AFFIDAVIT OF WILLIAM J. SMITH, JR.

STATE OF ALASKA)
) ss.
THIRD JUDICIAL DISTRICT)

William J. Smith, Jr., being first duly sworn upon oath, deposes and says:

1. Since November 18, 2019, I have been the Chief Information Officer (CIO) in the Office of Information Technology (OIT). Under Administrative Order 284 (AO284), dated April 25, 2017, OIT is housed in the Alaska Department of Administration (DOA).

2. I have reviewed and consulted with Treston Grady, OIT's Acting Chief Information Security Officer, on OIT's 2018 Annual Cybersecurity Report (OIT Report). Bill Vajda, my predecessor, prepared it in 2018 with assistance from then-Deputy CIO Dan DeBartolo, then-Chief Information Security Officer Shannon Lawson, then-Chief Technology Officer Ryan Mitchell-Colgan, then Chief Staff and Finance Officer Benjamin Shier, and then-Communications Manager Catherine Hatch.

3. I have also reviewed and consulted with Mr. Grady on the draft July 26, 2021, Intrusion Investigation Report (Mandiant Report) that Mandiant (i.e., FireEye, Inc., doing business as "Mandiant") prepared for the Alaska Department of Health and Social Services (DHSS). Mandiant is a cybersecurity company.

4. The OIT Report is 22 pages and includes 10 appendices, totaling another 181 pages. Every page of the 22-page report is marked "Confidential Deliberative Process Executive Privilege."

5. The OIT Report has been shared only on a need-to-know basis with persons inside OIT, the Office of the Governor, the Alaska Department of Administration, and the Alaska Department of Law.

6. The OIT Report was prepared pursuant to AO284 to advise the Governor "on executive branch agency compliance with information technology security and protection requirements with a summary of evaluations, an assessment of the development, adoption of, and compliance with, information technology standards, identification of any deficiencies, and plan for remedying the deficiencies." Accordingly, the OIT Report (a) provides the Governor a summary and evaluation of executive branch information technology (IT) plans, programs, and procedures and (b) recommends measures—e.g., statutory changes and specific investments—the Governor can take to strengthen the executive branch's IT security. It also identifies potential funding sources.

7. Disclosing the OIT Report would reveal opinions and recommendations of a close advisor of the Governor. Disclosing the report would also adversely affect my and my successors' ability to advise the Governor on the security of the executive branch's IT. This would occur because disclosing the information would reveal vulnerabilities in the executive branch's IT security—e.g., by revealing previous security incident details —thereby increasing the likelihood that the State of Alaska (State) would be successfully attacked. This would also occur because of the concern that the public would wrongly second-guess preliminary and final opinions and recommendations of the Governor's advisers.

8. A successful cyber-attack could result in the following: (a) interference with the implementation or enforcement of IT security plans, programs, and procedures, resulting in, e.g., the violation of Alaskans' and others' rights, the loss or destruction of property, and substantial interference with vital state activities; (b) the disclosure of confidential guidelines for investigations or enforcement, risking circumvention of the law; and (c) the endangerment of life or physical safety and a substantial risk to public health and welfare.

9. Mandiant owns the 37-page Mandiant Report and its 12 appendices, totaling another 28 pages. Every page with text is marked "MANDIANT PROPRIETARY AND CONFIDENTIAL." The Mandiant Report includes a 2.5-page Executive Summary that is a version of a 5-page draft Intrusion Investigation Executive Summary, dated June 24, 2021: the June 2021 executive summary contains about 2.3 pages of text; and the July 2021 executive summary principally adds some detail and corrects some numbers.

10. The Mandiant Report has been shared only on a need-to-know basis with persons inside OIT, DHSS, DOA, the Office of the Governor, the Alaska Department of LAW, and the U.S. Department of Justice (specifically, the Federal Bureau of Investigation or FBI).

11. The Mandiant Report was prepared as part of an in-depth investigation of a cyberattack involving a DHSS website server. The State detected the attack in May 2021.

12. The Mandiant Report details attacker attribution, the period and scope of the intrusion, the potentially exposed information, how much data the attacker transferred from the DHSS network, how much data the attacker transferred into the DHSS network, how the attacker undertook the attack, and immediate actions to prevent future attacks. The report includes information to help the State develop incident containment and attacker eradication plans.

13. DHSS has made public information about the cyberattack that is the subject of the Mandiant Report: e.g.,

a. http://dhss.alaska.gov/News/Documents/press/2021/DHSS_FAQs_FMS_Cyberattack-PR3_20210804.pdf;
b. http://dhss.alaska.gov/News/Documents/press/2021/DHSS_PressRelease_FMS_CyberattackUpdate_20210804.pdf;
c. https://content.govdelivery.com/attachments/AKDHSS/2021/06/07/file_attachments/1847116/DHSS_FMS_CyberattackUpdate_20210607.pdf; and
d. https://content.govdelivery.com/attachments/AKDHSS/2021/05/18/file_attachments/1812446/DHSS_FMS_WebsiteAttack_20210518.pdf.

14. Unlike the information DHSS disclosed, releasing the Mandiant Report would reveal (a) vulnerabilities in DHSS's and other state agencies' IT security and (b) information about how the State prevents, detects, contains, and investigates attacks. Disclosing this information would increase the likelihood that DHSS and those other agencies are successfully attacked, and such attacks could lead to the same kinds of consequences (detailed above) that would occur because of a cyberattack resulting from the disclosure of the OIT Report.

15. In addition, the Alaska Department of Law, and the FBI—as well as OIT—urge the State not to release the Mandiant Report. They have significant concerns over publicly releasing the specific details and descriptions of network locations, device IP addresses, specific code related to indications of compromise, the techniques the attackers employed, and the methods the State Security Office used to detect and contain the attack. There is a reasonable expectation that disclosing these details would provide the attackers (given their technological sophistication) and others valuable intelligence that could be exploited in the future to, for example, evade detection and being tracked.

16. The Mandiant Report is classified as "proprietary and confidential" in its entirety. The report and the other deliverables resulting from the incident response are the intellectual property of Mandiant. They contain detailed information describing and from which can be derived Mandiant's methods of investigation, technical capabilities, and analytical processes. These details represent sensitive commercial information.

17. The benefit to the public from the disclosure of the OIT Report or the Mandiant Report would be to better understand the executive branch's IT systems and infrastructure. This benefit does not outweigh the harms to the public and the State that disclosing either report would entail by revealing vulnerabilities in those systems and infrastructure and, in the case of the Mandiant Report, by also interfering with an ongoing law enforcement proceeding and making contracting with Mandiant and other cybersecurity firms more difficult, if not impossible. Releasing the reports could result in the theft or deletion of privacy-protected, financial, confidential business, confidential law enforcement, and other protected information and in damages to state agencies' IT systems and infrastructure, irreparably harming thousands of Alaskans and others and catastrophically impairing operations of the State.

William J. Smith, Jr.

SUBSCRIBED AND SWORN TO before me this 28 day of September, 2020.

NORTARY PUBLIC in and for Alaska

My Commission Expires: With office

State of Alaska
NOTARY PUBLIC
Kelley N. Roberson
My Commission Expires With Office