it is essential that a user's equipment be scalable so that such equipment does not use more energy or other natural resources than are necessary to satisfy the then-current workload.

DATA CENTER OPERATIONS

Managing the operations of a data center, particularly one that has multiple users, is a complex and exacting task that involves continuous monitoring and adjustments. For example, a data center owner must ensure that the aggregate electrical power being used by the data center at any time does not exceed the aggregate amount of electrical power committed (i.e., agreed to be made available) to the data center from the utility company and any other power sources. A data center owner must also ensure that each of the data center's users has access to the electrical power promised to such user. Beyond that, the operator must ensure that the electrical power throughout the facility is balanced appropriately (e.g., that cooling systems have sufficient power to cool the IT load). If the temperature in a data center gets too high or the humidity rises above a certain level, the equipment may not function as intended. Even if this malfunction does not disrupt the data center's operations significantly, it could adversely

affect the optimization and efficiency of the data storage, processing, and transmissions.

Regardless of whether the relationship between a data center owner and a user is governed by a lease, colo agreement, or MSA, a data center user may protect itself from a data center owner's mismanagement by entering into a Service Level Agreement (SLA) with the data center owner (or incorporating an SLA into the lease, colo agreement, or MSA). An SLA is a contract between a data center owner and a user in which the owner agrees to satisfy specified metrics and perform certain obligations related to the data center's operations. The primary differences between the covenants in a lease, colo agreement, or MSA and in an SLA are that: (i) a data center owner is strictly liable for a breach of an SLA; and (ii) a user is limited to the remedies specified in the SLA.

SLA requirements vary widely, but, at a minimum, these requirements include the amount and availability of electrical power to be provided to the user, guaranteed minimum uptime (i.e., the minimum annual availability of a data center),[33] and the temperature range and humidity levels that must be maintained within the data center.[34] For a significant user, an SLA may impose extensive additional performance targets and criteria, including required system configurations, voltage consistency, nature of backup systems, type of HVAC equipment, and battery capacity.[35] Items such as maximum response times for certain service requests (e.g., connection requests and remote services) are most often covered in an underlying lease, colo agreement, or MSA but may also be covered in an SLA.

SLAs are extremely technical, and the specifications are typically negotiated by qualified engineers and professionals who possess an in-depth understanding of a data center's operations. There are also crucial business and legal points in SLAs that should not be overlooked. These points include: (i) where a data center owner's obligations to satisfy the SLA criteria end (i.e., at what physical point in the network does a data center owner cease to be responsible for an SLA violation); (ii) a user's obligations to assist in meeting the SLA criteria; (iii) what constitutes a default that would entitle a user to exercise remedies under an SLA; and (iv) the nature of a user's remedies.[36]

Under a properly drafted SLA, a data center owner will be responsible for matters within its control but will not be responsible for failures arising from a user's equipment or a user's mismanagement. The appropriate physical location to shift responsibilities from a data center owner to a user will depend in large part upon the nature of the data center's use. If a data center user occupies several floors in a facility and runs its own equipment and operations, the point at which responsibilities shift between it and the data center owner would be further upstream than it would be in a colocation facility where a user occupies a single cabinet in a shared suite. Frequently, the exact hand-off spot is not specified in the SLA because the location might change based on shifts in infrastructure and installations; however, it is essential that the parties, and particularly the technical personnel, have a clear understanding of exactly where the operational responsibility is intended to be transferred from a data center owner to a user.

An owner's agreement to satisfy the criteria set forth in the SLA is conditioned upon the user fulfilling certain of its obligations. For example, many data centers use a "hot" aisle and a "cold" aisle. These two aisles are set up in a manner that facilitates the cooling process.[37] If a user were to place its equipment in a manner that would disrupt the hot aisle/cold aisle framework, then a data center owner would not be responsible for its failure to meet temperature and humidity (and potentially other) SLA requirements.

While an SLA obligates a data center owner to achieve a number of different targets, not all these targets are of equal importance to a user. For example, a complete power shut down at the data center (including a shutdown of all backup systems) for 30 minutes would have a different impact on a user than would 30 minutes of the data center operating at a temperature one degree above the target. Thus, a data center owner and a user would negotiate when an SLA violation would trigger the user's right to exercise the remedies specified in the SLA.

Certain violations (e.g., power outage to the data center) may trigger remedies automatically while other violations may not trigger remedies until they have occurred multiple times or the owner's notice and cure rights have expired.

SLA remedies are generally limited to credits against a user's future payments to the data center owner.[38] Some users may try to expand their remedies to include damages against a data center owner, but it is extremely rare for a data center owner to agree that a user would have the right to recover damages (even if the amount of the damages is capped) regardless of the identity or leverage of a user. Certain extreme SLA violations (e.g., if electrical power to the data center is turned off completely for more than 24 hours, three times within one week) might give a user a right to terminate its underlying user agreement (i.e., lease, colo agreement or MSA), but even in that event, a user would not have a right to collect damages. Negotiations over the size and application of the SLA credits are often extensive.

Certifications

Although data center users utilize an SLA to obtain assurances regarding the reliability of the data center's operations, data center owners have the option of providing additional assurances to their users by obtaining one or more third-party certifications. Depending upon the nature of the information passing through a data center, some of these certifications may be mandatory. Other certifications may provide a data center owner with an advantage over its competitors, particularly if a data center operator does not have a strong, established reputation. Most of the available data center certifications focus on redundancy and security.

With respect to redundancy, the most prevalent certification comes from the Uptime Institute, which has developed a four-tier system to assess the reliability and availability (i.e., the frequency with which operational disruptions occur) of a data center.[39] Not every data center owner spends the time and money required to obtain a tier certification from the Uptime Institute; however, both owners and users tend to reference the tiers to describe the reliability and availability of a data center's operations even if the data center is not certified.

Tier I data centers are the lowest tier of data center because they have the lowest availability. They typically have no (or minimal) backup systems, but even a Tier I data center has an uptime of approximately 99.671 percent.[40] In contrast, Tier IV data centers provide the greatest level of availability and reliability with a minimum uptime of approximately 99.995 percent.[41] In order to achieve such a high level of uptime, Tier IV data centers have substantial redundancy. Since Tier IV data centers are more expensive to build, operate, and lease as compared to Tier I data centers, a user would tend to gravitate to the tier that most closely aligns with its needs. Typically cloud data centers have the uptime of a Tier III or Tier IV data center even if they have not been certified formally as such.[42]

From a security perspective, there are a number of national and international certifications that are available to evidence a data center's compliance with security and operational protocols. In the United States, Systems and Organization Controls (SOC) 2 is a non-industry-specific certification that focuses on the security, availability, processing integrity, confidentiality, and privacy of a data center's systems and processes.[43] Other common security-related certifications include International Standards Organization (ISO) 27001 (an internationally recognized standard for information security management systems);[44] the Federal Risk and Authorization Management Program (FedRAMP) (a US government certification that ensures a data center's security controls align with government standards);[45] and the Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) certification, which assesses the security of cloud service providers, including the data center in which they operate.[46]

DATA CENTER ACQUISITIONS

Although purchasing an existing data center asset is substantially similar to purchasing another traditional type of commercial real estate product, there

are some unique sensitivities and concerns that arise with a data center. Before commencing a data center acquisition, an investor's counsel should obtain some basic information from the investor regarding the data center, including: (i) its current use(s) (e.g., colo facility); (ii) its intended use(s); (iii) whether it has an MMR; (iv) the maximum electrical power capacity of the data center; (v) whether the data center has any general security certifications (e.g., SOC2, ISO 27001) or industry-specific regulations (e.g., Health Insurance Portability and Accountability Act (HIPAA) or Payment Card Industry Data Security Standard (PCI DSS)); (vi) whether the data center needs to procure any certifications for the current or targeted users of the data center; (vii) whether the purchaser anticipates hiring any of the seller's employees; and (viii) whether the purchaser has any direct or indirect foreign ownership. The discussion below illustrates the relevance of these questions and the importance of answering them in the early stages of an acquisition process.

Location

There is an old adage that the three most important criteria in real estate investing are: "1. Location. 2. Location. 3. Location." That adage may pre-date data centers, but it is certainly applicable to them.

Beyond the typical considerations for any commercial real estate product type, such as proximity to customers, accessibility, demand for the product, number of competitors in the same vicinity, and compliance with applicable zoning, a data center investor should focus on locational attributes that maximize the data center's availability (i.e., minimize disruptions). Important considerations in evaluating the suitability of a data center's location include the following:

Electrical Power Source

Since a data center uses substantially more electrical power than other real estate product types, it is not enough for an investor to rely on a standard "will serve" letter from a utility company. Certainly, an investor would want to know that the electrical provider has agreed to provide electrical power to the data center. In addition, an investor would want to ensure that the electrical power provider has: (i) the ability to produce the required power; and (ii) the infrastructure necessary to transmit that power to the data center to support it, its redundancy, and the power required by the users within the data center.

An investor should also assess the costs and expenses, if any, required to bring the electrical power directly to the data center. For example, an investor should determine whether additional transmission lines would be required to bring the electrical power to the site and whether one or more new electrical substations would be required to support the data center's operations. If so, an investor should also determine who would have responsibility for constructing the substations. The electrical power analysis should consider not just the data center's initial demands for power, but also increases in demand that might occur over time as the IT load of the data center's customers grows.

Connectivity

A data center is not self-sufficient. In order for a data center to function, the digital data needs a pathway (i.e., fiber optic cable) through which it can enter and leave the data center. This makes it essential for a data center to be located proximate to one or more fiber routes. It is incumbent upon an investor and its lawyer to understand: (i) where the fiber routes are located; (ii) who owns the existing fiber routes (e.g., there may be a risk of disruption if the fiber is owned by an adjacent, competitive data center); (iii) whether the fiber routes are connected directly to the data center, and if not, whether, how, and at what cost a direct connection could be achieved; (iv) whether the owner of the fiber has the necessary easements or other legal rights to bring the fiber from its original source to the data center; and (v) if the fiber routes are owned by a telecommunications provider, the financial stability of that provider (e.g., there is a possibility that a data center's operations would be disrupted if the data center had only one fiber network and the applicable telecommunications provider had filed for bankruptcy).

Coolant

It is imperative that a data center's equipment be kept cool to avoid overheating. Data centers employ a number of design features to enhance their cooling (e.g., raised flooring and hot aisle/cold aisle layout), including cooling systems. Most frequently, water is used in the cooling process; however, climate change is adversely impacting the availability of water in many locations, causing water to become scarcer, more restricted, and more expensive than it was previously. As a result, and in an effort to be more green, newer data centers often use a coolant, either in addition to, or in lieu of, water.[47] Regardless of a data center's cooling mechanism, it is critical for a data center investor to confirm that the data center has a dependable and committed source of water (or other coolant). Without a reliable source of cooling, a data center would not be able to operate at capacity or, potentially, at all.

Natural Hazards

A data center investor should ensure that the data center's location minimizes the risk that the data center will be impacted by natural hazards. Among other things, this means that the data center should be in the 500-year floodplain. If it is not, the data center will not be attractive to users because of the increased flood risk.

It would be imprudent for a data center investor or its counsel to assume that an existing data center is in a 500-year flood plain. It may have been so at the time of construction, but the flood maps created by the Federal Emergency Management Agency (FEMA) could have changed following the construction of the data center. It is advisable to do some diligence beyond looking at FEMA's flood plain classification. Climate change is disrupting traditional weather patterns faster than FEMA can make changes to its maps. Accordingly, it is important for an investor and its counsel to review the recent history of the property and surrounding areas to confirm that the data center has not been impacted by any floods, and that there have been no other situations that might create a reasonable possibility of flooding which indicate that the data center may be vulnerable to flooding in the future.

Additionally, it is undesirable for a data center to be in any type of fire zone. As with flood maps, current fire zone maps are prone to inaccuracies because of recent climate change. Therefore, an investor should not rely solely upon fire zone maps and should review the recent history of the property and surrounding areas to assess the potential fire risk.

A data center investor's analysis of natural hazards should not stop with flood and fire zones. Locations near a coastline potentially prone to a tsunami or on a hillside that could be subject to erosion are also particularly undesirable. There are a number of environmental factors that could affect the success of the data center depending upon the geography of its locale. An investor should consider all applicable environmental factors prior to making its investment in a data center.

Physical Hazards

A data center investor must pay attention to any potential physical hazards surrounding the data center, focusing particularly on those that could cause catastrophic events. Even if the risk of a catastrophic event is remote, it could adversely affect the data center's operations. Anything that could threaten the continuity and reliability of operations make the data center less attractive and competitive to users. It is impossible to identify all the hazards that could reduce a data center's desirability, but data center investors typically seek to avoid having a data center located: (i) in close proximity to active train tracks because of the concern that a train might derail and hit the data center; (ii) under a flight path because of the concern that a plane would collide with the data center; and (iii) near large gas pipelines because of the concern that a pipeline explosion would impact the data center.

Typically, an attorney does not have the opportunity to visit the site that its client is buying, but that does not absolve the attorney of its obligation to perform diligence on a data center's location. Attorneys should use Google Maps or a similar application to

obtain a visual picture of the property that is being acquired. In doing so, an attorney obtains a better sense of the physical site and unique concerns that should be addressed during the diligence period and in the purchase documents. When looking at a data center for a client, an attorney should expand the Google search to review the area surrounding the data center in search of potential hazards or other risks that could disrupt the data center's operations.

Compatible Neighborhood

Data centers produce noise, vibrations, and, often, diesel fumes. Locating a data center in an environment that would be sensitive to any of those matters, such as a residential neighborhood, school, or life-science building is not ideal even if permitted by zoning. Doing so might require an investor to make additional capital expenditures to mitigate the effects of the data center's byproducts. It is advisable for an investor to check the community's receptiveness to data centers. Some areas are becoming politically resistant to data centers.[48] This opposition has the potential to create challenges for a data center developer on a host of matters, including difficulties obtaining tax incentives and permits.

DUE DILIGENCE

The due diligence for data centers is substantially similar to that of other commercial real estate product types and includes a review of contracts, leases, permits, titles, surveys, financial statements, tax statements, soils reports, environmental reports, physical condition reports, building plans, and other property-related information. What makes the due diligence for a data center unique is its increased focus in certain areas.

Electrical Power

Since one of the most fundamental elements of a data center is the electrical power available to it, one of the roles of a data center investor's lawyer during the due diligence process is to evaluate the likelihood that the data center will have continuous power. This analysis can be accomplished in a variety of different ways.

First and foremost, an investor should obtain an electrical power report from a qualified energy consultant. Much like other third-party reports that an investor obtains (e.g., an environmental report and a property condition report), a power report provides a third-party analysis of the use and consumption of electrical power in the data center. A power report will not only help an investor understand the current operations of the data center, but also may assist a data center owner in improving the efficiency of the data center's operations, including by making recommendations for optimizing the data center's use of electrical power. Among the other items that a power report addresses are the following: (i) Power Use Effectiveness (PUE), which is a metric frequently used to address the energy efficiency of a data center;[49] (ii) the energy consumed by a data center, including historical information and trends;[50] (iii) power monitoring and metering, including the types of meters used, the means for measuring and monitoring power, and the granularity of the data (in terms of individual equipment as well as the data center as a whole);[51] (iv) electrical power distribution systems within a data center, including information on the redundancy, latency, and reliability of the infrastructure;[52] and (v) cooling infrastructure, including the type, energy consumption, and effectiveness of the cooling systems.[53]

Typically, a data center owner would contract with an electrical utility company for the delivery of the electrical power to the data center. It is advisable for an investor's lawyer to review these contracts carefully and assess: (i) the nature of the utility company's obligation (e.g., whether the contract includes the utility provider's commitment to deliver electrical power as opposed to the utility provider's estimate of the power that it expects to be able to deliver); (ii) the amount of power that the utility company has agreed to make available to the data center (both the guaranteed minimum and maximum capacities, if applicable); (iii) any conditions (other than payment) that must be satisfied before the utility company is obligated to provide electrical

power to the data center (e.g., whether the provision of power is conditioned upon the building of new infrastructure by the utility company or the data center owner); (iv) whether or not the power is presently available or is expected to be available at a future date; and (v) whether there is a maximum term on the contract. Even if the contract seems watertight from an investor's perspective, an investor and its counsel should investigate the utility company and not rely solely on the contract.

In addition to reviewing the contract, a data center investor and its lawyer should consider the reliability of the utility provider (e.g., its financial condition and past performance) and, for existing data centers, any historic disruptions of power emanating from the utility provider and otherwise. These disruptions may take many different forms. Below are some examples, but the list is certainly not comprehensive.

In July 2022, Dominion Energy notified its data center customers in Eastern Loudon County, Virginia (a data-center-heavy area frequently referred to as "data-center alley") that the power for new facilities would be delayed for years because the utility's infrastructure could not handle the demand.[54] Subsequently, Dominion Energy announced that "[a]fter completing a comprehensive analysis of our system and accelerating several near-term projects, we've been able to lift the temporary pause and resume new data center service connections on an incremental basis."[55] Even with the turnaround in Dominion Energy's position, the amount of electrical power it anticipates providing may be less than the amount that the data centers are expecting, and shortages could persist until Dominion Energy's new infrastructure is completed in 2026.[56]

Another example involves Pacific Gas and Electric (PG&E), which filed for bankruptcy in 2019 but has since emerged.[57] For investors who were considering whether to buy a data center serviced by PG&E, it would have been important to understand the effect of the bankruptcy proceedings on the enforceability of previously executed electrical power commitments by PG&E to the data center and on any contracts involving obtaining electrical power from a third-party source.

In recent years, California, among other states, has faced rolling blackouts from its electric utility providers during times of peak demand. It would be important for a data center investor to understand the frequency and duration of these blackouts and assess the likelihood that they would adversely impact the data center's operations, including the cost and impact of running generators during such blackouts.

As a final example, some utility companies have an unofficial "use it or lose it" policy, meaning that if the electrical power is not being used by a facility, a utility company may re-direct the excess power elsewhere despite the utility company's commitment to make the power available to that facility. Such a policy would adversely affect a data center's operations if it were to result in the data center's inability to access the power it needed when demand increased.

Fiber Access

As noted above, a data center cannot fulfill its intended function unless it has fiber to transmit the data in to and out of the data center. Proximity to the fiber is necessary but not sufficient; a data center owner must also have all of the legal rights to use the fiber. Accordingly, a critical part of a lawyer's due diligence is: (i) determining the identity of the owner of the fibers from their originating source to the data center; (ii) confirming that the owner of the fibers have an easement or other permanent legal right to use the real property under which the fibers are located; (iii) determining where and how the fibers connect to the data center; (iv) ascertaining the ownership of, and responsibility for, the fibers once they enter the data center; (v) identifying the costs associated with using the fibers; and (vi) reviewing and analyzing each of the fiber contracts, in a manner similar to the legal analysis applicable to the electrical power contracts, to ensure that the data center is able to rely on the perpetual (or at least long-term)

use of the fibers. This diligence may seem excessive, but it is critical.

This author worked on a data center acquisition that failed to close because the fibers connecting the data center to the end users ran under an adjacent property, and the owner of those fibers had no legal right to locate the fibers under the adjacent property. The owner of the adjacent property did not object to the existence of the fibers but would not grant an easement or other legal right for the fibers to traverse its property. Further, the owner of the adjacent property had taken steps to ensure that the owner of the fibers would not acquire rights through the adjacent property by adverse possession or otherwise. Effectively, this meant that the data center that was being acquired could be shut down instantaneously if the adjacent property owner ceased to cooperate and demanded the removal of the fibers on its property. Even if this risk were considered small, it was not a risk that the data center investor was willing to accept.

The investor and its counsel may want to consider performing diligence on the fiber providers, which are often telecommunications companies. For example, if there were only one fiber in and out of a data center, then the data center would be completely reliant upon that fiber to operate. In this instance, it would be prudent for a data center investor to investigate the financial stability and reputation of the fiber provider. In contrast, if there were multiple fibers in and out of the data center, each owned and operated by a different company, then the failure of one company might not have a material adverse impact on the data center's operations.

Security Compliance

Both physical security and cyber security are critical to the successful functioning of a data center and should be an area of focus for the investor and its counsel. If a data center has a current data center certification (e.g., SOC2 or ISO 27001), then an investor may not consider it necessary to obtain an additional third-party report to assess the overall security of the data center.

If a data center is performing operations that are subject to HIPAA, PCI DSS, or other regulations, then an investor and its counsel should confirm that the data center has the appropriate certifications for such use. Otherwise, the data center is at risk of losing some of its customers. It is worth noting that since a data center owner would not have access to the data of its users, an owner would not know whether any regulatory certifications are required unless the owner has been notified by a user. This notification typically takes the form of an obligation imposed upon a data center owner in a lease, MSA, or colo agreement.

If a data center does not have any current security certifications, a potential investor should consider whether to obtain a third-party security assessment prior to acquiring the data center. A security assessment typically evaluates a number of matters, including: (i) the data center's established physical and electronic security policies; (ii) the operations' compliance with established security policies and compliance with any applicable regulations (e.g., HIPAA); (iii) the overall effectiveness of the data center's infrastructure and vulnerabilities; and (iv) the mechanisms for protecting the privacy and confidentiality of data.[58] Even if a data center does not need any regulatory certifications for its existing users, the investor may want to expand the security report to include an assessment of whether certifications reasonably would be available to the data center for future regulated users (e.g., hospital systems).

Condition of Systems

Data center investors, like other real property investors, generally obtain a Property Condition Report to tell them about the general condition of the improvements and building systems; however, a data center investor's investigation should not stop there. An investor should obtain a report that assesses the condition of the critical infrastructure and equipment in the data center, the remaining useful life, building management systems, Tier levels/equivalents, energy efficiency, and potential points of failure.[59]

In addition to evaluating a data center's primary systems, an investor would be wise to assess the backup systems as well to ensure that they are functioning properly. To accomplish this, an investor would obtain a third-party report that assesses the redundancy of the backup infrastructure and processes and determines whether they meet the standards that the data center has committed to in the SLAs and otherwise. This type of report may include an analysis of one or more of the following: (i) the effectiveness, reliability, and scalability of the backup systems; (ii) the backup testing and verification processes, including frequency and comprehensiveness; and (iii) redundancy and disaster recovery capabilities of the systems and their ability to continue to operate in the event of a disaster or failure of the primary system.[60]

Equipment Leases

The due diligence involved in the acquisition of a real estate product includes an evaluation of equipment leases. In this author's experience, traditional real estate products often have equipment leases for incidental equipment (e.g., photocopiers) but do not rely on equipment leases to finance the acquisition of major equipment. Similarly, data center owners do not tend to finance their equipment. In contrast, data center users frequently enter into equipment leases.

Operating costs, scalability, maintenance costs, and constantly changing technology often motivate a data center user to lease some of its computing equipment. By leasing equipment rather than buying it, a data center user can reduce its up-front capital investment and spread the costs over the term of the equipment lease. It can also provide a data center user with greater flexibility and scalability because the user can add or remove equipment as necessary to match its demands. Data center users rely heavily on technology, which changes rapidly. By leasing equipment rather than buying it, a data center user would be able to replace outdated equipment at the end of a lease term with newer and more competitive equipment.

Another reason that some data center users elect to lease some of the equipment rather than buy it is that many equipment leases place maintenance responsibility with the lessor rather than the lessee. While this allocation of responsibility may appeal to some data center users, it could deter others because of the security concerns that arise by having third parties maintain the equipment.

It is incumbent upon a data center investor and its counsel to ensure that the investor fully understands which equipment leases are an obligation of a data center owner as opposed to the user.

SLAs

An SLA is often an exhibit to a lease, MSA, or colo agreement rather than an independent contract. Regardless of the form they take, SLAs should be a principal focus of any data center investor's due diligence. If a data center does not achieve the metrics and targets set forth in an SLA, then the data center could lose income because of fee credits provided to a user as a remedy for an SLA violation. Even worse, a user might have the right to terminate its lease, colo agreement, or MSA because of an SLA violation.

Most data center owners have a preferred form of SLA. As part of its diligence, a data center investor should review the seller's form to confirm that the data center is able to achieve the requirements established by the SLA. Beyond reviewing the standard form of SLA, an investor and its counsel should also review any user's SLA that differs in any respect (regardless of how minor the deviation may seem) from the SLA form.

In addition to a typical contract review, an SLA should be reviewed by a specialist. SLAs are highly technical, so only someone who is a trained expert in the subject matter would be able to understand the full scope of an SLA's requirements in the context of the applicable data center's infrastructure and operations and assess the likelihood that the data center would be able to maintain the SLA's required metrics.

MSAs

There are a lot of similarities among leases, colo agreements, and MSAs; however, there is one unique aspect of an MSA that requires special consideration in connection with a data center acquisition. MSAs are designed to govern the entire relationship between the parties across multiple properties (and often multiple jurisdictions). Some MSAs contain provisions that contemplate the sale of a property covered by the MSA and allow for the MSA to be segregated automatically into two separate agreements (one between the original parties, and one between the purchaser and the user) upon the sale of a property. A surprising number of MSAs do not contain this type of a provision or contain one that is insufficiently drafted to accomplish the stated purpose.

It is important that early in the diligence process, a data center investor's counsel determine whether the investor's purchase of the property would cause all of the MSAs to become separate independent contracts between the new owner and the applicable user. If not, then a data center purchaser should commence discussions immediately with the seller to determine how to address the matter so that the investor will be able to benefit from the MSAs without being responsible for, or impacted by, data center operations at properties other than the one which the investor is purchasing.

Warranties

While the due diligence in any real estate acquisition should include identification and review of any unexpired warranties, this step is particularly crucial in a data center acquisition. Given the quantity and cost of the equipment in a data center, a purchaser and its counsel should determine which equipment is covered by warranties, the scope of the coverage, and the requirements for a valid assignment of the warranties, including any fees that would need to be paid or consents that would need to be obtained. It is worth noting that data centers frequently have equipment located on their roofs and that such equipment could adversely affect a roof warranty. If an investor wants to purchase a data center that has equipment on its roof, then the investor and its counsel should review the roof warranty carefully to identify any adverse impact that such equipment would have on the warranty.

Employees

Data centers are complex to operate and require skilled employees. Edge data centers in remote locations may have difficulty finding employees with the requisite skill set. Even if skilled employees are available, an employee with historical knowledge of a data center, particularly a data center that has multiple users, could provide significant value to a data center purchaser.

While a seller's employees often accept new employment from a data center's purchaser, a purchaser should not expect that a data center seller would agree to allow the data center purchaser to hire the seller's employees. If a seller operates many data centers, then the seller may choose to move employees from the property being sold to one of the seller's other properties. Therefore, an investor and its counsel should determine at the beginning of a sale transaction whether the investor wants to hire any of the seller's data center employees.

If a new data center purchaser does want to hire any of the seller's data center employees, and the seller is amenable to such hiring, then the purchaser should engage labor and employment counsel to perform the necessary diligence on employment matters (e.g., analyzing information on the individual employees, salaries, and benefits and reviewing any collective bargaining agreements) as well as to advise on all applicable local and federal regulations.

Committee on Foreign Investment in the United States

Another matter that an investor should evaluate in purchasing a data center is the potential impact that the Committee on Foreign Investment in the United States (CFIUS) [61] could have on the transaction. CFIUS is an inter-agency committee, chaired by the United States Secretary of the Treasury, that advises the president of the United States on the

risks created by foreign ownership of US businesses. CFIUS has jurisdiction to review any transaction that could result in foreign control of a US business, as well as certain non-controlling foreign investments involving a TID US Business, defined as:

> any US business that: (a) Produces, designs, manufactures, fabricates, or develops one or more *critical technologies*; (b) Performs the functions as set forth in column 2 of appendix A to this part with respect to covered investment *critical infrastructure*; or (c) Maintains or collects, directly or indirectly, *sensitive personal data* of U.S. citizens."[62]

CFIUS excludes from its scope certain foreign investors[63] and certain non-controlling foreign investments in investment funds.[64]

A decade ago, few real estate lawyers knew of CFIUS because it was presumed to apply only to businesses and not to real estate.[65] Even today, many real estate lawyers are still unaware of CFIUS despite the fact that in 2018, the Foreign Investment Risk Review Modernization Act (FIRRMA) expressly expanded CFIUS' authority to include the review of certain real estate transactions.[66] The Department of the Treasury subsequently adopted additional regulations establishing, clarifying, and further defining CFIUS' jurisdiction over real estate.[67]

Any data center that falls within the definition of "covered real estate" is subject to CFIUS' jurisdiction. Data centers are unique from other real estate product types, regardless of where they are located, because, under CFIUS, they could be considered a "TID US Business"[68] under the "critical infrastructure" classification or "maintenance and collection of personal data" classification or both. If a data center is so classified, then CFIUS would have jurisdiction if there were any (not just a majority) foreign investment in the data center.

Counsel to a data center investor should inquire at the start of the transaction as to whether the purchasing entity has any direct or indirect foreign ownership regardless of the size of the foreign investment. If the purchaser does, and the foreign ownership in the investor is not exempt from CFIUS as either an "excepted investor" or an excluded investment fund, then counsel must perform further diligence to determine whether the specific data center could be considered a TID US Business.

If a transaction falls within CFIUS' jurisdiction, then, depending upon the nature of the transaction, the parties may be mandated to file under CFIUS prior to closing the sale. Even if a filing is not mandatory, it may be prudent for a purchaser voluntarily to seek CFIUS' approval prior to the closing of the sale.

If CFIUS ever evaluates a transaction (including a post-closing evaluation) and determines that the transaction presents national security concerns, CFIUS may impose monetary penalties up to the value of the violative transaction, as well as a wide variety of other remedies,[69] including requiring an immediate fire sale of the property.[70] Accordingly, if a data center purchaser were to determine that its transaction falls within CFIUS' jurisdiction but decides not to file with CFIUS prior to the closing of the sale, the purchaser should still perform a thorough CFIUS-type analysis to assure itself that CFIUS would not conclude that the sale presents national security risks.

PURCHASE AND SALE AGREEMENT

A data center Purchase and Sale Agreement (PSA) is substantially similar to that of traditional real estate product types. The key differences are in the description of the property, scope of the due diligence, contract assignments, bulk sales laws, and applicable employee-related provisions and CFIUS provisions.

Description of Property

In reviewing the description of the real property set forth in a PSA, an investor's counsel should confirm that the legal description for the property includes the real property being purchased and also all of the easements, access agreements, and other legal documents that govern the rights of the fibers to travel to and from their respective sources to the data center. Fiber access is equally (if not more)

important to the data center operations than physical access. Whereas public policy in some states would mandate the creation of an access easement for a landlocked parcel, such public policy would not extend to "landlocked" fiber. Therefore, it is critical to ensure that a data center's legal description includes any fiber easements necessary for the data center to operate.

Counsel to a data center purchaser should obtain title insurance over the fiber access easements. Procuring this insurance may be challenging because many title underwriters are not familiar with the importance of fiber and may resist undertaking the extra work required to track the fiber back to its original source. Accordingly, counsel should not wait until the last moment to address the title matters because counsel may need additional time to educate the underwriter and obtain the purchaser's desired title coverage.

While many purchase agreements contain a generic reference to the real property, the improvements thereon, and the personal property, it is beneficial for a data center purchaser to include a more detailed description of the data center property in the PSA. Given the extensive amounts and types of equipment in a data center, as well as the fact that valuable equipment may be subject to a lease, it is important to be precise about the property that a purchaser is acquiring. Among a data center's assets that should be included in the property description (unless the purchaser expressly and knowingly agrees to exclude such items from its purchase) are the following: transformers, switches, servers, storage devices, networks, routers, switches, load balancers, firewalls, cables, ducts, controls, cooling systems, air conditioning units, chillers, cooling towers, power distribution units, uninterruptible power supply systems, backup power generators, backup power supplies, backup storage devices and other backup power systems, electrical wiring, fire suppression systems, fire alarms, smoke detectors, sprinkler systems, environmental monitoring systems, access control systems, surveillance cameras, biometric authentication systems, intrusion detection systems, security alarms, fire extinguishers, risers, internet exchange facilities, telecommunications networks and facilities, base intellectual property, including monitoring and management software and tools, conduits, fiber optic cables, rights governing fiber optic cables, warranties, and data center-related certifications. If known, the specific certifications should also be identified.

It is further recommended that all the equipment that is, or could be construed to be, personal property or fixtures be listed on a schedule to the PSA. Preparing such a schedule is often very labor intensive, but it is the best way to avoid any misunderstanding between a purchaser and a seller relating to the personal property and fixtures that are being transferred. A schedule is even more important in a data center where the users own or lease their equipment because of the risk that the purchaser erroneously assumes that is is buying equipment which actually belongs to a user.

Due Diligence Materials

A typical real estate PSA requires a seller to provide the buyer with a copy of all contracts (excluding contracts that will terminate at the closing of the sale). Counsel for the purchaser of a data center may want to expand the generic contract requirement in a PSA to expressly include specific key contracts such as the electrical power contracts, contracts with telecommunication providers, contracts relating to the fiber, contracts with the MMR provider (if different than the seller), leases, colo agreements, MSAs, SLAs, equipment leases, warranties, and, if applicable, employment agreements, retention agreements, salary and benefits information, job descriptions, employment, salary and position history for each employee, and collective bargaining and similar agreements.

As discussed above, there are a number of third-party data center assessments that are not generally applicable to traditional real estate products. To facilitate a purchaser's diligence, it is advisable that the PSA: (i) require the seller to provide the purchaser with a copy of all of the reports that the seller has in its possession or control; and (ii) grant the purchaser

a right to obtain its own reports, including security assessments, power assessments, backup system assessments, and assessments of regulatory compliance. A data center investor and its counsel should ensure that the due diligence period is long enough for the investor to obtain and review all the necessary reports.

Contract Assignments

Frequently a data center owner is a party to material contracts (e.g., colo agreements, MSAs, and electrical power contracts) which are more complex than standard service contracts (e.g., landscaping). For example, many service contracts are freely assignable and terminable on 30-days' notice without penalty whereas many other data center contracts are not assignable without a counterparty's consent, payment of a fee, and satisfaction of other conditions.

Additionally, unlike many real estate leases which are often freely assignable by a property owner, data center leases, MSAs, and colo agreements often contain significant restrictions on an owner's ability to assign the contracts. Many data center users rely upon the operational expertise of a data center owner and want the right to approve a successor owner.

Counsel to a data center purchaser should pay careful attention to the PSA provisions addressing the assignment and assumption of contracts, including the leases, MSAs, and colo agreements. Counsel to a purchaser should ensure that the responsibilities and costs of satisfying any assignment conditions are clearly set forth in the PSA. Counsel also should ensure that the purchaser has the option of extending the closing date of the acquisition to guarantee that all critical contracts are transferred legally to the purchaser at closing or that other arrangements are in place to enable the data center to continue to function post-closing until the contracts had been transferred to the purchaser (e.g., implementing a transition services agreement between a seller and a purchaser).

Certifications

If a data center has received any certifications (e.g., Uptime Institute or HIPAA), counsel to the purchaser should identify any necessary steps to ensure that the certifications will remain in effect following the closing. Any such steps should be delineated in the PSA. The PSA should set forth each party's obligations (including payment obligations) to complete each of such steps. Finally, a PSA should condition a purchaser's obligation to close upon the effective transfer of the certifications and give the purchaser the right to extend the closing if necessary to effectuate all of the transfers.

Bulk Sales

Bulk sales laws regulate the sale of a substantial portion of an inventory or a business outside of the ordinary course of its business. Many states no longer have bulk sales laws, but they have not been eliminated entirely. Depending upon the jurisdiction, a data center sale could fall within the scope of a state's bulk sales laws either because it constitutes the sale of a business or because of the valuable tangible personal property that would be transferred, such as contracts, customer agreements, intellectual property and other intangible assets. Accordingly, counsel to a purchaser should determine whether the bulk sales laws apply would apply to the acquisition, and, to the extent they would, ensure that the PSA clearly allocates responsibility for compliance, sets forth the remedies for non-compliance, and provides sufficient pre-closing time to enable compliance with all applicable bulk sales laws.

Estoppels

It is typical for a purchaser of a commercial property (other than multifamily property) to request an estoppel from all the tenants at the property, and the same is true for the purchaser of a data center. If the governing agreements are colo agreements or MSAs rather than leases, then a purchaser should evaluate the appropriateness of obtaining an estoppel in the specific context. For example, it would be unrealistic for a purchaser of a large colocation data center with thousands of users to expect the

seller to request an estoppel from each of the users. Instead, the parties might agree to obtain estoppels from the most significant users, who are usually identified based upon the aggregate amounts they pay for both space and electrical power. In contrast, a purchaser of a single-tenant facility would expect the seller to request an estoppel from the tenant.

While an estoppel certificate from a data center user contains many of the same terms as a traditional tenant estoppel (e.g., names of the parties, base rent amount, term), there are some key differences. For example, an estoppel from a data center user would identify electrical power, including the amount of electrical power that has been allocated to the user, the way the power cost would be determined (discussed below) and, to the extent applicable, the rate that the user would pay for the power. A purchaser would also want a user to identify in the estoppel whether any SLA violations had occurred and, if so, the extent of those violations and any remaining rent credits possessed by the user.

Additionally, since MSAs and colo agreements would be amended by service order requests, which could be voluminous, it may be difficult for a user to confirm the accuracy or completeness of anything other than the original MSA or colo agreement and any unfulfilled or unpaid service requests.

Prorations and Post-Closing Rent/Fees

Data centers are operating businesses as well as real estate, so a lot can change between one day and the next. Due to the dynamic nature of the business, a data center investor's counsel should pay close attention to post-closing reconciliations and true ups when drafting the provisions in a PSA that relate to prorations, rent, and fees received post-closing. For example, a service order under a colo agreement might be submitted and completed pre-closing but unpaid as of closing, uncompleted and unpaid, or paid but not completed. The PSA provisions should address each of the foregoing possibilities.

Another example of the complexity of proration calculations would be electrical power costs, which could change dramatically day to day. Depending upon how a seller tracks and charges its users for electrical power, it could be difficult for a purchaser and seller to accurately determine the pre-closing and post-closing electrical costs at the closing. In some instances, it would be prudent to perform multiple true ups prior to the final reconciliation so neither purchaser nor seller retains the other party's money for an extended period. Determining how best to address the foregoing matters is fact-specific and should be the subject of careful consideration by a data center investor and its counsel.

Employees

If a data center purchaser wants to hire any of the seller's employees, the PSA must provide for that right and set forth the process for doing so. Among other things, a purchaser's counsel should ensure that the seller grants the purchaser an express right to approach, interview, and hire the seller's employees. The purchaser should also have the right to perform diligence on the employees and all the terms of their employment. If the seller's termination of employees would trigger the Worker Adjustment and Retraining Notification (WARN) Act or other state or local laws, the purchaser's counsel should draft the PSA so that it clearly allocates responsibility for compliance to the seller, sets forth the purchaser's remedies if the seller fails to comply, and includes sufficient pre-closing time to enable the seller to comply.

CFIUS

If CFIUS has jurisdiction over a data center purchase, then a purchaser's counsel must determine whether to address this matter in the PSA. The PSA should address CFIUS expressly if a purchaser is obligated to make a mandatory filing under CFIUS or the purchaser's counsel believes it would be advisable to make a voluntary filing under CFIUS and obtain clearance prior to closing. Regardless of whether a purchaser will make a pre-closing filing, if any foreign person or entity holds any direct or indirect ownership interest in the purchaser, the PSA should obligate the seller to cooperate with the purchaser in any CFIUS review or investigation, whether before or after closing. A seller's obligation to cooperate

should include, but not be limited to, an obligation to provide any materials and other information requested by CFIUS.

LEASES, COLO AGREEMENTS, AND MSAs

A lease grants a tenant a legal interest in the subject real property. It also affords a tenant a number of legal rights that vary depending upon the applicable jurisdiction. Although data center property owners used leases more frequently during the early years of the data center industry than they do now, the industry trend has moved towards licenses (i.e., colo agreements and MSAs). Ironically, this trend has been driven by users even though a user typically has fewer rights under a license than it would under a lease.

A data center owner would continue to use a lease when a user occupies at least one suite in the data center and is responsible for the operations within its suite(s). A lease would also be used when a single user occupies the entire data center. Overall, though, the current trend in the data center industry is to use a license to govern the relationship between a data center owner and a user.

Although leases, colo agreements, and MSAs are different agreements used for different purposes (e.g., a lease would have additional provisions relating to the real estate interest such as covenants relating to hazardous materials), they share many more similarities than differences. A lease, colo agreement, and MSA will each address the following critical matters: (i) the grant by an owner to a user of the right to use certain space in the data center (i.e., lease or license depending upon the agreement); (ii) the base monthly charge (typically characterized as "base rent" under a lease and "monthly recurring charge" under a license) that a user would pay to a data center owner; (iii) the amount of electrical power that would be made available to a user; (iv) the charge that a user would pay to an owner for the use of the electrical power; (v) a user's obligations to manage its electrical power and the consequences of utilizing more power than has been allocated to it; (vi) the charge that a user would pay to an owner for other utilities and operating expenses; (vii) the amount of any security deposit; (viii) the term of the agreement; (ix) additional services that an owner would make available to a user for an additional charge; (x) incorporation of the SLA; (xi) the obligation of a user to pay taxes on its equipment and operation; (xii) requirements relating to the surrender of the space occupied by a user and, if applicable, such user's equipment; (xiii) insurance requirements applicable to both parties, (xiv) a user's waiver of certain claims and damages against an owner; (xv) an indemnity by a user for the benefit of an owner; (xvi) casualty and condemnation; (xvii) events of default; and (xviii) restrictions on assignment.

As with any agreement, most of the terms are negotiable depending upon the circumstances and leverage of the parties. Whether negotiating a lease, colo agreement, or MSA, counsel to a data center owner or user should be aware of the following provisions that are unique to data centers.

Base Rent/Monthly Recurring Charges

Whether described as "Base Rent" (under a lease) or "Monthly Recurring Charges" under a colo agreement or MSA, a data center user will pay a data center owner a specified amount of money at scheduled times (e.g., monthly basis). The amount of this charge would be based not just on the size of space that a user requires, but also on the amount of electrical power that would be made available to a user under its agreement.

Electrical Power Charges

Most data center users will pay an additional charge for their actual electrical power usage, including power used by equipment cooling and supporting the data center. The exception is typically smaller users that have only a rack or cabinet of space and will pay a fixed amount for their power without any independent measurement of their power usage. For other users, the way the electrical power charge will be calculated varies depending upon the particular data center's equipment and the terms of the agreement between an owner and a user.

The manner of payment for power usage is a commercial and technical point that will be negotiated in conjunction with other commercial points. The most common methods to calculate electrical power charges, any of which could be used in a lease, colo agreement, or MSA are as follows:

The power allocation method imposes a gross charge upon a user and would most typically be utilized when a user requires a small amount of power. Under its colo agreement or MSA, a user would have the right to consume a specified amount of electrical power. The cost of the user's actual consumption of electrical power would be included in the base charges under the colo agreement or MSA, rather than being separately charged. The gross amount would reflect not just the cost of the electrical power allocated to a user but also the electrical power costs of the data center required to support the user's equipment (e.g., cooling systems).

Under the uplift method, a separate power meter directly measures the user's IT load. A user would be required to pay for its metered IT load consumption and a percentage surcharge on the IT load to account for all the costs of operating the data center in excess of the IT load (e.g., cost of utilities used by the cooling systems). This additional charge is often referred to as the "cooling load factor" even though it may account for utilities used by mechanical and electrical equipment supporting the data center. Under the uplift model, the percentage surcharge is fixed regardless of the actual costs of supporting a user's IT load. For example, under an uplift model, a user might pay 160 percent of the direct metered costs of its IT load, of which 100 percent would be the actual cost of its IT load, and 60 percent would be the additional cost for the data center's infrastructure.

Under the PUE method, a separate power meter directly measures a user's IT load. A user would be required to pay for its metered IT load consumption. In addition, a user would be charged its proportional share of PUE based upon a formula such as the following:

PUE = Total Power Used by the Data Center/ Total IT Load of the Data Center

Proportional share = User's IT Load / Total IT Load of the data center

The actual PUE for a data center varies over time and in response to various conditions, making it a dynamic and complex model. A user would usually pay an estimated monthly amount for PUE, and there there would be a periodic reconciliation between estimated and actual costs. Except for scenarios in which a user's total utility consumption (including IT load and other utility costs) would be separately metered, such as in single-tenant facilities, this power charge model most closely mirrors a data center user's actual aggregate utility cost. Large sophisticated users are the ones that most frequently employ a PUE model for determining their power costs. Some users may try to cap the aggregate electrical power costs that can be imposed upon them; however, with the never-ending demand for electrical power likely to result in rising electrical costs, a data center owner should seriously consider the matter before agreeing to this request.

The electrical power provisions in an agreement should clearly specify how power charges are determined. When the electrical power provisions in an agreement are long or complex, a data center owner and a user may discover, after the term of the agreement has commenced, that each has a different interpretation of the provisions. To avoid this situation, it is important that each party and its counsel review the provisions independently to ensure understanding and then both parties should review the provisions together. Depending upon the complexity of the provisions, it may also be advisable to obtain a technical review of the power provisions as well. If a calculation of the electrical power charge is not fixed or would not be clearly ascertainable by a juror, then the parties should attach an exhibit to the agreement which shows at least two examples of an electrical power charge calculation to minimize the risk of a future dispute.

Electrical Load Management

Typically, a lease, colo agreement, or MSA will set forth a user's obligations for managing its electrical power usage to ensure that it does not exceed its power allotment. These agreements may further detail how much power a user would be permitted to draw on any individual piece of equipment or circuit. Depending upon the circumstances, a user might be entitled to some type of notice of a violation before penalties are assessed against it. It is worth noting that significant violations by a user could invalidate its SLA. Accordingly, it is essential that counsel and its client fully understand (and have the equipment necessary to monitor and manage) the client's electrical power management obligations.

Term

A user under a colo agreement or MSA may seek the right to terminate the agreement upon 30-days' notice. This type of provision is often sought by users who are able to disengage from one data center and move to another with relative ease. This provision may also be sought by users who want the right to move if the data center's operations are efficient or effective. Large, dependable data center owners are frequently able to resist such a termination right and require a user to commit to a longer-term arrangement. Accordingly, termination rights are often a source of negotiation between a data center owner and user.

Policies and Procedures

Typically, a lease, colo agreement, and MSA will each obligate a user to comply with the data center's policies and procedures. These are often far more detailed and cumbersome than the policies and procedures attached to an office, industrial, or retail lease. Many of these provisions are designed to maintain the security and confidentiality of the data and the facility in which the data is housed. These procedures may also include highly technical requirements (e.g., maximum structural load per square foot). Counsel for a data center user should review these provisions carefully. It is worth noting that if a user violates the policies and procedures (or certain policies and procedures), the user's SLA could be invalidated, at least in part.

Liability of a Data Center Owner

While any property owner is concerned about its liability under a lease, a data center owner's concerns are magnified because of the extensive nature of its obligations and the critical role that it plays in a user's operations (e.g. a user's equipment attaches to the facility's infrastructure or an owner provides operational services to a user). Unlike an owner of an office or industrial building whose obligations to a tenant would be limited, a data center owner bears a material risk that its action or inaction can damage a user and its customers. This risk, combined with the sensitivity of a user's data within a data center and the potential consequences of a disruption to a user's (or a user's customer's) business means that, if a data center owner's liability were uncapped, that owner could face a claim for substantial damages, including consequential damages.

While many commercial property owners protect themselves from liability by including a provision in the applicable lease that limits the landlord's liability to its interest in the property, this typically is not an adequate safeguard for data center owners whose property is often valued at hundreds of millions of dollars (or more).

Instead, data center owners typically limit their liability in one of two ways. For certain matters, such as services provided by a data center owner to a user, an owner's liability often is limited to the aggregate amount paid by the user for those services. For more significant matters, liability usually is limited to a credit against future amounts payable by a user to the data center owner with an additional liability cap based on time (e.g., maximum of six months of charges) or aggregate dollars. Many data center owners are also successful in limiting a users' claims to actual damages.

Mutual indemnities, often found in office and industrial leases, are not common in data center leases, colo agreements, or MSAs because a data center

owner's obligations are far greater than those of an owner of an office or industrial building. If a data center owner were to provide an indemnity to a user similar in scope to that provided by an owner of an office building, the data center owner would expose itself to substantial liability. Therefore, data center owners strongly resist providing any indemnities.

DATA CENTER MORTGAGE LOANS

Data centers are a high-value real estate product, with some hyperscale data centers valued at more than $1,000,000,000. Very few organizations have the cash available to build or buy a large data center. As a result, data center owners frequently seek third-party financing. There is often significant competition among developers to construct build-to-suit data centers for a large, creditworthy tenants. Financing these projects also sparks competition among potential lenders.

It is common for these high-credit tenants of build-to-suit space to possess a termination right under their leases if the applicable project is not constructed within 120 to 180 days of the required completion date. This termination right, which exists regardless of whether a force majeure event has occurred, presents a significant risk to both the developer and the lender of the project.

As any construction lender knows, even a simple commercial construction project may run 120 days behind in completion for many reasons, including the supply chain issues that have plagued the construction industry in recent years. Because a build-to-suit data center is highly specialized, it cannot be reconfigured easily or inexpensively for another tenant in the event of a lease termination, which could result in large losses for both the developer and the lender. In the current market, these high-credit tenants have a significant amount of leverage so it likely that they will continue to be able to obtain a lease termination right. Accordingly, a lender should account for the lease termination risk in its pricing.

While data center construction loans are typically underwritten as real estate loans, there is a split among lenders as to how to treat a bridge loan or permanent loan secured by a data center. Some lenders treat it as a real estate loan. Other lenders underwrite and document it as a secured cash flow loan. Ultimately, the loan documents for a data center loan would be substantially similar regardless of whether the loan is underwritten as a real estate loan or cash flow loan, but the focus of, and negotiation dynamics for, those documents would differ.

It is advisable for a data center owner and its counsel to determine early in the transaction how the lender will underwrite the loan. This information will help an investor and its counsel better understand the lender's concerns and the areas in which the lender may be more flexible. For example, a cash flow lender may be more likely to grant a data center owner greater control over the real estate (e.g., the ability to put certain items on title or perform certain alterations at the property) than would a real estate lender. In contrast, a real estate lender would be focused primarily on the real estate and might be more accommodating than a cash flow lender in negotiating the financial covenant terms and definitions.

Also, if the loan size is over $50,000,000, as many data center loans are, a lender might want the right to syndicate the loan. If the loan is syndicated, there is a reasonable probability that at least one lender in the syndicate would underwrite the loan from a cash flow perspective and at least one lender would underwrite the loan from a real estate perspective. It is important for the syndicate's lead agent and its counsel to understand this dichotomy and structure and negotiate the loan documents so that they address the concerns of both cash flow lenders and real estate lenders. If an agent and its counsel are not sensitive to both sets of concerns, in order to obtain loan approval from the syndicate's members, the agent may have to ask the borrower to make material concessions near the end of the transaction, which could jeopardize the transaction and the agent's relationship with the borrower.

It is advisable for a lender that is underwriting and documenting a data center loan to expand its diligence and analysis to include the matters which

are discussed above under data center acquisitions (e.g., additional diligence matters and documentation considerations). It should also pay particular attention to the SLAs because a breach of an SLA's obligation could result in a user receiving rent credits or even having a right to terminate its lease, colo agreement, or MSA. And if other users have similar SLAs, then the breaches arising under multiple SLAs would magnify the deleterious effects on a data center's income. For this reason, both real estate lenders and cash flow lenders typically protect themselves by including debt yield and debt service coverage ratio covenants in their loan documents.

The other area of special concern to a lender is CFIUS. If the data center ownership is subject to CFIUS review, and that review is not completed prior to loan closing, then a purchaser risks a CFIUS review in the future. In a worst-case scenario, CFIUS could unwind a data center purchaser's acquisition of the data center and/or impose a substantial penalty, which could force a data center to sell quickly at a discounted rate). Under such a scenario, a lender could incur significant financial losses. Given the uncertain results of a CFIUS review, a lender may want to condition its loan on the completion of a successful CFIUS review.

It is also worth noting that if a foreign lender forecloses or takes a deed in lieu of foreclosure, then that transaction could be subject to CFIUS' jurisdiction. Any foreign lender (or lending syndicate with a member that is a foreign lender) should perform a CFIUS analysis prior to taking title to the data center to ascertain the likelihood that the transaction would fall under CFIUS' jurisdiction. If so, it would be advisable for the parties to obtain CFIUS approval prior to a foreclosure or other transfer of title to the data center. This is another risk that should be considered in a lender's underwriting.

CONCLUSION

The ever-increasing demand for data centers suggests that they are here to stay. Hopefully, this look behind the walls of the digital palace has shone a light on data centers and removed some of their mystery.

Appendix

GLOSSARY OF TERMS

Defined Term	Full Term
CFIUS	Committee on Foreign Investment in the United States
Colo Agreement	Colocation Agreement
CSA	Cloud Security Alliance
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
Fiber	Fiber Optic Cable
FIRRMA	Foreign Investment Risk Review Modernization Act
HIPAA	Health Insurance Portability and Accountability Act
IOT	Internet of Things
IT	Information Technology
IT load	The total electrical power demand of a user's IT equipment and systems within the data center (as distinguished from other electrical components within the data center such as lights and cooling equipment)
KW	Kilowatts
latency	Time it takes to process digital data
MMR	Meet-Me Room
MSA	Master Service Agreement
MW	Megawatts
PCI DSS	Payment Card Industry Data Security Standard
PG&E	Pacific Gas and Electric
POP	Point of Presence
PSA	Purchase and Sale Agreement
PUE	Power Use Effectiveness
Redundancy	Scope of back-up systems
SLA	Service Level Agreement
SOC	Systems and Organization Controls
STAR	Security, Trust, and Assurance Registry
TID U.S. Business	Technology, Data and Infrastructure US business
WARN	Worker Adjustment and Retraining Notification

Notes

1 The opinions expressed in this article are those of the author and do not necessarily reflect the views of her employer, its clients, or any of her, its, or their respective affiliates. This article is for general information purposes and is not intended to be, and should not be taken as, legal advice.

2 For ease of reference, a glossary of the defined terms used in this article is attached as an appendix.

3 What is a Data Center?, Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-data-center.

4 Elvis Picardo, Understanding High-Frequency Trading Terminology, Investopedia (Jan. 31, 2022), https://www.investopedia.com/articles/active-trading/042414/youd-better-know-your-highfrequency-trading-terminology.asp#:~:text=2%EF%BB%BF-,Latency,a%20competitive%20edge%20in%20trading.

5 What is Data Center Redundancy? N, N+1, 2N, 2N+1, CoreSite, https://www.coresite.com/blog/data-center-redundancy-n-1-vs-2n-1.

6 Data center regulations for the US, Site24x7, https://www.site24x7.com/learn/datacenter/data-center-security-and-privacy-for-usa.html; PCI DSS: What it is and What I Need to Do About it, Rack Solutions, https://www.racksolutions.com/news/blog/pci-dss/.

7 Ravi S. Vemuri, A Five-Layer View of Data Center Systems Security, 2 ISACA J., Mar. 2022, at 1, 3, available at https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/a-five-layer-view-of-data-center-systems-security.

8 Richard L. Sawyer, Am. Power Conversion, Inc., Calculating Total Power Requirements for Data Centers, White Paper #3 (2004), available at https://www.insight.com/content/dam/insight-web/en_US/article-images/whitepapers/partner-whitepapers/calculating-total-power-requirements-for-data-centers.pdf.

9 Data Center FAQ's, H5 Data Centers, https://h5datacenters.com/data-center-faqs.html.

10 For purposes of this article, the author assumes that a data center owner and a data center operator are the same unless expressly noted otherwise.

11 Julius Neudorfer & Frank J. Ohlhorst, Schneider Electric, Data Ctr. Efficiency Metrics and Methods (2010), available at http://viewer.media.bitpipe.com/979246117_954/1279665297_327/Handbook_SearchDataCenter_efficiency-metrics_final.pdf.

12 U.S. Energy Info. Admin., 2018 Commercial Building Energy Consumption Survey Table C14: Electricity consumption and expenditure intensities, 2018 (Dec. 2022), available at https://www.eia.gov/consumption/commercial/data/2018/ce/pdf/c14.pdf.

13 Josh Mahan, Understanding Data Center Energy Consumption, C&C Tech. Grp., (June 8, 2023), https://cc-techgroup.com/data-center-energy-consumption/#:~:text=in%20the%20world.-,How%20Much%20Power%20Does%20a%20Data%20Center%20Use%20Per%20Square,as%20high%20as%20300%20watts.

14 One KW equals 1,000 watts of power.

15 One MW equals 1,000,000 watts of power.

16 Miranda S. Spivack, More Data in the Cloud Means More Centers on the Ground to Move It, N.Y. Times (Jun. 27, 2023), https://www.nytimes.com/2023/06/27/business/data-centers-internet-infrastructure-development.html?auth=login-email&login=email.

17 Id.

18 Joanie Wexler, How IoT Is Impacting the Data Center, The Forecast, (May 3, 2019), https://www.nutanix.com/theforecastbynutanix/technology/how-iot-Is-impacting-the-data-center.

19 Spivak, supra note 16.

20 Id.

21 Id.

22 Id.

23 Dan Rabb, Power Shortages Are Turning More Data Centers Into Their Own Utilities, Bisnow (Jun. 11, 2023), https://www.bisnow.com/national/news/data-center/power-shortages-are-turning-data-centers-into-utilities-119340.

24 Discover our data center locations, Google Data Ctrs., https://www.google.com/about/datacenters/locations/; Azure global infrastructure, Azure, https://azure.microsoft.com/en-us/explore/global-infrastructure; AWS Local Zones locations, Aws https://aws.amazon.com/about-aws/global-infrastructure/localzones/locations/.

25 Shad Sechrist, Understanding the Differences Between 5 Common Types of Data Centers, Data Ctr. Frontier, (May 18, 2022), https://www.datacenterfrontier.com/sponsored/article/11427373/belden-understanding-the-differences-between-5-common-types-of-data-centers.

26 There are technical differences between an MMR and a POP room that go beyond the scope of this article.

27 Does Data Center Location Matter for Cloud Services?, US Signal (Jan. 4, 2022), https://ussignal.com/blog/does-data-center-location-matter-for-cloud-services.

28 Why Edge Data Centers Are Being Built in the Suburbs, LDP Assocs., Inc. (Dec. 20, 2021), https://www.ldpassociates.com/why-edge-data-centers-are-being-built-in-the-suburbs/.

29 Edge data centers: how to participate in the coming boom, PwC, available at https://www.pwc.com/us/en/industries/industrial-products/library/edge-data-centers.html.

30 Brad Alexander, Six Ways Edge Computing is Changing the Digital Ecosystem Landscape, Data Ctr. Frontier (May 25, 2022), https://www.datacenterfrontier.com/sponsored/article/11427359/dartpoints-six-ways-edge-computing-is-changing-the-digital-ecosystem-landscape.

31 Ryan Beyler, Hyperscale and edge drive data center demand as the rise of AI takes center stage, Jones Lang LaSalle (Apr. 13, 2023), available at https://www.us.jll.com/en/newsroom/data-centers-2023-global-outlook.

32 Jacob Roundy, A primer on hyperscale data centers, TechTarget (Feb. 24, 2023), https://www.techtarget.com/searchdatacenter/tip/A-primer-on-hyperscale-data-centers.

33 The importance of Uptime in the Data Center, Datacenter.com (Sep. 11, 2019), https://datacenter.com/news_and_insight/the-importance-of-uptime-in-the-data-center/.

34 Data Center SLA, Stream Data Ctrs., https://www.streamdatacenters.com/glossary/data-center-sla/.

35 Linda Rosencrance et al., Definition: service-level agreement (SLA), TechTarget, https://www.techtarget.com/searchitchannel/definition/service-level-agreement.

36 Emily Naughton, Service Level Agreements: Understanding Practical Remedies in Data Center Leases, Data Ctr. Knowledge: Indus. Persps. (Sep. 18, 2017), available at https://www.datacenterknowledge.com/industry-perspectives/service-level-agreements-understanding-practical-remedies-data-center-leases.

37 Data Center Infrastructure Resource Guide, Anixter, Inc., available at https://www.anixter.com/content/dam/Anixter/Guide/12H0013X00-Data-Center-Resource-Guide-EN-US.pdf.

38 Naughton, supra note 36.

39 Tier Certification, Uptime Inst., https://uptimeinstitute.com/tier-certification.

40 Andreja Velimirovic, Data Center Tiers Explained, Phoenix NAP (Nov. 25, 2021), https://phoenixnap.com/blog/data-center-tiers-classification.

41 Id.

42 Mary Zhang, Data Center Tiers: What's the Difference Between 1, 2, 3, and 4?, Dgtl Infra: Data Ctrs. (June 24, 2022), https://dgtlinfra.com/data-center-tiers-difference-1-2-3-4/.

43 What is SOC (System and Organization Controls) 2 and How to Become Compliant?, Marcum Tech. (Sep. 27, 2022), https://www.marcumllp.com/insights/what-is-soc-system-and-organization-controls-2-and-how-to-become-compliant.

44 The ISO provides several other certifications, including the ISO 9001 (quality management systems and compliance with customer requirements) and ISO 22301 (continuity of management systems during disruptions). What Are the Different Types of ISO Standards?, RiskOptics (Jul. 12, 2023), https://reciprocity.com/resources/types-of-iso-standards/.

45 Program Basics, Gen. Servs. Admin. FedRAMP, https://www.fedramp.gov/program-basics/.

46 Security, Trust, Assurance and Risk (STAR), Cloud Security Alliance, https://cloudsecurityalliance.org/star/.

47 Urs Hölzle, Our commitment to climate-conscious data center cooling, Google: The Keyword (Nov. 21, 2022), https://blog.google/outreach-initiatives/sustainability/our-commitment-to-climate-conscious-data-center-cooling/.

48 Matthew Barakat, Backlash to Data Centers Prompts Political Upset in Northern Virginia, Assoc Press (Jun. 22, 2023), https://apnews.com/article/virginia-election-data-centers-prince-william-229cb44d34ccf4bd1cc4e9f0d0131649 available at \.

49 What Is PUE (Power Usage Effectiveness) and What Does It Mean?, Vertiv, https://www.vertiv.com/en-asia/about/news-and-insights/articles/educational-articles/what-is-pue-power-usage-effectiveness-and-what-does-it-measure/.

50 Data Center Efficiency Report, Xcel Energy, https://www.xcelenergy.com/staticfiles/xe-responsive/Marketing/CO-MN-Bus-Data-Center-Study-Template.pdf .

51 Data Center Metering and Resource Guide, U.S. Dep't of Energy, (Feb. 2017), available at https://datacenters.lbl.gov/sites/default/files/DataCenterMeteringandResourceGuide_02072017.pdf.

52 Kazi Main Uddin Ahmed et al., A Review of Data Centers Energy Consumption and Reliability Modeling, Inst. of Electrical and Electronics Eng'rs 15236, 1 (Nov. 2021), available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9599719.

53 Id.

54 Rich Miller, Dominion Power Resumes New Connections, But Loudon Faces Lengthy Power Constraints, Data Ctr. Frontier, (Sept. 26, 2022), https://www.datacenterfrontier.com/energy/article/11436951/dominion-resumes-new-connections-but-loudoun-faces-lengthy-power-constraints.

55 Id.

56 Id.

57 Judy Lin, Newsom and PG&E strike deal to end company's bankruptcy, CalMatters (Mar. 20, 2020), https://calmatters.org/environment/wildfires/2020/03/california-pge-bankruptcy-gavin-newsom-deal. See also Associated Press in San Francisco, PG&E: California utility firm files for bankruptcy after deadly 2018 wildfires, The Guardian (Jan. 29, 2019), available at https://www.theguardian.com/us-news/2019/jan/29/pge-bankruptcy-california-wildfires-utilities.

58 Marc Blackmer, Data Center Resilience and Risk Assessment, ShardSecure (Nov. 15, 2022), https://cloudsecurityalliance.org/blog/2022/11/15/data-center-resilience-and-risk-assessment/; HIPAA Compliance Requirements, Colocation Am., https://www.colocationamerica.com/data-center-certifications/hipaa-compliance.

59 See EYP Mission Critical Facilities, https://www.eypmcfinc.com/data-center-due-diligence.

60 Christopher Tozzi, Data Center 101: Data Center Backup and Recovery, Data Ctr. Knowledge (Feb. 9, 2023), https://www.datacenterknowledge.com/manage/data-center-101-data-center-backup-and-recovery; 5 Basics for Disaster Recovery in the Data Center, Serv. Express, https://serviceexpress.com/resources/5-basics-disaster-recovery-preparation/.

61 CFIUS was formed in 1975 pursuant to Section 721 of the Defense Production Act of 1950, as amended, and as implemented by Executive Order 11858, as amended by 31 C.F.R. Part 800 (2020).

62 C.F.R. § 800.248 (2020) ((emphasis added). See also 31 C.F.R. § 800.212 (2020) ("The term covered investment

critical infrastructure means, in the context of a particular covered investment, the systems and assets, whether physical or virtual, set forth in column 1 of appendix A to this part"); 31 C.F.R. § 800.214 (2020) ("The term critical infrastructure means, in the context of a particular covered control transaction, systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security"); 31 C.F.R. § 800.215 (2020) (defines "critical technologies"); and 31 C.F.R. § 800.241 (2020) (defines "sensitive personal data").

63 31 C.F.R. § 800.219 (2020) (defining "excepted investor," which is a class of persons that are not subject to CFIUS). An excepted investor includes, among others, citizens of Australia, Canada, New Zealand and United Kingdom of Great Britain and Northern Ireland, currently the only countries whose citizens are automatically excluded. CFIUS Excepted Foreign States (800), U.S. Dep't of the Treasury, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states (last visited July 13, 2023).

64 31 C.F.R. § 800.307 (2020) (excluding certain foreign investors in an investment fund from the application of foreign ownership in a TID U.S. business).

65 At that time the law did not contain any express application to real estate transactions although it is worth noting that it did not contain any express exemption for real estate transactions either.

66 FIRRMA, H.R. 5515 115th Cong. §1703(a)(4)(B) (2018) ("CFIUS jurisdiction includes the purchase, lease, or concession of private or public real estate that: is located within, or will function as part of, an air or maritime port; [or] is in close proximity to a U.S. military installation or another facility or property of the U.S. Government that is sensitive for reasons relating to national security").

67 31 C.F.R. § 800.211 (2020) ("covered real estate means real estate that (a) Is, is located within, or will function as part of, a covered port; or (b) Is located within: (1) Close proximity of any military installation described in § 802.227(b) to (o), or another facility or property of the U.S. Government, in each case as identified in the list at part 1 or part 2 of appendix A to this part; (2) The extended range of any military installation described in § 802.227(h), (k), or (m), as identified in the list at part 2 of appendix A to this part; (3) Any county or other geographic area identified in connection with any military installation described in § 802.227(a), as identified in the list at part 3 of appendix A to this part; or (4) Any part of a military installation described in § 802.227(p), as identified at part 4 of appendix A to this part, to the extent located within the limits of the territorial sea of the United States").

68 A data center "collocated at a submarine cable landing point, landing station, or termination station" is considered critical infrastructure. See 31 C.F.R, pt. 800, Appendix A, Column 1(v).

69 See 31 C.F.R. § 800.901–2 (2020).

70 See Ralls Corp. v Comm. on Foreign Investment in the United States, 758 F.3d 296 (D.C. Cir 2014) (addressing CFIUS' ordering of the immediate divestiture of a wind farm owned by a Chinese corporation because of its proximity to a Navy training facility).