North Orange County Community College District

April 13, 2023

***VIA EMAIL***

Amy Parker

apark0006@student.cerritos.edu

**Re: Response to April 3, 2023 Public Records Act Request**

Dear Ms. Parker

This letter shall serve as the North Orange Community College District’s (“District”) response to your requests to Fullerton College and Cypress College, pursuant to the California Public Records Act (“CPRA”), for all the services/protocols, ports, and categories of domains which have outbound traffic from the Fullerton College or Cypress College network blocked and or monitored/logged[[1]](#footnote-1).

Please be advised that the CPRA does not require that public agencies produce records within 10 days of receiving a public records request. Rather, Government Code section 7922.535(a) requires public agencies to respond to public records requests within 10 days by indicating whether the request seeks copies of disclosable public records and when those records can reasonably be made available.

Additionally, while Government Code section 7922.525 provides you a general right to inspect public documents, it does not provide you the right to show up unannounced at a public agency’s office and immediately inspect whatever you desire. Regardless of the method used to submit a public records request, the District will determine when the records can be made available to you.

**District Response**

The District has determined that your request seeks, in part, records disclosable under the CPRA. As you may know, the CPRA does not require the District to create records; the District’s obligation under the CPRA is limited to producing existing records. (*Haynie v. Superior Court* (2001) 26 Cal.4th 1061, 1075.)

Your request seeks three discrete categories of information. For the sake of clarity, the District’s response is divided by type of information sought.

**Request No. 1: A list of all services/protocols that have outbound traffic blocked logged or monitored from the Cypress or Fullerton College networks.**

The District does have records responsive to your request, but they are not disclosable public records. The District is permitted by Government Code section 7922 to withhold records when the public interest in disclosure is clearly outweighed by the public interest served by not disclosing the record. Here, the public interest in non-disclosure is significant. The District expends significant resources ensuring the proper use and security of its systems. Your request is limited to outbound traffic, but that does not mitigate the risk caused by the disclosure of all services/protocols that have traffic blocked, logged or monitored. One of the common Tactics, Techniques, and Procedures (TTPs) that actors do after the initial breach is to set Command and Control (C2) communications via outbound traffic back to a server controlled by the attacker. If the information you requested was disclosed, it would provide attackers with a list of services and protocols to avoid when attempting to remove data from district networks. This is not merely a hypothetical concern. Approximately once a month, the District thwarts an attack that is attempting to steal confidential personal information stored on District servers.

The public interest in disclosure of the full list of services or protocols that have outbound traffic blocked, logged or monitored is minimal. It is public knowledge that the District manages its IT systems, and restricts access to certain computing resources when they pose a security risk. For example, see Cypress College's Computing Resources Acceptable Use Policy. This publicly posted policy provides that Cypress College has the right to limit, restrict, or deny access to any and all computing resources as the individual situation may require. Providing a list of every service or protocol that is blocked, logged, or monitored would only serve to provide bad actors with a list of systems to avoid.

The District is aware of your work studying how Cerritos College manages its network, and wants to be as helpful as possible without compromising District security. The District cannot provide you the documents you request, as doing so would pose an unacceptably high risk to District information security. However, the District is aware that the treatment of SSH traffic is of concern to you. The District can tell you that it does not categorically block outbound SSH traffic. Occasionally, specific security issues arise that require the District to block elements of SSH. When that concern is resolved, the block is removed.

**Request No. 2: All ports which have outbound traffic blocked, logged or monitored from the Cypress College or Fullerton College networks.**

The District does have records responsive to your request, but they are not disclosable public records. The District is permitted by Government Code section 7922 to withhold records when the public interest in disclosure is clearly outweighed by the public interest served by not disclosing the record. Here, the public interest in non-disclosure is significant. The District expends significant resources ensuring the proper use and security of its systems. Disclosing all the ports that have outbound traffic blocked, logged or monitored would be the equivalent of publicly broadcasting which door you leave unlocked each time you left your house.

In your correspondence with the District, you indicated that you did not see a security risk in disclosing this information because it could be obtained by any student with a port knocker. This is technically true, but it ignores important context. In order to run a port knocker, the person would need to physically come to campus, log on to the network with a login connected to their student or employee identification, and remain on campus while the port knocker proceeded to run. Requiring these steps imposes significant costs and risks on potential bad actors, and gives the District time to respond to someone who is on their network running a port knocker. If this information was publicly disclosed, the District would lose the ability to impose those costs on a potential bad actor. Instead, the District would have to treat every person who logged on to their system as if they already knew all of this information. This would greatly increase the District’s security costs and inhibit student and employee use of the District’s systems.

**Request No. 3: All categories of domains that have outbound traffic blocked, logged or monitored from the Cypress College or Fullerton College networks.**

**Response to Request No. 3:** The District does not block, log or monitor categories of domains. The District’s firewall blocks individual malicious domains that pose a risk to the District’s information security. The list of blocked domains is based on threat intelligence from third party vendors, and proprietary characteristics determined by the District’s firewall vendor. None of those characteristics are based on the information or opinions that are hosted on a particular domain. The list of blocked domains is updated daily.

In response to your request, the District will provide you with the block list as it existed yesterday, April 12, 2023. The District reasonably anticipates being able to provide you this information within seven days.

In accordance with Government Code section 7922.540, subdivision (b), the individual responsible for the denial of any portion of your request is Kai Stearns, District Director, Public and Governmental Affairs.

Sincerely,

Kai Stearns

NOCCCD District Director, Public and Governmental Affairs

1. On April 3, 2023, you submitted a Public Records Request for all services/protocols, ports, and categories of domains which have outbound traffic from the Fullerton College network blocked and or monitored/logged. On April 5, 2023, you submitted a request for the same information from Cypress College. In your April 5 request, you indicated that you would accept one response to your requests if the District’s responses would be identical. The District’s responses would be identical, so the District will only be providing one response to your requests. [↑](#footnote-ref-1)