



Department of Health and Social Services Cyberattack Frequently Asked Questions August 4, 2021

The Department of Health and Social Services (DHSS) recognizes there are many questions that have not been answered about this cyberattack. Due to the nature of the situation, many factors must be considered before information is released publicly. This includes protecting the processes being used to counter the attack and the sensitive nature of the ongoing investigation. DHSS is working closely with our security partners and the state Office of Information Technology (OIT) to ensure our systems are securely restored and to protect Alaskans' personal data. We thank Alaskans for their patience as we continue to progress through the investigation, restoration and after-action review.

Q: How is the department responding to this attack?

A: DHSS is using the National Institute of Standards and Technology (NIST) Risk Management Framework's Computer Security Incident Handling Guide ([Special Publication 800-61 rev2](#)), which includes three main steps:

1. **Detection and analysis:** Determining what was attacked and how. This phase has been completed.
2. **Containment, eradication and recovery:** Significant progress has been made in removing the attacker from DHSS systems and we have no evidence of the attacker being active in our environment at this time. Recovery work continues to build back resilient systems and restoring services. A firm timeline on full restoration of services is not yet known as the Information Technology Incident Response Team is developing and implementing new processes and technologies to provide more secure and resilient services.
3. **Post-incident activity:** Strengthening people, processes and tools so that all information technology services are more resilient to cyberattack. Recommendations for future security enhancements and any additional funding needs will be provided to Commissioner Crum.

Q: When was the attack first discovered?

A: First signs of a potential attack were identified on May 2, 2021 at which time the State Security Office and DHSS immediately started investigating to identify and isolate any affected systems, applications and accounts to contain the threat. The incident was also immediately reported to law enforcement. DHSS subsequently retained FireEye, a leading cybersecurity firm that provides incident response consulting services through Mandiant, to help conduct an in-depth investigation of the incident.

By May 17, 2021 the investigation revealed a server that supported the operation of the DHSS website was compromised. The website was taken offline to prevent further disruption and harm to servers, systems and data. The public was then notified of the attack and disruption of services via social media on May 17 and a press release on May 18. Subsequent updates on the progress of the investigation have been provided in press releases on June 7 and August 4.

Q: Who or what attacked Alaska?

A: FireEye has identified those behind the attack as a highly sophisticated group known to conduct complex cyberattacks against organizations that include state governments and health care entities. DHSS is focused on responding to and recovering from the attack and will not comment on the identity of the group due to the ongoing investigation or speculate about their intentions.

Q: Are they still attacking DHSS?

A: Currently there is no evidence of continued attacks against DHSS. Right now, DHSS continues to work through the recovery process. Cyberattacks occur across the world every day and we know that this specific attacker could return. In collaboration with our partners, the DHSS IT Incident Response Team is taking a systemic approach to strengthen our people, processes, and technology and we are developing more robust incident response capabilities to respond more swiftly to cyberattacks in the future.

Q: Why did they attack Alaska?

A: DHSS is focused on responding to and recovering from the attack and will not speculate on the intentions of the attackers.

Q: What was attacked inside DHSS?

A: At this time, due to pending investigations, details on the nature and scope of this attack will not be released.

Q: Was personal health information compromised?

A: At this time, Mandiant has thoroughly examined the department's technology infrastructure and has currently found no evidence that Alaskans' protected health information or personally identifiable information has been stolen. However, this is still a dynamic situation, and all systems are continuing to be monitored. If at any time DHSS becomes aware of compromised protected health information or personally identifiable information, the department will notify partners, vendors and individuals who were directly affected by the attack.

Q: Was the cyberattack a ransomware attack?

A: At this time, there is no indication of this being a ransomware attack, however this is still a dynamic situation, and all systems are continuing to be monitored.

Q: How did the cyberthreat group gain access to the system?

A: The cyberthreat group exploited a vulnerable website and spread from there. Providing any further specific details could give our attackers information that would help them, and others, be more successful in future cyberattacks.

Q: Has DHSS removed the attacker from the department's systems?

A: DHSS continues to work through the recovery process. We have no evidence of the attackers being active in our environment at this time, however we continue to address potential risks as part of a thorough response conducted in partnership with Mandiant, the State Security Office and law

enforcement. There is real concern that this group will come back to try again, so we continue to make our environment more resilient while monitoring our systems for new threats.

Q: Do you have a timeline for when online services will be restored?

A: There is still no timeline for when all services that are currently offline will be back online. The large size of the department's IT infrastructure and complexity of the data and systems used by the department requires a careful, meticulous approach that will take more time to make our services more resilient and get them back online.

Q: Are background checks still being conducted?

A: The Health Care Services (HCS) Division is continuing to conduct background checks through manual processing and review. Depending on circumstances, the process could take up to 15 days but at this time are typically being handled in 2-3 days. That could change if the volume increases. Larger health care providers with multiple requests can notify the Background Check Unit they will be sending their applications in batches along with appropriate payment for bulk processing. To help keep turnaround times low, HCS has brought on additional staff, authorized overtime, and is diverting all calls to a live person, whenever possible. When call lines are full, customers are called back within hours. See this temporary webpage for more information about the interim background check process and to download forms: dhss.alaska.gov/dhcs/.

Q: Are requests for vital records, such as birth, death and marriage certificates, still being processed?

A: With access to the system restored on July 26, the Health Analytics and Vital Records Section (HAVRS) has been transitioning back to automated processes and addressing the backlog of work created by the outage. Both the Juneau and Anchorage Vital Records Offices have restored most of their certificate services, with a few limitations in place so staff can focus on processing the backlog orders. There is no timeline for how long it will take to eliminate the backlog, but this task is a priority for HAVRS and staffing has been adjusted to work through the process as quickly as possible. More details about limitations and current capabilities at HAVRS are posted online at dhss.alaska.gov/dph/vitalstats/pages/.

Q: Where can I find information about a DHSS service or program while the website is unavailable?

A: For phone assistance during business hours (8 a.m. - 4:30 p.m.), please contact the department at 907-269-7800 or [download this detailed list of contacts](#) for divisions, sections and programs. Many divisions have temporary webpages available with their most critical information and forms at dhss.alaska.gov.

Q: Where can I find information about COVID-19 while the website is unavailable?

A: For questions specific to COVID-19, the COVID-19 vaccine helpline is available at 907-646-3322 from 9 a.m. - 6:30 p.m. on weekdays, and 9 a.m. - 4:30 p.m. on weekends. You may also email covid19vaccine@alaska.gov for help or visit the temporary COVID-19 section of the DHSS website at dhss.alaska.gov/dph/epi/id/pages/COVID-19/default.aspx.

Q: Has DHSS contracted with any cybersecurity companies because of this cyberattack?

A: Yes, DHSS retained FireEye, a leading cybersecurity firm that provides consulting services through Mandiant, to help conduct an in-depth investigation of the incident.

Q: What work did they provide to DHSS?

A: Mandiant provided incident response services to assist us with detection and analysis, as well as containment, eradication and improving our resilience to cyberattack.

Q: How much have you spent on the cyberattack?

A: The DHSS contract with FireEye and Mandiant is \$459,500. It is not known at this time how many total Department of Health and Social Services staff hours have been spent working on this cyberattack.

Q: What is the department doing to prevent any further attacks?

A: As systems are being brought back online, steps are being taken to build them back to be as resilient as possible to be protected from future cyberattacks. Also, as part of the overall response to the attack, an after-action review will be conducted in coordination with trusted cybersecurity partners. Recommendations for future security enhancements and any additional funding needs will be provided.

Q: Is this related to any other cyberattacks either in Alaska or outside of Alaska?

A: DHSS is coordinating its efforts with the state Office of Information Technology, which can comment on what other actions are being taken at the state level.

Q: Have any other state systems outside of DHSS been compromised?

A: DHSS is coordinating its efforts with OIT, which can comment on what other actions are being taken at the state level.

###