# Sensitive data from a US anti-terror program was easily available for years, records show

August 27 2019, by Emily Baumgaertner, Los Angeles Times

Credit: CC0 Public Domain

The Department of Homeland Security stored sensitive data from the nation's bioterrorism defense program on an insecure website where it was vulnerable to attacks by hackers for over a decade, according to

government documents reviewed by the Los Angeles Times.

The data included the locations of at least some BioWatch air samplers, which are installed at subway stations and other public locations in more than 30 U.S. cities and are designed to detect anthrax or other airborne biological weapons, Homeland Security officials confirmed. It also included the results of tests for possible pathogens, a list of biological agents that could be detected and response plans that would be put in place in the event of an attack.

The information—housed on a .org website run by a private contractor—has been moved behind a secure federal government firewall, and the website was shut down in May. But Homeland Security officials acknowledge they do not know whether hackers ever gained access to the data.

Internal Homeland Security emails and other documents show the issue set off a bitter clash within the department over whether keeping the information on the .org website posed a threat to national security. A former BioWatch security manager filed a whistleblower complaint alleging he was targeted for retaliation after criticizing the program's lax security.

The website shared information among local, state and federal officials. It was easily identifiable through online search engines, but a username and password were required to access sensitive data.

A security audit completed in January 2017 found "critical" and "high risk" vulnerabilities, including weak encryption that made the website "extremely prone" to online attacks. The audit concluded that there "does not seem to be any protective monitoring of the site," according to a Homeland Security report summarizing the findings.

An inspector general's report published later that year said sensitive information had been housed on the BioWatch portal since 2007 and was vulnerable to hackers. The report recommended moving the data behind the government's firewall and said Homeland Security officials had agreed to do so.

It is unclear how valuable the data would have been to a terrorist group or enemy state. Scientists have warned that the BioWatch technology is unreliable. The system recognizes only a narrow range of microbes, and it struggles to differentiate between typical environmental bacteria and dangerous threats.

Still, several biodefense experts said it was disturbing that Homeland Security officials failed to adequately secure sensitive information from one of the nation's anti-terrorism programs.

"Advertising your vulnerabilities is never a good thing. Letting your adversaries readily access your vulnerabilities—that's a national security risk, in my judgment," said Tom Ridge, who as the nation's first Secretary of Homeland Security oversaw the 2003 launch of BioWatch but has since denounced the program as ineffective. "Every American citizen would wonder, 'What else is so easily accessible by the rest of the world?'"

James F. McDonnell, an assistant secretary appointed by President Donald Trump to oversee Homeland Security's new Countering Weapons of Mass Destruction Office, which includes BioWatch, said the data that was housed outside the secure government firewall was not important enough to cause a national security threat, but he said officials have taken steps to strengthen cybersecurity across the department. He noted that the problem predated his appointment.

"What happened before, happened before. You can't put the genie back

in the bottle," he said. "There's been a real ramping up on concerns about cybersecurity."

—-

The security problems add to a long list of troubles for BioWatch.

The program, which has cost taxpayers more than $1.6 billion, was launched two years after letters laced with anthrax spores killed five people and sickened 17 others shortly after the Sept. 11, 2001, terrorist attacks. BioWatch became part of Homeland Security's Office of Health Affairs in 2007.

A 2012 Times investigation identified serious shortcomings, including false alarms and doubts about whether BioWatch could be relied on to identify a bioterrorism event. In 2015, a Government Accountability Office study concluded that the program could not be counted on to detect an attack and said BioWatch generated 149 false alarms from 2003 through 2014.

Each day, public health workers across the country collect filters from the air samplers and run tests on the contents, searching for signs of dangerous pathogens in the air. In some cases, reports of suspicious lab findings are uploaded to the BioWatch portal for review by other officials.

Some local officials objected to storing these and other sensitive documents on a federal server that other government officials could access without their knowledge or consent, according to the inspector general's report. As a result, the report said, the Office of Health Affairs decided against moving the portal inside the Department of Homeland Security's firewall.

—-

In August 2016, Harry Jackson, who worked for a branch of Homeland Security that deals with information security, was assigned to the BioWatch program. Three months later, he said in an interview with The Times, he learned about biowatchportal.org and demanded the agency stop using it, arguing that it housed classified information and that the portal's security measures were inadequate.

Two other department officials tasked with monitoring how sensitive information is handled echoed the concerns in emails to BioWatch managers, according to records reviewed by The Times.

BioWatch officials pushed back. Michael Walter, the program's manager, said in a conference call with other Homeland Security officials that information about the location of the network's air samplers would not undermine its effectiveness since it was designed to detect a massive biological warfare attack. The samplers are in plain sight, he said, according to a recording of the call made by Jackson and reviewed by The Times.

Larry "Dave" Fluty, then Health Affairs' principal deputy assistant secretary, argued during the same call that the agency had previously decided that treating the information as classified—and therefore triggering stricter access guidelines—would require security clearances for some 1,000 local officials who are involved in gathering and analyzing data from the air-collection units.

"It was determined from a policy standpoint that that can't happen," he said.

Weeks after the conference call, Steven Lynch, then chief of Homeland Security's special security programs division, wrote in a memo reviewed

by The Times that the agency planned to move the portal onto a .gov site behind the secure federal firewall. Still, he said, experts concluded there was "no evidence of criminal or suspicious activity" involving the .org portal and "minimal to no risk of unauthorized access."

But a complaint made to the inspector general hotline had already triggered an internal audit of biowatchportal.org.

The audit turned up 41 vulnerabilities, and a scan detected a possible attempt by a hacker to access the portal. The auditing team was unable to validate the scan's finding, and the team recommended that the contractor overseeing the site investigate. It is unclear whether that was done.

The contractor, Logistics Management Institute, declined to provide a comment. Walter, Fluty and Lynch did not respond to emails or phone calls from The Times.

—-

In January 2017, Jackson published his concerns about the portal in the Journal of Bioterrorism & Biodefense. His article detailed what he called "negligent" security that required only single-factor authentication to access the website.

Department of Homeland Security officials removed BioWatch from Jackson's portfolio, then suspended his security clearance and later placed him on administrative leave. They notified him that he had not sought the proper approval to publish his article and that it included information that should not have been made public. They also cited his recent conviction for drunken driving.

Jackson filed whistleblower complaints with several federal agencies,

alleging he was the victim of retaliation for criticizing the program's security. In one, he wrote that a successful hacker could "monitor the system, manipulate data, and create false flags so as to stake out federal, state and local response to a possible incident."

The complaint continued: "To this date, DHS will never know the harm that has resulted from this because there is no intrusion detection capability."

The inspector general's report published later that year said no classified information was found on the BioWatch portal, but it confirmed that "critical and high risk vulnerabilities" could allow an attacker to access sensitive information on the site.

In October 2017, Homeland Security reinstated Jackson's security clearance but issued him a warning. A letter notifying him of the decision did not address his whistleblower claim. He left the agency a few weeks later.

No federal agency agreed to investigate Jackson's complaints. In May, he filed an appeal with the Office of the Intelligence Community Inspector General. He is awaiting a response.