

ONE HUNDRED SIXTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

October 9, 2020

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dodaro:

The Department of Health and Human Services (HHS) is the primary agency responsible for protecting public health and providing essential human services, especially for those who are least able to help themselves. The Department works closely with state, local, tribal, and territorial governments to administer more than 300 programs covering a wide spectrum of activities and healthcare services, many of which involve the collection of sensitive data.

HHS relies extensively on information systems and networks to conduct operations, process transactions, account for assets, deliver goods and services to constituents, and communicate with individuals and other organizations. In doing so, HHS information systems collect, process, and maintain highly sensitive information including proprietary business information, public health records, and personally identifiable information. Such information is used to deliver goods and services to beneficiaries of the agency's programs. Thus, a disruption in the information systems owned and operated by HHS could be catastrophic for the many Americans that rely on its goods and services. Given this, it is important that HHS implements protections to secure its information systems and provides ongoing assistance to address emerging cybersecurity threats across the agency.

In addition, as HHS and its component agencies are engaged in the nation's efforts to respond to and recover from the Coronavirus Disease of 2019 (COVID-19) pandemic, the agency has faced an increase in various cyber-based threats to its information systems and data. These incidents and others like them, pose a serious challenge to the agency's ongoing efforts to provide timely services during the COVID-19 pandemic. As such, protecting HHS computing operations during the pandemic response is paramount to the nation's security, economic well-being, and public trust.

The Chief Information Security Officer at HHS recently acknowledged that the ongoing COVID-19 public health crisis has placed a new target on HHS, and malicious actors have boosted their efforts to infiltrate the agency and access sensitive data.¹ In addition, it was reported in March 2020 that HHS suffered a cyber-attack on its computer system. According to people familiar with the incident, it was part of a campaign of disruption and disinformation that was aimed at undermining the response to the coronavirus pandemic and may have been the work of a foreign actor.² Further, emerging cyber threats, such as the advanced persistent threat groups that exploited COVID-19 in early 2020, underscore the importance of effectively protecting information systems supporting the agency.

Given the types of information created, stored, and shared on the information systems owned and operated by HHS, it is important that the agency implement effective incident response handling processes and procedures to address persistent cyber-based threats. Based on the agency's expressed concern and recent past incidents, we would request that the GAO evaluate HHS's incident response capabilities. This should include assessing the agency's forensic threat intelligence data infrastructure used in responding to major or significant incidents involving persistent threats and data breaches.

Thank you for your prompt attention to this request. Please work with Kevin McAloon of the Majority Committee staff at (202) 225-2927 and Alan Slobodin of the Minority Committee staff at (202) 225-3641 on the specifics of your evaluation.

Sincerely,



Frank Pallone, Jr.
Chairman



Greg Walden
Ranking Member



Diana DeGette
Chair
Subcommittee on Oversight
and Investigations



Brett Guthrie
Ranking Member
Subcommittee on Oversight
and Investigations

¹ *Pandemic Advances Cybersecurity Efforts at HHS as Agency Becomes Bigger Target*, CISO Says, Meritalk, (August 19, 2020).

² *Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak*, Bloomberg (March 16, 2020).