Department of Health and Social Services

2021 Cyberattack: Frequently Asked Questions

Updated Sept. 16, 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, after-action review, and becoming more resilience to future cyberattacks.

A Health Insurance Portability and Accountability Act (HIPAA) and the Alaska Personal Information Protection Act (APIPA) breach notification was announced on Sept. 16, 2021, notifying all Alaskans about the potential of health and personal information being compromised as a result of the cyberattack. More information about the breach and actions concerned Alaskans can take to protect themselves against identify theft can be found below in Q&As 7-9 below and at dhss.alaska.gov.

Q1: How is the department responding to this attack?

A1: 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 restore 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.

Q2: When was the attack first discovered?

A2: First signs of a potential attack were identified on May 2, 2021, through proactive surveillance, by a security monitoring firm which then notified the State Security Office. DHSS was subsequently notified on May 5 and 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 then 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. A HIPAA and APIPA breach notification, along with a press release, was announced on Sept. 16, 2021, notifying Alaskans about the potential of health and personal information being compromised as a result of the cyberattack.

Q3: Who or what attacked Alaska?

A3: 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.

Q4: Are they still attacking DHSS?

A4: 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.

Q5: Why did they attack Alaska?

A5: DHSS is focused on responding to and recovering from the attack and will not speculate on the intentions of the attackers.

Q6: What was attacked inside DHSS?

A6: At this time, due to a law enforcement investigation, details on the nature and scope of this attack will not be released. Providing any further specific details could give our attackers information that would help them, and others, be more successful in future cyberattacks.

Q7: Was personal health information compromised?

A7: Mandiant thoroughly examined the department's technology infrastructure and found no evidence that Alaskans' protected health information or personally identifiable information has been stolen. However, given the capabilities of the nation-state sponsored attacker and the scope of access they had to the department's infrastructure, we cannot be assured there is a low probability that protected health information was compromised, and therefore, in accordance with HIPAA and APIPA, we are notifying Alaskans their health or personal information may have been compromised. On Sept. 16, 2021, DHSS posted a breach notification to its website and issued a press release to media outlets statewide notifying the public about the breach of data.

Q8: What type of data was compromised?

A8: The attackers potentially had access to the following types of individuals' information:

- Full names
- Dates of birth
- Social Security numbers
- Addresses
- Telephone numbers
- Driver's license numbers
- Internal identifying numbers (case reports, protected service reports, Medicaid, etc.)
- Health information
- Financial information
- Historical information concerning individuals' interaction with DHSS

DHSS does not have information about exactly what information could have been compromised or who specifically might be impacted which is why all Alaskans are being notified. To help provide context for what types of data may be stored on DHSS computer systems, consider the wide variety of services the department provides, including, but not limited to: Medicaid coverage; birth, marriage, divorce and death certificates; vaccine records; diseases or conditions mandated to be reported to the State; reports of child or adult harm; or records for individuals involved with the juvenile justice system or Pioneer Homes.

Q9: What can Alaskans do if they think their private information is at risk?

A9: Free credit monitoring is being made available to any concerned Alaskan as a result of this breach. More information about the breach, including the breach notification statement and frequently asked questions, are available at dhss.alaska.gov. On Tuesday, Sept. 21, 2021, a toll-free hotline will be available (5 a.m. to 5 p.m. Alaska time) to answer questions and assist people with signing up for the free credit monitoring service. That phone number and the website for the credit monitoring service will be provided on the DHSS website at dhss.alaska.gov.

Between Sept. 27 and Oct. 1, 2021, email notices will be sent to all Alaskans who have applied for a Permanent Fund Dividend which will include a code they can use to sign up for the credit monitoring service. People who don't receive a code will need to contact the toll-free hotline for assistance. Questions may also be directed to DHSS at 1-888-484-9355 or PrivacyOfficial@alaska.gov, however the sign-up process for the credit monitoring service will need to go through the toll-free hotline available Sept. 21.

Q10: Was the cyberattack a ransomware attack?

A10: There is no indication of this being a ransomware attack.

Q11: How did the nation-state sponsored attacker gain access to the system?

A11: The nation-state sponsored attacker 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.

Q12: Has DHSS removed the attacker from the department's systems?

A12: 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.

Q13: Do you have a timeline for when online services will be restored?

A13: Some services have been restored. 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 has required a careful, meticulous approach that takes time to make our services more resilient and get them back online.

Q14: Are background checks still being conducted?

A14: 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. 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. Visit the HCS temporary webpage for more information about the interim background check process and to download forms.

Q15: Are requests for vital records, such as birth, death and marriage certificates, still being processed?

A15: With access to the Electronic Vital Records System restored on July 26 and the online ordering system, VitalChek, restored on Sept. 8, 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. For all types of orders, there continues to be a longer than normal delay due to the backlog of requests. Please expect up to two months from the time the order is placed. More details about limitations and current capabilities at HAVRS are posted online at dhss.alaska.gov/dph/vitalstats/pages/default.aspx.

Q16: Where can I find information about a DHSS service or program while the website is unavailable?

A16: 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.

Q17: Where can I find information about COVID-19 while the website is unavailable?

A17: 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 COVID-19 section of the DHSS website at dhss.alaska.gov/dph/epi/id/pages/COVID-19/default.aspx.

Q18: Has DHSS contracted with any cybersecurity companies because of this cyberattack?

A18: Yes, DHSS retained FireEye, a leading cybersecurity firm that provides consulting services through Mandiant, to help conduct an in-depth investigation of the incident.

Q19: What work did they provide to DHSS?

A19: Mandiant provided incident response services to assist us with detection and analysis, as well as containment, eradication and improving our resilience to cyberattack.

Q20: How much have you spent on the cyberattack?

A20: 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.

Q21: What is the department doing to prevent any further attacks?

A21: 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. Additional steps are being planned for post-incident hardening of our IT infrastructure. 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.

Q22: Is this related to any other cyberattacks either in Alaska or outside of Alaska?

A22: 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.

Q23: Have any other state systems outside of DHSS been compromised?

A23: DHSS is coordinating its efforts with OIT, which can comment on what other actions are being taken at the state level.

# # #