The COVID-19 pandemic has increased priorities around health information security, crowdsourced penetration testing and collaboration.

The Department of Health and Human Services has witnessed a significant spike in cyberattacks since the pandemic began, but has also experienced a change in how the agency prioritizes cybersecurity in its pandemic response efforts.
“When it comes to cybersecurity, HHS wasn't thought of as a premier area, and we really enjoyed that type of anonymity in the past — being just a bit under the radar, moving fast, doing a good job. But that's all over,” HHS CISO Janet Vogel said during a Meritalk virtual event last week. “With COVID-19, we are strengthening our program in many ways, every day.”

In the midst of transitioning its employees to mass telework in March due to COVID-19, HHS was hit with a distributed denial-of-service attack. Vogel — who’s served almost 17 years in the federal government, working within various IT departments and CIO shops — said the attack came “very quickly” and “ramped up faster” than anyone could’ve predicted.

“We have employed tools, we have recruited people, and just done about everything you could think of to keep up with the speed of change that we're dealing with,” Vogel said.

The agency has increased its vigilance around safeguarding health information related to the pandemic, which includes valuable intellectual property data, COVID-19 vaccine research and cyber data, which are prime targets for bad actors looking to make a profit off of that data, Vogel said.

But before the pandemic, HHS struggled with changing the culture and attitude around cybersecurity and even viewed it as more of an “inconvenience."

“In the past, we’ve been the office of ‘no’,“ Vogel said, regarding a lack of appropriate cyber workforce investments, training and resources. “One of the biggest challenges is the perception of cybersecurity, so the culture and attitude around security has been very difficult to change — until you hit a pandemic situation.”

The agency has since focused on increasing employee education related to phishing attacks, spam emails and other potential threat vectors, as well as enhancing its cybersecurity outreach programs for remote workers.
For instance, HHS has increased its penetration testing through a bug bounty program to effectively utilize cybersecurity talent and knowledge across the country in identifying potential system vulnerabilities for rewards, which was previously difficult to launch at the agency.

“We implemented a more crowdsourced penetration-testing method to make sure that we can prevent what could happen,” Vogel said.

The agency has completed thousands of hours of external penetration testing, as well, which has equated to “350 full days each year” of remote testing. “That’s very much a part now of our continuous diagnostics mitigation strategy,” she said.

In addition to adopting more remote penetration-testing solutions, HHS has benefited from using machine-learning capabilities for identifying threat patterns and stopping attacks before they begin, and is currently looking into AI for email security.

HHS is also closely working with other federal partners in ways they never had before, such as several security projects related to pandemic cyber activity with the Department of Defense, Vogel said, further noting that "cybersecurity is now a necessity" and that "the perspective of cybersecurity is changing" across the entire health department.