INTELLIGENCE UPDATE

# Critical national infrastructure status: what does it mean?


Peter Judge

15 Oct 2024

Governments have been classifying data centers as part of the critical national infrastructure (CNI), adding them to the list of services essential to keep a nation functioning in the event of a major incident.

CNI covers a range of sectors, such as power, water and food distribution, as well as healthcare and emergency services. CNI plans are designed to ensure that key services can access the resources they need to continue to function in the event of a natural disaster, a major accident or a physical or digital attack. The plans also look at interdependencies between sectors.

Data centers are already explicitly considered to be part of CNI in many countries, including Germany and, since September 2024, the UK. In other countries, such as the US, some data centers are "implicitly" CNI because they are essential to services on the CNI list, such as telecommunications, finance and logistics.

During a major incident, such as a fire, flood or pandemic, operators can expect the necessary approvals to keep data centers with CNI status running. This includes prioritizing electricity to facilities during an emergency, fuel for diesel backups during an extended outage, and permission for staff to travel during lockdown restrictions.

Developers can also expect CNI status to help indirectly when seeking approval for new projects.

To include data centers in national contingency plans, governments will require more information about the facilities and a better understanding of the sector's operations. However, this may affect privacy clauses in colocation agreements.

The meaning of CNI status varies by country and is often not disclosed to the public. As data centers have only recently begun to appear on CNI lists, the implications for the sector are still being worked out. Uptime Intelligence has not yet been able to determine what CNI means in all cases, however, there are certain discussions that may affect the operation of data centers that handle critical services.

The increasing visibility of data centers has already led to more regulations (see *Digital*

*resiliency: global trends in regulation*), and CNI status can be seen as a sign of an emerging "social contract" that will confer responsibilities alongside possible benefits.

CNI status is merely one result of society's increasing reliance on digital services. Whether or not they appear on an official CNI list, data centers are critical to society and can expect greater support from government — and greater attention.

# The pandemic revealed national differences

The COVID-19 pandemic illustrated the potential significance of CNI status. In 2020, recognition of the importance of data centers was patchy, and operators in different countries had different experiences when negotiating lockdown rules.

In Germany, data centers greater than 5 MW had already been formally recognized as CNI, so operators were reportedly granted automatic exemptions from travel restrictions and given approval to operate during lockdowns. Finland also recognized data centers as CNI.

In other countries, the situation was not so clearly defined and required urgent negotiations. France, Norway, Sweden and the Netherlands recognized some data centers as critical. A much larger group of countries, including Ireland, the UK and Denmark, recognized the importance of online services without formally classifying facilities as critical.

In most countries, data center staff were eventually recognized as key workers, which allowed operators to continue delivering services and manage their own risk. This development opened discussions in the sector, with some operators, which had previously been wary, now beginning to see the benefits of CNI status.

Almost all (95%) of national CNI plans now include information and communications technology (ICT), according to a 2023 report by the German Council on Foreign Relations. Although the term ICT brackets IT and communications and does not explicitly specify data centers, it means that some data centers effectively have CNI status in these countries because they are used to deliver IT services and other CNI functions.

For example, the US Cybersecurity and Infrastructure Security Agency maintains a list of 16 critical infrastructure sectors, with particular reference to cyberattacks. Data centers are not explicitly mentioned on this list, but they are critical to the operations of several sectors, such as IT, financial services and healthcare.

Many countries will have case-by-case arrangements for specific facilities. In the UK, for instance, some commercial facilities, referred to as List X sites, are approved to hold confidential information, such as defense research, for the UK government and have effectively been treated as CNI for some years.

# CNI status brings scrutiny

Even where the data center sector is explicitly listed as part of CNI, there are usually no published documents that state which facilities are included in the classification or what level of support will be available under emergency conditions. Disaster planning is usually classified due to sensitivity.

CNI designation is best seen as opening a communication channel between the government and the operators so that the sector's needs and expectations can be discussed and agreed upon. As part of this designation, data centers need to be considered alongside other services as part of plans for many specific scenarios, including an analysis of the interdependencies between sectors.

Clearly not all data centers will be considered critical, and not all data is critical either. In most countries, only data centers that are used to deliver CNI services, such as healthcare and financial services, are regarded as part of CNI. In countries that broadly classify data centers as CNI, it is acknowledged that not all facilities are actually critical.

Governments need to understand which facilities are critical and for what reasons in order to build a register of CNI data center sites and assess the interdependencies between the services involved. This list determines which colocation facilities and which aspects of hyperscaler operations can be considered CNI — and therefore important for disaster planning.

Some operators and enterprises with their own data centers may have concerns over this aspect of CNI because it will require them to share information about their facilities' locations as well as the workloads and clients that are supported. This may break the terms of the contracts they have with clients.

It has also been suggested that governments may require detailed failure reports for any incidents at a data center that affect critical services.

One data center manager asked Uptime Intelligence whether CNI status would give the state the power to enter DC premises or demand access to the data. So far, there have been no reports of any CNI rules requiring this level of access, but CNI procedures for data centers are still emerging.

There are, however, signs that data center operators will have to meet government expectations. For example, the UK government's Department for Science, Innovation and Technology (DSIT) has identified that the current concentration of data centers in two national hubs (Slough in Berkshire and London Docklands) could increase risk. As such, DSIT has signaled a desire to see facilities located in other parts of the country.

Suggestions like this are likely to develop into regional development plans, or data center zoning plans, similar to those in the Netherlands and Germany.

Another issue is the role of cloud providers and cloud services. DSIT has indicated it is aware that some critical national services may depend at least partially on international cloud platforms, so CNI planning will have to negotiate some border issues.

In the US, some operators have raised concerns that CNI rules may allow local authorities to requisition power from on-site power generation — even behind the meter — to support the electricity grid.

Also, governments may require data centers on the CNI list to comply with specific standards, as would facilities in other CNI sectors.

Operators and enterprises with facilities will need to engage with the government to resolve these and similar issues. They will also need to press for reasonable demands for information and services, as well as make sure that governmental authorities require compliance with appropriate existing standards where possible.

# Can CNI status help the sector?

Despite an explosion of demand, data center operators in different locations are experiencing increasing barriers to new projects. These often take the form of objections to development on green field sites or the use of water. In some case, the project can find it difficult to obtain a connection to the electricity grid.

Some developers are hoping that CNI status will help with these issues, although it is likely that there will be no direct impact on the development of new projects. In most countries, local authorities make the planning decisions.

However, if data centers are locally listed as CNI, the developer will have a case to ask for a review of the decision if a local authority rejects a project by saying that it is “not needed” or “not strategically important.” In the UK, this will not automatically overrule a denied planning application, but it may weigh in the balance.

Governments that assign CNI status to data centers may treat the sector more positively in other ways, perhaps by supporting the development of the necessary skills used to run facilities.

The UK government’s announcement of CNI status for data centers promises another benefit, arguing that the move will “boost business confidence in investing in data centers in the country.” While data centers may not be experiencing a shortage of investment globally — if anything, the reverse is true — the government wants to encourage investors to support the development of data centers in the UK rather than elsewhere.

## The Uptime Intelligence View

Granting data centers with CNI status acknowledges the truth that modern society relies on the

online services they deliver. This will lead to greater involvement in the sector by regulators and officials, with the aim of increasing resiliency. It may also bring more support for some data center projects.

CNI status will require negotiation to address several issues including the status of internal facilities, colocation sites and international cloud platforms. Data center operators should prepare to engage with authorities to ensure that the demands of CNI status are realistic.

## ABOUT THE AUTHOR


### Peter Judge

Peter is a Senior Research Analyst at Uptime Intelligence. His expertise includes sustainability, energy efficiency, power and cooling in data centers. He has been a technology journalist for 30 years and has specialized in data centers for the past 10 years.

**pjudge@uptimeinstitute.com**

## About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions.

With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.