STACEY MARZ
Administrative Director

Alaska Court System

303 K STREET
ANCHORAGE, ALASKA
99501

(907) 264-0548
FAX (907) 264-0881

August 18, 2021

Mr. Nat Herz
Alaska Public Media/Alaska Public Radio Network
Via email: nherz@alaskapublic.org

Re: Appeal of Denial of Court Records

Dear Mr. Herz:

This responds to your emailed appeal of the court system's June 23, 2021 denial of your request for contracts and other documentation "that the court system has entered into for cybersecurity-related or other IT services since the April 29 discovery of the cyberattack" on the court system. I have reviewed your original request, the denial, and your appeal, as well as contracts and other documents in the court system's possession that might be deemed encompassed by your request. Unfortunately, we are unable to produce any documents to you, because all information that we have is confidential or otherwise not subject to disclosure. I therefore must deny your appeal.

I. Administrative Rule 37.5(e) makes these documents inaccessible.

As explained in Ms. Rabinowitz' initial denial, the court's Administrative Rules govern disclosure of records in the court's possession, including the administrative records that your request seeks. Under Administrative Rule 37.5(e)(2)(D), the documents you have described are not accessible to the public, because the information could jeopardize the integrity of the court's information technology or recordkeeping systems.

The documents that are covered by your request reveal the steps that the court took to respond to and counter the attack, including the company/companies with whom the court contracted, the scope of services for which the court contracted, how rapidly the court in fact reacted, how much money the court expended to react, the specific steps taken and changes to the overall systems and to individual accounts that may have been made to repel any additional attacks, and numerous other responsive measures that the court undertook.

As you may imagine with a cyberattack of this magnitude, the court system considers the

intrusion to be criminal in nature, and has consulted law enforcement entities for guidance. Those law enforcement experts have advised the court system not to disclose any of the facts mentioned above. The attackers are advantaged when they have information about what a target of a cybersecurity attack has done in response, thus increasing the risk not only to that target for ongoing attacks, but also to other potential targets who may share related systems. Disclosing even, for example, the names of the companies with whom we may have consulted or contracted, or the amount of funds that the court may have expended in its response efforts, would arm the attackers with information that could be used to undermine the new security measures that we took, and would inform them of the dollars that we may have been willing to pay to counter the attack and to minimize the potential for another attack. According to law enforcement entities who are most familiar with these attacks, all information the attackers learn about a target's response weakens the target and strengthens the probability of another incident occurring, thus jeopardizing the integrity of the court's IT system (and the State of Alaska's IT system as a whole).

Your appeal specifically notes that you'd expect that the records at issue could be redacted to remove specific details of the court's cybersecurity plans, infrastructure, and shortcomings, but still be produced with the more general sections that describe areas where the state's cybersecurity infrastructure could use improvement or require additional resources. Again, however, even revealing what companies were engaged, or what general steps were taken, or what vulnerabilities were patched, or how quickly the court reacted would increase the likelihood of additional attacks, thus threatening the ongoing security of the court's systems.

II. Withholding the documents comports with the underlying purposes of the court's public access rules.

As you point out, Administrative Rule 37.5(e)(2)(D) does not incorporate any balancing test in its description of which administrative records are inaccessible to the public. The fact that the court's IT systems could be jeopardized by disclosure is, by itself, grounds for denial. I will add though, that my conclusion is supported by the overall purposes of the court's public access rules as expressed in Administrative Rule 37.5(a)(1). That subsection lists the goals of providing public access – and many of those goals would be undermined by disclosure of the records you seek. Specifically, disclosing these documents would not support but could instead destabilize the role of the judiciary (see AR (a)(1)(B)), would not contribute to but instead would jeopardize public safety (see AR (a)(1)(D)), would not minimize but instead could increase the risk to individuals (see AR (a)(1)(E)), would not protect but instead could compromise proprietary business information (see AR (a)(1)(G)), and could indeed unduly burden the ongoing business of the judiciary (see AR (a)(1)(K)). This is not an exhaustive list of the potential ways that disclosing the information you want could be harmful and undermine the court's mission, but I'm hopeful that it does illustrate the very severe consequences that could flow from disclosure.

III. The public records act does not apply, but these documents would be exempt from disclosure even under that act.

You mention an exception to the state's public records act and your assumption that at least some information in those documents should be provided because it "could not reasonably interfere with

implementation or enforcement of security plans or disclose confidential guidelines for investigations and risk circumvention of the law." The judicial branch is not covered by the public records act in Title 40 (except for the statutes addressing personal information that are not at issue
here), so that argument does not directly inform this response. Nevertheless, I will reiterate that even disclosing boilerplate terms of a contract or dates or costs of certain court actions could indeed be informative to those who conducted the attack and could indeed disclose confidential guidelines and increase the risk for further circumventions of the law by those who conduct cyberattacks. So even by that standard, these records may not be made public.

Further, to the extent that parallels maybe drawn to the public records act even though it does not govern the court's documents, I would point specifically to certain exceptions in that act that support my conclusion. Namely, AS 40.25.120(a) exempts from disclosure records or information compiled for law enforcement purposes if the disclosure could reasonably be expected to interfere with enforcement proceedings, or would disclose confidential techniques and procedures for law enforcement investigations or prosecutions. Since law enforcement is currently investigating the cyberattack on the court system and investigators have cautioned the court not to discuss or disclose information relating to its responses, the exceptions to disclosure in the act, though not directly apt, provide additional support to deny your appeal.

The court system is proud to provide public access to its case records and administrative records in as reasonable a manner as possible, consistent with its rules. We strive to respond quickly and thoroughly to document requests from the public, and are generally reluctant to deny access, at least to some redacted or scaled-down information to help a person who is requesting documents. Nonetheless, because of the unique nature of the cyberattack, and the tremendous risk of additional attacks that can come from providing even small amounts of information concerning a target's responses, this is an instance where the court must deny access.

Sincerely,

Stacey Marz
Administrative Director

cc (via email): Mara Rabinowitz, Communications Counsel
Nancy Meade, General Counsel