Bond Case Briefs

Municipal Finance Law Since 1971

US Agencies Fall Short on Cyber Risk Management, GAO Report Finds.

Several US federal agencies tasked with measuring and assessing cybersecurity standards have neglected duties in this area, a report recently published by the Government Accountability Office (GAO) said.

The report follows a 2013 presidential directive that passed into law in last year's US defense policy bill, handing responsibility for cyber risk management to nine agencies across 16 critical infrastructure sectors. Those agencies include the departments of Agriculture, Defense, Energy, Health and Human Services, Transportation, Treasury and Homeland Security, as well as the Environmental Protection Agency, and the General Services Administration.

Yet, of the 16 critical infrastructure sectors the departments were meant to assess for the adoption of cybersecurity standards, 13 where found to consist of incomplete checks, as reported by Government Executive.

Specifically, GAO said agencies had failed to confirm sectors' compliance with a framework known as the National Institute for Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST). Agencies for nine of the sectors were found not to have taken steps to determine this framework adoption. These sectors included chemical emergency services, healthcare and public health, financial services, commercial facilities, communications, nuclear reactor, materials and waste.

The report took note of the perspective of some of the agencies as to why these duties went unfulfilled.

"Officials from [US Department of Health and Human Services] stated that other priorities, such as the COVID-19 response and managing response planning and recovery from an increase in ransomware attacks, have stretched resources thin and shifted the focus away from determining adoption of the framework," the report said.

Some agencies fared better than others. For example, the Department of Energy had made a start of tracking requests for sector-based cybersecurity toolkits. Despite this however, most agencies did not succeed in tracking and assessing levels of implementation.

Juggling priorities

GAO clarified that the purpose of its report was to respond to the increasing threat of cyber attacks "like the May 2021 ransomware cyberattack on an American oil pipeline system that led to regional gas shortages", adding that such events represent "a significant national security challenge".

It said NIST was launched "to better protect against cyber threats", providing a programme with core security functions and technical safeguards to manage risks of vulnerabilities and intrusions.

Implementation of the NIST standards is voluntary however, which the report cited as another reason some agencies said their assessments fell in priority. Other difficulties they faced included "developing precise measurements of improvement" when measuring adoption.

The report offered recommendations, including that agencies work to "develop metrics to assess the effectiveness of its framework promotion efforts". It said the Department of Homeland Security (DHS) agreed with the recommendation, and had started taking steps to implement it.

Commenting on the measures already taken to improve the rate of assessment, GAO said NIST launched an information security measurement programme in 2020, while the DHS had set up an information network allowing sectors to "share best practices".

GAO also said it had made efforts to encourage agencies to develop methods for determining the level of framework adoption and reporting sector-wide improvements. However, it added: "most agencies have not yet implemented these recommendations".

"Implementing GAO's prior recommendations on framework adoption and improvements are key factors that can lead to sectors pursuing further protection against cybersecurity threats," it said.

globalgovernmentforum.com

By Jack Aldane on 20/02/2022 | Updated on 20/02/2022