US government agencies have shadow IT infrastructure problem, cybersecurity risks, says GAO

Many US government agency IT facilities are still operating as access points to federal systems without proper oversight and cybersecurity.

Source: https://www.zdnet.com/article/us-government-agencies-have-shadow-it-infrastructure-problem-cybersecurity-risks-says-gao/

Federal agencies are facing increasing cybersecurity risks due to a bevy of IT facilities aren't being tracked as full-fledged data centers, according to a General Accountability Office report.

As noted previously, federal agencies have been consolidating and closing data centers over the years, but a narrower definition of what facilities should fall under an optimization program means that IT infrastructure is falling through the cracks.

In its report, the GAO noted that agencies closed 102 data centers in fiscal 2019 with plans to close 184 more. The catch is that the Office of Management and Budget (OMB) also narrowed the definition of a data center. As a result many facilities are still operating as access points to federal systems without proper oversight and cybersecurity. Here's the OMB's definition of a data center:

A data center generally is a purpose-built, physically separate and dedicated space that contains one or more racks of servers, mainframes, and/or high performance computers; has a dedicated uninterruptable power supply and/or backup generator for prolonged power outages; and/or has a dedicated cooling system or zone. Agencies are to report facilities matching these criteria as tiered data centers.

The issue with that definition? It misses a lot of infrastructure, according to the GAO. Simply put, the US government has a massive shadow IT infrastructure that may be lacking in cybersecurity.

The GAO is recommending that these IT facilities in the US government continue to be tracked. "Each one is a potential target for cyberattacks," said the GAO. The OMB requires 24 agencies to report on data center metrics such as virtualization, energy monitoring and server utilization, but not a count of all servers.

Also:

- AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know
- Survey: Despite new tactics, companies still face challenges implementing cybersecurity measures
- Most common cyberattacks we'll see in 2020, and how to defend against them

From the report:

OMB's June 2019 revised DCOI reporting requirements further changed the definition of a data center, including no longer requiring agencies to report most of the facilities previously categorized as nontiered data centers. As noted previously, OMB directed agencies to stop reporting on spaces not designed to be data centers as part of their inventory. As a result, agencies are no longer required to report on about 2,000 facilities, some of which are considerable in size and will continue to operate. Based on OMB's revised definition of a data center, agencies revised their data center inventory counts and now reported 2,727 operating data centers at the beginning of fiscal year 2019.

According to the GAO, 260 data centers over 1,000 square feet will continue operating, but no longer need to report metrics into the OMB. These facilities aren't counted in the government IT inventory. The Social Security Administration plans to operate 5 data centers that are each more than 8,000 square feet without reporting requirements to the OMB. GAO said:

In July 2019, we found that IT systems supporting federal agencies, such as those found in the government's data centers, are inherently at risk.46 Specifically, we reported that because these systems can be highly complex and dynamic, technologically diverse, and often geographically dispersed, these factors increase the difficulty of protecting their security. Since each physical location represents a potential access point to an agency's interconnection with other internal and external systems and networks, each location also poses a risk as a point of potential attack. We also noted that IT systems are often riddled with security vulnerabilities-both known and unknown.

The GAO has a bevy of recommendations to the OMB and agencies, but the biggest ones revolve around documenting the total inventory of infrastructure as well as decisions about what facilities are counted as mission critical.