Lamont reshaping digital security

State to focus more on ‘technical expertise’ after key departure

By Stephen Singer

Connecticut’s top cybersecurity official, who played a key role in crafting the state’s approach to digital security, has left his position as Gov. Ned Lamont reworks state policy to focus more on “technical expertise.”

Arthur House, appointed chief cybersecurity officer in 2016 by then-Gov. Dannel P. Malloy, helped shape Connecticut’s initial response to intrusions into computer systems tied to businesses and government agencies. Two years later, officials reported that responses to cyberattacks included a state police cyber crimes unit, a plan to respond to large-scale cybersecurity attacks and Connecticut’s participation in national efforts to protect elections from cyber attacks. He left his job Oct. 11.

Mark Raymond, the state’s chief information officer, said Wednesday he and House “split the cybersecurity baby.”

“I focused on the state of Connecticut security,” he said. “[House] focused on broader, nongovernment entities and businesses. In that role, his expertise was more policy and strategy and less implementation.”

The Lamont administration is looking for someone who will focus on technology and security, Raymond said. A search is underway and a selection will be made as soon as possible, he said.

Lamont praised House, who was his national security adviser in his winning Democratic primary challenge against U.S. Sen. Joe Lieberman in 2006. He called him invaluable and a “great friend.”

House “really got us off to a strong start when it comes to cybersecurity,” the governor said.

Lamont said Administrative Services Commissioner Josh Geballe believes state government needs a cybersecurity expert “with the technical expertise” to ensure “we have a firewall that protects all of our computer systems and then work with the private sector as well,’ Lamont said.

House previously was chairman and one of three commissioners of the state Public Utilities Regulatory Authority. He developed a cybersecurity action plan that identified ways to beef up cybersecurity across the state, specifically in electric, natural gas and water utilities.

He will stay on as a consultant and said cybersecurity for Connecticut and any other entity requires technical competence, strategy and an action plan.

“I’m glad we have an action plan that guides us in the future,” House said. “We also need some policy guidance.”

The state’s cybersecurity action plan is particularly necessary in Connecticut, home to insurance companies and defense contractors with data ranging from personal financial information to military secrets.
A report issued by House earlier this month as he wrapped up his work said phishing and spear phishing — fraudulent emails ostensibly from a known or trusted sender to get individuals to reveal confidential information — “remain prevalent and dangerous, the single most common means to attempt entry” into a company’s systems.

The range of state computer records is immense and touches on nearly every facet of public policy, including taxes, business compliance with environmental and labor laws and regulations, elections procedures and other areas.

Still, Raymond said that with cybersecurity risks evolving, “No one can say for certain that everything is safe.”

Stephen Singer can be reached at ssinger@courant.com.