

# INFORMATION TECHNOLOGY

## A REPORT ON THE DEPARTMENT OF EQUITY AND DIVERSITY'S INVESTIGATIONS

---

<b>Chapter 1 - The Events and History</b>	<b>3</b>
Introduction	3
Early Context	4
First Contact	5
Problems, People, and Plagiarism	6
Student Services and Dr. Robyn Brammer	8
The Office of Business Services	8
Looping in ASCC - Part I	9
Meeting with VP/AS Lopez	9
The Intervention (or lack thereof)	10
A Temporary End	11
The First Public Records Act Request	12
December 5, 2022	12
The California Public Records Act	14
Looping in ASCC - Part II	19
<b>Chapter 2 - Technical Analysis and Explanations</b>	<b>20</b>
Introduction	20
Internet Control Message Protocol (ICMP)	20
Secure Shell (SSH)	22
Network Holes	24
<b>Chapter 3 - College Policy (BPs and APs)</b>	<b>27</b>
Introduction	27
Due Process	27
BP and AP 3720	29
BP 3720	29
AP 3720 - Preamble	30
Privileges and Responsibilities	31
Individual User Rights	31
Appropriate Uses of District Computer Resources, Prohibited Uses of College Computer Resources, and Unauthorized Use/Failure to Follow Procedures	32
Additional Guidelines	32
Disclosure	33

---

---

BP and AP 3050	34
Introduction	34
BP 3050	34
AP 3050	34
California Public Records Act (BP and AP 3300)	39
<b>Chapter 4 - Statements and Opinions</b>	<b>42</b>
<b>Chapter 5 - Summary and Recommendations</b>	<b>46</b>
Summary	46
Recommendations	46
<b>Appendix A: Real-World Example Usage of ICMP</b>	<b>48</b>
<b>Appendix B: December 5 Document</b>	<b>49</b>
<b>Appendix C: VPN Testing</b>	<b>54</b>
<b>Appendix D: PRA #3 Response (Direct Falsehoods)</b>	<b>55</b>
<b>Appendix E: Final Update, January 17-18</b>	<b>56</b>
<b>Attributions</b>	<b>58</b>
<b>Certificate of Affirmation</b>	<b>59</b>

---

# Chapter 1 - The Events and History

## Introduction

Over approximately the past year, I have been advocating for greater freedom for students, faculty members, and administrators on the Cerritos College network. This network is controlled by the Department of Information Technology, headed by Director Patrick O'Donnell. The Department is subservient to the Office of Business Services, headed by Vice President/Assistant Superintendent Felipe Lopez. My efforts initially began by trying to get the Secure Shell protocol, more commonly known as SSH, unblocked for outbound traffic on the network; it is vital for many utilities employed by various types of students, and especially computer science/Computer Information Systems students. Over the past several months, I have uncovered a long line of unethical and potentially illegal behavior perpetrated by the Department, including unethical spying on students, restriction and censorship of information, a disregard for California state law and college policy, and an abandonment of the college's ethics policy as well as the position's dedication to supporting the needs and education of students. This has been aided by actions of the Department of Business Services, who have obfuscated information and been an accomplice in many of the obstructive actions perpetrated by the Department. Given the lack of forward progress and transparency<sup>1</sup> on these

---

<sup>1</sup> In the spirit of transparency, I will openly provide copies of all emails related to this investigation by request. Contact me at [apark0006@student.cerritos.edu](mailto:apark0006@student.cerritos.edu) regarding this. In general: what the Department finds, they desire to keep private; what I find, I desire to keep public.

---

issues, I have no option but to report what Equity and Diversity has uncovered thus far in terms of its investigation into these behaviors.

## **Early Context**

Last year, I first discovered that SSH was not usable on the Cerritos College network. This didn't make any sense, and was a significant detriment to me completing my work while at the college; I kept a lot of my coursework and notes on my home file server at the time, which I accessed using SCP, which runs over SSH. I also wanted to keep code I wrote on GitHub, an online code-sharing and repository platform; however, code is uploaded to it via SSH, making yet another thing which can't be done on the Cerritos College network due to current restrictions. This irked me; while I could still access what I needed through usage of a mobile hotspot, this was cumbersome, and an option not available to most of Cerritos College. It also didn't help when I was just trying to use the college's network in a normal fashion; I had to fully circumvent the network, making it unusable as a direct resource.<sup>2</sup>

I also later found out that many other protocols and websites were blocked on the network. Many types of Internet Control Message Protocol (ICMP) requests were being eaten, including the ubiquitous Echo Request (type 8) - known more commonly as a "ping". It also appears that other vital message types, such as type 3

---

<sup>2</sup> A VPN would be another alternative for circumvention, albeit one not usable by most of the student population due to technical inexpertise or a lack of funds to purchase access to a public one/set up a private one. This most directly impacts the students who need the college's network the most. IT could've provided a VPN for circumventing the network, but the time for them to actually provide that has long lapsed. It also doesn't solve the fundamental problem, only creating a stopgap solution. Further, see Appendix C for more information.

---

(Destination Unreachable), may be blocked. There is a notable exception for subdomains on second-level domain “cerritos.edu”; requests to these do not appear to have their Echo Requests consumed. Further technical investigation also demonstrated that these requests were *not* blocked for intranetwork traffic, but rather only outbound requests coming from within the network.

## **First Contact**

I had tried to contact the Department several times previously regarding this issue, as well as other issues (such as a major discovered security vulnerability within PeopleSoft), but I never got any responses. On September 8, 2022 at 5:35 PM, I sent in a HelpDesk ticket named “Errors with SSH” in which I outlined that SSH and ICMP were unreasonably blocked. This was finally able to receive the first response of any communications I had attempted with IT previously, when Director O’Donnell responded to the ticket on September 9 at 10:32 AM. He gave an extremely un-descriptive response, immediately closing the ticket after:

“The College security policy does not allow this type of access. So you will not be able to do any of these items.”

I attempted to respond twice, once on the same day at 1:09 PM and again on September 14 at 7:34 PM, asking for information on who set the ambiguously-referred-to “security policy” for more information. This received no responses; while I can only speculate, I believe that they were not received due to the ticket being so rapidly closed.

---

## Problems, People, and Plagiarism

After other unsuccessful attempts at communication, on October 12, 2022 at 9:28 PM, I sent Director O'Donnell a direct email asking to discuss the policies which led to SSH continuing to be blocked on the network. He responded the next morning at 8:48 AM. As it turns out, the aforementioned "network policy" truly was a vague, blank check; he said that the "network policy is to keep the campus safe from all outside and inside security threats." To justify why this means SSH should be blocked, he then said that the Department "only open[s] necessary ports for instruction and operations." This is, of course, not a real explanation; for one, the college network is expressly usable for purposes not directly related to college-provided instruction (AP 3720)<sup>3</sup>; also, the block on SSH is protocol-based, not port-based (the network detects that a packet is an SSH packet and blocks it, not just blocking traffic on the standard SSH port 22). He then further claimed that "[o]pening access to outside server[s] is not allowed as it could be a security threat to [the Cerritos College] network." Of course, this is not directly true either. Allowing outbound traffic is the express point of the network; it itself does not make the network vulnerable. Having inbound SSH access could be a potential (albeit rare) threat, but no one was asking for that; only outbound access was requested.

He further continued his explanation by listing "reasons not to allow SSH." This list was borderline comedic. Presented as his own justification, a quick Google search

---

<sup>3</sup> [https://www.cerritos.edu/board/\\_includes/docs/AP/AP\\_3720.pdf](https://www.cerritos.edu/board/_includes/docs/AP/AP_3720.pdf)

---

reveals that the list was actually stolen from an article<sup>4</sup> by Venafi, a server identity management corporation. Further, this article is not actually about outbound SSH! It exclusively refers to security risks posed by servers accepting inbound SSH connections. It also is not recommending to “not use SSH” even within that context, but rather how to secure machines with SSH servers. The fact that the Director was unable to even double-check that his copied explanation was relevant to the matter at hand is extremely concerning; that should be part of the bare minimum when responding to a concern by a student.

At this point, I was still assuming good faith on the Director’s part, but that he was just mistaken in some sort of rush. I clarified that I was referring to outbound traffic, and then listed explanations of how each point in the copied explanation was not relevant to the situation. I also drew connections to how, on the parts of some explanations which may have been relevant, the college would already be experiencing those categories of vulnerabilities anyways - the ones applicable also would’ve been present in standard Web traffic, which is not *entirely* (more on that later) blocked by the college. I sent this response on October 13 at 9:45 AM. From this point forward, Dean of Student Services Elizabeth Miller was included in most applicable conversations. I received no response until I sent a follow-up CC’ing Dean Miller back in; this became a pattern, where emails passing through the Department would not receive secondary responses unless Dean Miller was CC’ed.

---

<sup>4</sup> <https://www.venafi.com/blog/what-are-most-common-ssh-security-risks>

---

He simply responded that, as he “said in the past” (while this may have been true, there are no records indicating such, and I have no memory of such), I should “work with [my] instructor[(s)] to talk about these items,” and that “[w]e will not be making these changes you requested.” This completely ignored all of my responses to the points he gave; if the justification he gave was solid, wouldn’t he have been able to respond to my responses?

## **Student Services and Dr. Robyn Brammer**

The newly appointed Vice President/Assistant Superintendent of Student Services, Dr. Robyn Brammer, attended the ASCC Cabinet meeting on October 17 to discuss the purchase of a new student life application. Prior to the meeting, I intended to contact her to get another level 2 (VP/AS level) administrator’s perspective on the issue; after being informed by Dean Miller that she had decent technical knowledge, I decided to speak with her before she left during the meeting. She was equally perplexed as to why SSH was blocked, and affirmed the viability of my intentions to speak to the superior of Director O’Donnell - Vice President/Assistant Superintendent of Business Services Felipe Lopez. She also informed me that she herself was having similar issues; a tool needed in the Office of Student Services required SSH access, and she was thus unable to use the tool.

## **The Office of Business Services**

On October 18 at 2:19 PM, I sent an email outlining what had occurred thus far with the Department to VP/AS Lopez. I included as much detail as possible in this email,



---

providing indication of the effective nonresponse I had received from the Director. To demonstrate that this was not just a student issue, I included the issues Dr. Brammer was facing. One would think that a student issue would be enough for an administrator to take action, but Cerritos College has consistently demonstrated that the most effective way to get things to change is when administrators themselves are concerned; student needs, and often even faculty needs, are disregarded. Thankfully, he responded quickly (same day at 2:56 PM), and offered to have his secretary Linda Kaufman schedule a meeting between him and I. Due to scheduling conflicts, this meeting ended up being scheduled for November 7 at 4:00 PM following the conclusion of that day's ASCC Cabinet meeting.

## **Looping in ASCC - Part I**

On October 24, I gave a report during the ASCC Cabinet meeting regarding what had happened up to this point. I intended to give this report during the October 17 meeting, but was unfortunately unable to; however, due to the delays, I was able to include the scheduling of the Business Services meeting in my report. I detailed how I had been trying to cooperate with the Department on the issue, but was consistently getting stonewalled. I also mentioned the reasons why the escalation had to occur.

## **Meeting with VP/AS Lopez**

After some minimal discussion with other members of ASCC in the meantime, November 7 finally came. Raining down hard, I made it to the Cabinet meeting; it

---

concluded, and I made my way over to the Office of Business Services. After a long wait for the meeting to be able to begin, I finally met VP/AS Lopez in person. I presented my case regarding the blocking issue; I detailed everything, from how Director O'Donnell continually disregarded my emails and the interest of the students, to the technological explanation behind why SSH should be accessible over the college network, and finally the needs administrators like VP/AS Dr. Brammer had. He did listen, and seemed to care about the student concern about the issue. Little did I know, however, that would be the end of all true cooperation between the Department of Business Services and the student body.

## **The Intervention (or lack thereof)**

On November 19, at 5:28 PM (12 days after the meeting), I sent an email to VP/AS Lopez asking for updates on the situation at that point. He had sent me nothing - no follow-ups, no progress updates. ASCC as a whole also received no information. November 22, at 3:19 PM (15 days after the meeting), I sent another follow-up email. This one finally received a response (the next day, at 8:13 AM) - a response which drastically shifted my perspective on the state of Cerritos College administration. VP/AS Lopez had completely cut ASCC out of all discussions on the matter, providing us no updates, ability to be a part of discussion panels, or ASCC tech-knowledgeable leaders a chance to present their case. The decision was made entirely behind closed doors, with contributions from the college's insurance

---

carrier, the “cyber and security consultant”, and “staff”.<sup>5</sup> There was no follow-up, no back-and-forth, just a simple “investigation” with no traces or presented evidence - and a presented conclusion of inaction. The response was condescending to a minimal degree; not as condescending as responses from Director O’Donnell, but still not showing a full degree of respect for the concerns presented.

## **A Temporary End**

Now, up to this point, all of this was about SSH and ICMP. I care very strongly about these being unblocked; I even planned to integrate the issue as part of my future Secure Communications Act. However, it seemed as if the amount it was taking to fight was too much for such a small issue as SSH. While I absolutely could have escalated it further at that point - potentially the President, or even the Board of Trustees - it wasn’t worth it for such a small, marginal issue. I’m normally not one to quit on issues, as I believe that every little thing that someone gets away with within a position of power forms a brewing ground for more problematic behavior later on; however, I was almost ready to admit defeat. I had a meeting scheduled with Student Trustee Hector Ledesma (December 2, 4:15 PM), as we had several items to talk about; I brought this up in my meeting with him. He agreed - the most that would be reasonable would be a mention in passing to the President, given how marginal of an issue it was. Without a reasonable way to do that, I largely let the

---

<sup>5</sup> It should be noted that the names of the staff and the insurance carrier were not provided in the emails. This is not uncommon as many organizations do hide who they discuss with in situations like these, but it is important to note as it still breaks standards of transparency and is contextually relevant given that student government was cut out of the conversation.

---

investigation die out. I kept my efforts barely alive, but they fell significantly and were quickly petering out.

## **The First Public Records Act Request**

After my meeting with Student Trustee Ledesma, I sent a request under the California Public Records Act, codified as Government Code sections 6250-6270, requesting a list of the services, protocols, domains, and ports that were blocked for outbound traffic from the network. This request was sent directly to Director O'Donnell on December 2 at 7:32 PM. I made clear that it was for public benefit in my request. I received no response from Director O'Donnell at all; receiving any response came long after a series of events which changed the nature and scope of the investigation entirely.

## **December 5, 2022**

December 5 was the last meeting day for the ASCC Cabinet. It was a pro forma session; we met at the library instead of in Auto Partners, and quickly ended the meeting so that we could celebrate and de-stress for finals. Members of multiple branches all came in to enjoy the festivities. Several administrators and other staff members also passed by to enjoy what was to be seen. I was able to speak to several of them. This included Stephanie Rosenblatt, the Library's Reference and Instruction Coordinator. She explained to me the struggles the Library had been having with the Department, how resources they and students needed to access were often blocked. She had run into many of the same issues with nonresponse,

---

condescending responses when provided, and disregard for student needs that I had. This is when she dropped the bombshell that fully reopened my investigation. She was in receipt of a document - definitively a public record - from the Department, dated and received October 2021, stating categories of websites that were either allowed fully, monitored/logged, or blocked. This occurred at approximately 3:10 PM. She further clarified a harrowing fact about the document: it stated that the Department was logging information about which users were visiting certain categories of sites, including religion and abortion.

I was absolutely shocked to hear this. There was absolutely no possible way to justify this. Given the nature of web traffic, at minimum they were logging the domains of websites visited under these categories; that's enough to determine if someone's looking into a religion, or is a member of a religion, or is seeking out/planning to get an abortion. I requested the document, sending an email at 3:11 PM; she promised to get the document back to me, and was able to retrieve it and send it to me the next day at 12:40 PM.

In the meantime, I decided to visit the Department's office. It's very much hidden away in an unmarked corner of the Social Sciences Building; VP Gomez had to help guide me to it. I had two potential objectives: to speak in person with Director O'Donnell (if possible), and to potentially browse records myself (permitted under the California Public Records Act; any member of the public is allowed to walk in at

---

any time and browse records). I asked his secretary, Vikki Stevens, if he was in a meeting, and if not whether I could speak to him. She responded flippantly with “who’s asking?” and then proceeded to conduct an interrogatory about why I was there. She confirmed that I would not be able to meet him directly, responding with a statement of the Director’s inherent superiority over students, and shut down my requests. I did not make the request to browse records<sup>6</sup>, due to the level of intimidation present; however, I did make sure to ask her to have the Director verify receipt of the Public Records Act request (which never occurred).

Due to the ASCC social events of the day, I was able to loop in some of the members of ASCC to the live action. I spoke briefly to President Naqvi, albeit many of the factors listed in this report were not fully communicated. My in-person interactions with the IT office were witnessed directly by VP Gomez. I also communicated heavily about this with Dean Miller, who I have continued to follow up with.

## **The California Public Records Act**

Before I continue, I should clarify what the California Public Records Act is. Passed in 1968 and signed by then-California Governor Ronald Reagan, the Act, sometimes referred to as the CPRA or PRA, requires, except under some limited circumstances, that public agencies disclose governmental records and documents - including

---

<sup>6</sup> While true, I have now since met with the Department in person and provided a request to search records. For details, please view Appendix E.

---

communications, except for attorney work-product *in preparation for a lawsuit* and where otherwise exempted. It is currently located in the California Government Code as sections 6250-6270. It was further enshrined into our state's Constitution by the "Sunshine Amendment," which outlined the general right the Act provides through Proposition 59 in 2004. It is similar to the federal Freedom of Information Act, but actually goes much further and protects the rights of independent activists (FOIA allows agencies to charge for document searches, but this is generally not allowed under CPRA).

Cerritos College handles CPRA requests through its guidelines in BP 3300 and AP 3300.<sup>7</sup> These are surprisingly thin, likely owing to the lack of common handling of CPRA requests. They do not contain many of the important rights the CPRA provides, such as the right to have a recommendation on how to narrow/adjust the search to actually match relevant records in the case the search does not provide any disclosable records (as long as there is no section 6254 exception). While requests are officially designated to be handled by the President's office, the designee allowance tends to lead requests to be handled by level 2 officials. In my case, I submitted my requests generally to the Director, who is a level 3 official, but my responses all came from VP/AS Lopez who is level 2 as stated previously.

---

<sup>7</sup> [https://www.cerritos.edu/board/\\_includes/docs/AP/AP\\_3300.pdf](https://www.cerritos.edu/board/_includes/docs/AP/AP_3300.pdf)

---

In none of my requests have I received responses back from the Director himself. Granted, only one request sent directly to him has lapsed in its allowed time period (stated under CPRA and AP 3300 as ten days, not ten business or instructional days). In total, I have sent three requests. The first one has already been mentioned, and will be covered shortly; the second was sent to the Office of Business Services, intended target VP/AS Lopez, through his assistant (the aforementioned Linda Kaufman). It was sent on December 4 at 7:31 PM. The third request, again sent to the Director, was sent January 2, 2023; as of writing this report, it has not received a response (timestamped January 5 at 9:13 PM)<sup>8</sup>. It directly asked for categories of websites which were blocked/monitored/allowed, attempting to see if the Department or the Office would acknowledge the existence of the categories system and of the December 5 document, or if it would outright reject the concept and thus attempt to obstruct further.

On both of the first requests, I sent follow-ups before the responses were sent back. I received both responses through VP/AS Lopez, who opted to provide a PDF-based letter instead of an email. The first response was received 7 days after the CPRA submission on December 9, 2022 at 4:02 PM. VP/AS Lopez responded by denying this request, using a 6255 exemption by claiming that providing information about service, port, and website blocking (to *any* degree, clarified later) would pose a security threat to the network and thus the public's interest was to

---

<sup>8</sup> This is no longer the case; for more critical evidence regarding the conduct and behavior of the Department and the Office, see Appendix D, which covers the Office's response to PRA #3.



---

withhold the records. This denial is incorrect on the facts from multiple angles. A list of blocked domains, or even categories of domains, poses no threat to the college. A list of blocked ports would only be a problem if there was absolute incompetence in the cybersecurity handling of the network such to expose an easily exploitable vulnerability; such information could be directly figured out by any student with a minimal amount of time on their hands by using a port knocking tool. The way the response was written also appears to be copy-pasted from an anonymized source without credit, as it refers to the network in the abstract (“a public agency’s IT system”). It also links to the AUP, BP 3720, and AP 3720, none of which are relevant to a *public records request*.

At 4:47 PM, I followed up with a request to use the aforementioned narrowing right in the CPRA; I proceeded to follow up on December 12 at 11:23 AM, and on December 18 at 8:19 AM. I received a response finally on December 19 at 3:39 PM, which merely restated the original point and denied the narrowing request on the grounds that no other applicable records existed. This denial provides multiple pieces of evidence of illegal behavior. To begin with, the re-referencing of the AUP is not a relevant record, rather a misdirection. To claim there are *absolutely no applicable records* is also absurd, when one could easily think of anything such as a previous reference to emails transiting the office about SSH being blocked. The real level of illegal behavior, though, presents itself when the December 5 document is considered. It is definitively a public record, as defined by the CPRA. Its existence

---

was known by the Department, as it generated said document, which would thus imply that the category listings are also public record. The fact that not even the December 5 document was disclosed indicates that there is an intentional avoidance of providing records; there is no way good faith could be present here with such high levels of obfuscation and obstruction.

The second request concerned contacts and communication involved in the review of whether SSH and ICMP remained blocked. This request was also denied (9 days after sending, December 13 at 10:20 AM) on the basis that there were no such records. There are only two possibilities that could generate such a result. One, that there were absolutely no communications which occurred in the discussion apart from oral communications with no scheduling. I find this extremely unlikely, and it should also match my original emails about the request. Given that VP/AS Lopez mentioned speaking to the insurance carrier - an industry which tends to document such conversations for later reference, where not doing so leaves massive potential for liability - this is an extremely unlikely scenario. It would also imply, in a workplace culture where everything is discussed by email or by email-scheduled meeting, that all conversations (including with the Director and with VP/AS Dr. Brammer) were held orally with no scheduling, unless they never occurred (contradicting promises made previously, and also implying falsehoods presented in the response email). There is only one other possibility: there were conversations that were not admitted to. If there were conversations covered by exceptions, the

---

requirement would be to state that there were applicable records but that they could not be disclosed under an exception. But no, operative words were used here - “the District does not have any records that meet your request.” I then asked directly for clarification: “Were all conversations then held in-person with no documentation of the discussions or any justifications from each side?” (December 13, 10:27 AM). He ignored the question and instead said “there are no records that meet your request” (December 19, 3:30 PM). Given the near impossibility of the first option, illegal behavior likely occurred here; and if the first option occurred, deceptive behavior had taken place, with an intentional obstruction of a student investigation. Either way, the Office’s conduct on this matter was unacceptable.

## **Looping in ASCC - Part II**

As of January 6, 2023, I have not received a response back to CPRA request #3.<sup>9</sup> At this point in the report, I am currently working on setting up a group of high-level ASCC members to discuss this; these discussions will occur before this report is delivered, albeit likely before it is finalized. The challenge now lies with ASCC to take action, and with individual representatives to ensure accountability is upheld now and in the future.

---

<sup>9</sup> This is no longer the case as of January 10; see Appendix D, which contains the response to PRA #3. That response contains a lot of important additional evidence regarding the conduct of the Office and the Department.

---

## Chapter 2 - Technical Analysis and Explanations

### Introduction

This section is not immediately relevant for most. It simply contains technical explanations - as verbosely described as possible, to leave no room for ambiguity or deniability. It also does not relate to the investigation as a whole, but rather to the reasons specific technical-related denials are invalid. If such information is not important, interesting, or relevant to you, it would be wise to skip this chapter and move onto Chapter 3; please refer to the pages guide at the front of this report.

### Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol, also known as ICMP, is a protocol that is used by computers to communicate status information about packets being transmitted. Essentially, it allows computers to detect and manage errors in the transmission of packets across a network. It runs on top of the Internet Protocol, allowing it to use IP's resources; because there are two main versions of IP, IPv4 and IPv6, there are also two versions of ICMP (ICMP for IPv4 and ICMPv6). However, given that almost all network traffic is still done over IPv4, ICMP for IPv4 is the important focus.

The protocol defines a list of "control messages" that computers can use to indicate certain types of statuses and requests over a network. The most famous one is code 8, the "Echo Request" (and its sister type, code 0, the "Echo Reply"). Whenever

---

you “ping” a device to check if it is online/measure latency, your device actually sends out an Echo Request, and the intended target sends back an Echo Reply. All IP-compliant devices - thus, all devices on the Internet for the most part - support this, as ICMP is a key internet standard (as published by the Internet Engineering Task Force).<sup>10</sup> The Echo Request has thus become a key tool for internet communication and the proper functioning of applications and services.

As mentioned previously, however, Cerritos College blocks many types of ICMP requests, including the Echo Request and Echo Reply. Now, why does it do this? There is an excellent explanation provided by the technical team at ShouldIBlockICMP.com,<sup>11</sup> which advocates for reasonable security methods while also supporting compliance with IETF RFCs. It does acknowledge that there are some security concerns with certain parts of ICMP, especially when they are implemented incorrectly; the standard is large, and some unused parts have been previously exploitable. However, it also clarifies parts of ICMP that are not vulnerable and should not be blocked; this includes the Echo Request and Echo Reply system, as they have no vulnerabilities.

This leaves no reason on the surface for ICMP to be *entirely* blocked. But what are the downfalls? Well, many programs use ICMP to determine how to operate, especially in terms of client/server communications. An application may ping

---

<sup>10</sup> <https://www.rfc-editor.org/rfc/rfc792>

<sup>11</sup> <http://shouldiblockicmp.com/>

---

servers to determine which one to use. These applications are unusable on the Cerritos College network. Someone developing their own application would have to create a proprietary equivalent to the pinging system; this of course doesn't work when a student just wants to use an existing application, and also highlights the absurdity of blocking the entirety of ICMP. This becomes a general theme; many of these blocks can be circumvented. So who is affected? **Normal** students. Those who can't afford or don't have the technology or technological knowledge to circumvent these absurd policies, are thus subjected to them. This is not just a freedom issue, or a privacy issue, or a civil rights issue, it is an equity issue.

## Secure Shell (SSH)

SSH was what started this whole investigation; it itself deserves an investigation as to whether it poses any threat to the college network. SSH itself is just a general protocol for operating services in a secure manner. The most common usages of it, however, are for file transfer (over SCP/SFTP/RSYNC, which avoid the problems of FTP and other insecure file transfer protocols) and for remote logins to computers. If TeamViewer and AnyDesk are usable, both of which do have many security problems, why is SSH blocked?

Ironically, SSH is actually one of the most secure ways to handle most protocols. There have been very few vulnerabilities in even implementations of the protocol - and almost nothing in the protocol itself. The "vulnerabilities in the protocol" usually refer to improper encryption types, which are not the defaults in almost every

---

well-recognized and commonly used SSH software. The OpenSSH implementation by the OpenBSD project, the most commonly used implementation, has only occasional vulnerabilities which require absurdly rare setups and user error to exploit.<sup>12</sup> This is in comparison to the myriads of vulnerabilities in software and web systems which Cerritos College students use on their computers on a daily basis, and which is even already present on Cerritos College systems. There is no reason for SSH to be blocked.

In fact, there appears to be only one reason the Department would even want to stop SSH from being used: stopping tunneling. A commonly supported utility, SSH tunneling is when traffic over certain ports is re-routed through another server, transported and encrypted via SSH. This allows for an effective proxy or VPN effect depending on the particular setup and usage. Many networks<sup>13</sup> try to stop VPNs from being used on them (for outgoing traffic); this doesn't make any sense, of course, as there is no network security reason to block VPNs for outgoing traffic. (This contrasts with incoming traffic, where blocking VPNs is a reasonable mitigation against many types of attacks where IP addresses would be blocked upon confirmation of suspicious activity). The reason that VPNs are blocked for outgoing traffic is simple: a desire to spy on and control traffic. If the network is provided as a simple public service for students to use, there would be no desire to do this; blocking VPNs is a method of controlling what students can see. It is an act

---

<sup>12</sup> <https://www.openssh.com/security.html>

<sup>13</sup> See Appendix C.

---

of censorship and of espionage, implemented by the most authoritarian of governments - and also, on occasion, by power-hungry educational institutions which seek to control what their users can do.

James F from ServerFault has outlined that SSH itself has no risk. There is one other potential risk that he outlines: problems with reverse tunneling.<sup>14</sup> This is where a user with internal access creates a reverse tunnel via SSH to allow an outside attacker access to the network. There are some flaws with this logic in the context of the college, though. For one, since the network has public access, anyone could come and do the attack themselves; the attacker may as well just run the attack from their device. Shutting off that device from the network would still have the same effect as the attack needs to be run through the device. A dedicated attacker could also just implement a proprietary protocol which is not blocked by the network (could even run CNC over HTTP); thus, SSH presents no vulnerability to the network that does not already exist through other means.

## **Network Holes**

This explanation concerns the first CPRA request. VP/AS Lopez outlined that the reason for denial was that the records “includes [sic] information regarding the District’s cybersecurity systems, infrastructure and mechanical control systems, or information that would reveal vulnerabilities to, or otherwise increase the potential for an attack on” the college’s network. This implies that providing ANY information

---

<sup>14</sup> <https://serverfault.com/a/25566>



---

about blocked services, protocols, ports, and domains, to ANY extent, would threaten the network. This is simply false. I will group these explanations into three categories: services/protocols, ports, and domains.

First is services/protocols. These are somewhat easy to test for a dedicated investigator. All it takes is to get a list of commonly used protocols, set them up on a foreign server, and test them. It is better to test them across a variety of ports, including known good ports (like 80, the port for HTTP), to remove the effects of port blocking from the results. Does this test for all possible services? Of course not, but it would reveal at least some relevant ones which are allowed or blocked by the college. There is thus no reason to deny the information; revealing it does not create any threat which is not already known.

Second is port scanning. This is even easier to do. There are many open source port knocking tools available, which with a single, once-configured server, allow for testing the entire span of TCP and UDP ports (1-65535, 0 if you count IANA's "reserved" port as usable and all systems in the chain support it) in a short amount of time. These tools are so simple that anyone can create them; for instance, if I ever were to continue this investigation with a port knock, I would likely use this<sup>15</sup> scanner which is free and open-source on GitHub. Because of this being able to be easily done, a list of available ports does not provide a threat. It also doesn't

---

<sup>15</sup> <https://github.com/TotallyMonica/port-knocker>. Note: this tool was not made by me, although I have contributed minorly to its documentation. It was made by someone in a similar situation who was investigating a similar condition at their college.

---

provide a threat inherently; what is vulnerable is not the list of allowed/blocked ports, but rather the services running through them.

Lastly is domains. This one is even sillier to decline. Individual domains are testable by anyone with a simple web browser or CLI toolkit. A batch of known acceptable domains could be tested rapidly through an automated script. There is also no vulnerability present from what domains are actually blocked; domain names themselves have no inherent vulnerabilities (this should not be confused with vulnerabilities in the wider DNS system which are irrelevant to this discussion).

---

## Chapter 3 - College Policy (BPs and APs)

### Introduction

This section covers various college policies applicable to this situation. In addition to the Computer and Network Use Policy (BP/AP 3720, previously referenced and cited), it also covers various standards of conduct, including BP/AP 3050 (“Institutional Code of Ethics”) as well as the right to due process. Information on due process rights also requires examining applicable state and federal law, as well as court precedent, and thus those are included within the limited reasonable scope in this chapter.

### Due Process

The Constitution guarantees all those within the United States (interpretable as citizens or as all people, depending on one’s contextual reading) the right to due process of law: from the first section of the Fourteenth Amendment, “No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law”.<sup>16</sup> This section has been interpreted by courts to have the word “state” mean “any governing body,” which would include Cerritos College. State Constitution Article 1 section 7(a) also states that “[a] person may not

---

<sup>16</sup> <https://www.law.cornell.edu/constitution/amendmentxiv>

---

be deprived of life, liberty, or property without due process of law".<sup>17</sup> This applies to all governing bodies within the state.

Cerritos College does acknowledge this from *within AP 3720*, stating that "[a]n authorized user is entitled to due process rights as described in Board Policies, Administrative Procedures and collective bargaining agreements." (lines 81-82) Of note, I can not find any other Board Policies or Administrative Procedures which describe due process rights, although there may be others that invoke them. Either way, this is an admission that due process does apply to the network.

Most implementations of due process require public hearings, at minimum upon challenge, of all policies that infringe the rights of those which the policy applies to. In this case, the freedom being fringed is the accessibility of certain services such as ICMP and SSH, as well as the logging of information as described in the December 5 document. I directly challenged these to the Office of Business Services, but the investigations were not based on due process. Instead, they completely cut student governance out of the equation, and hid the details of it. While this can be a somewhat regular, albeit poor occurrence, it is unacceptable that no information about the process was provided in the response to CPRA #2 (and not just that it was not provided, but that its existence was denied). This is not national security information protecting the country from an imminent attack, this is students trying

---

<sup>17</sup> [https://leginfo.legislature.ca.gov/faces/codes\\_displayText.xhtml?lawCode=CONS&article=1](https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&article=1)

---

to use the resources at their disposal to further their education in a context where the provided justification does not actually support the concept of increased attack threats.

In rejecting the CPRA requests, and by cutting out the student voice from decisions on protocol blocking, the Department and the Office, led by VP/AS Lopez and Director O'Donnell, have violated the due process rights of students in an absolutely absurd manner. There is no transparency here; there are only intentional actions which curb the rights of students and which shatter the protective glass of transparency into our public institutions, replacing them with an opaque set of theoretically immovable bricks. Of course, no object is ever truly immovable; change can occur, but only once these violations are realized by the public.

## **BP and AP 3720**

Given the importance of BP/AP 3720, and how commonly they are referenced by the Department and the Office (as well as VP/AS Lopez himself), we must review what these actually are, and what effects they have; whether they are built equitably and with the students' needs in mind, or built to create a state of control over the content students can access to serve the interests of the administrators over the students.

### **BP 3720<sup>18</sup>**

---

<sup>18</sup> [https://www.cerritos.edu/board/\\_includes/docs/BP/BP\\_3720.pdf](https://www.cerritos.edu/board/_includes/docs/BP/BP_3720.pdf)

---

BP 3720 merely establishes/provides for the existence of AP 3720. This is the standard setup with Cerritos College Board Policies. However, there is a key bit of information here which is important to keep in mind: "Employees and students who use District computers and networks and the information they contain, and related resources have a responsibility ... to respect the rights of others" (9-11). As will be demonstrated, and which the evidence for has already been listed, the Department and the Office have not been respecting the rights of others, in particular students using the network.

### **AP 3720 - Preamble**

AP 3720 will be looked at by section, as it is a long document (10 pages). Congruent irrelevant sections may be combined, but sections with content will be left for independent analyses and review. The Preamble summarizes the document, with the main priority being to outline that it is a violation of policy to interfere with or misuse the network. There is a strange section (lines 13-15), which states that "It is considered a violation of District policy to use the District's network and/or Internet access in such a way that it interferes with or is incompatible with the user's performance, duties, or responsibilities." The former of these prohibitions - interference with personal performance - is likely where the prohibition on gaming over the network is derived from. It is a strange prohibition, as not all activities on the college network are performed during classes or when students need to complete work; leisure time while on campus is standard. The preamble also requires to "read, understand, and comply with" (17) AP 3720, which is a clause

---

most violate as only the most curious of individuals read policies like it. There is more standard boilerplate about unacceptable usage, and then a critical line of intention: "The District is committed to providing access to computing resources to all members of its current student body, faculty, staff and members of the Board of Trustees and other authorized community members." (23-25) It later clarifies that this is part of the "educational and service missions of the District". (26-27) Given the amount of unnecessary limitations and restrictions placed on the network, however, is Cerritos College fulfilling this? In fact, AP 3720 addresses this more directly on lines 29-31, stating that the District is responsible for "making [the network] accessible to the largest possible group of authorized and legitimate users and uses within the financial and educational constraints of the District." This is after its commitment to security. Given the demonstrations in this document of why many of its blocks are unnecessary, how can the Department claim to be abiding by the terms of AP 3720?

### **Privileges and Responsibilities**

These sections do not contain much of notable substance aside from standard assumptions about how users should behave with regards to the network. There is minimal information of interest here. The harshness about software piracy is at first glance overdone, but is standard to limit the District's liability.

### **Individual User Rights**

This section contains the aforementioned due process recognition. It next provides for free speech and academic freedom; whether this is actually being implemented

---

is disputable given the effective censorship placed upon the network. It also mentions intellectual property rights for students, and provides warnings for privacy and offensive material receipt, thus disclaiming the District's liability. Most important are lines 108-111, which provide the Department a blank check "to access and monitor all files, and Internet and email use"; this has to be done for an "extraordinary reason", but the Department regularly employs (and abuses) the "basic system security" clause. It is not necessary to *log who searches for information about religion, or abortion, or any other applicable category* to maintain basic system security. It is not necessary to do it for the safety of the college, or of the students of the college. Either way, this clause is far too broad, and should be evaluated in the future to ensure that the rights of Cerritos College students are respected by the Department.

### **Appropriate Uses of District Computer Resources, Prohibited Uses of College Computer Resources, and Unauthorized Use/Failure to Follow Procedures**

These two sections are also fairly standard; while some revision could be done to ensure the facts and terminology are correct and up-to-date, it is not of immediate concern. ASCC has had to address the subsection entitled "Commercial and Political Use" before, however; its position is covered under JR-2223-01 ("Empowering ASCC to Advocate for Legislation"), statement #5 and resolves #3 and #7.

### **Additional Guidelines**



---

While there is nothing of concern in this section, it should be noted that the requirement that vulnerabilities are immediately reported (335-337) is not enforced nor actually relevant/helpful. On May 15, 2021 at 11:00 AM, I reported a major vulnerability I discovered in PeopleSoft through the college's PeopleSoft HelpDesk. This received no responses.

## **Disclosure**

In this section, the District states that it "reserves the right to monitor all use of District computer and network system [sic] to assure compliance with [AP 3720]", but that it "will only exercise this right for legitimate District purposes". Yet again, we see that the Department has even gone beyond the absurdly low bar the college has set for itself in terms of how egregious its conduct is. Monitoring the categories which it does is not a "legitimate District purpose", unless searching those categories were to become, in spite of basic rights and freedoms, an illegal activity. It should also be noted that the December 5 document lists that the "terrorism" category should not be logged, which is absolutely absurd given the context.

The "'Cenic' Policy" section is not covered here, as it is a basic blurb about the District's Internet Service Provider (ISP) and how all users of the network must follow their policies in addition to AP 3720. It holds no relevance to this investigation; Cenic themselves are not responsible for any of the blocking decisions which have occurred.

---

## **BP and AP 3050**

### **Introduction**

This section reviews the ethics of the Department; whether they acted ethically in their handling of these situations and in their day-to-day actions. It also reviews the ethics of the Office of Business Services, and in particular VP/AS Lopez's handling of the events so far. Since ethics and morals can be subjective, this analysis is based on the college's own ethics policy (BP<sup>19</sup>/AP<sup>20</sup> 3050, "Institutional Code of Ethics"), which is binding on all individuals related to the college (including students, but especially faculty, staff, and administrators, like Director O'Donnell and VP/AS Lopez). To use BP/AP 3050 also requires reviewing them and their contents, which this section does.

### **BP 3050**

BP 3050 does almost nothing. It merely requires the existence of a "written code of professional ethics for all of its personnel", requiring that the District uphold it and delegating responsibility for doing so to the President's office. The aforementioned code is AP 3050. It would be helpful to have some basic ground rules laid here, with the details in AP 3050 - but the current state of BP 3050 is fairly consistent with other Board Policies.

### **AP 3050**

---

<sup>19</sup> [https://www.cerritos.edu/board/\\_includes/docs/BP/BP\\_3050.pdf](https://www.cerritos.edu/board/_includes/docs/BP/BP_3050.pdf)

<sup>20</sup> [https://www.cerritos.edu/board/\\_includes/docs/AP/AP\\_3050.pdf](https://www.cerritos.edu/board/_includes/docs/AP/AP_3050.pdf)

---

AP 3050 is the true code of ethics for the college, and the standard by which all employees are supposed to act with regards to the College, other employees, and students of the college. It is not a long document; it is the bare minimum by which all employees should know and follow at the college at all times. And yet, as will be explained here, the Department and the Office have been in continuous violation of it. The first page of the Procedure defines ethics (so as for it to be unambiguous during policy enforcement), states the importance of ethics, and sets some baseline expectations. These include being “committed to the principles of honesty and equity” (shoddy at best currently), not abridging student or employee freedoms “for any purpose” (a standard not followed), and not allowing the desires/interests of individual college members to be above the interests of the public. Employees are also supposed to exercise “dispassionate, fair, consistent, and equitable” judgements (not occurring), “exhibit openness and reliability in what they say and do” (not occurring), “confronting issues and people without prejudice” (arguable with regards to the Department), and to “demonstrate [an] ... uncompromising commitment to the principles of ethical behavior” (given the utter disregard for the aforementioned, not occurring).

On the second page is a list of responsibilities District personnel have, and thus must follow, as “practitioners of ethical behavior”. Each one shall now be analyzed individually with regards to the following of it by the Office and the Department:

- 
1. *"To provide and protect student access to the educational resources of the District."* **Not followed by either the Department or the Office.** This one is fairly simple and direct. The Department has not "provided and protected" to the fullest extent the educational resources of the District. Rather, it has stifled student access to them, through blocking educational websites (such as those required by students whose complaints traversed the Library) and other services necessary for the fulfillment of their education. The Office has fully supported these movements and has kept them going, and is thus complicit; it has not striven to "provide and protect" student access to these resources.
  2. *"To protect human dignity, intellectual integrity, and individual freedom, and assure that students are respected as individuals, as learners, and as independent decision-makers."* **Not followed by either the Department or the Office.** This has four main parts, with "intellectual integrity" somewhat stifled in general by websites being blocked:
    - a. Regarding individual freedom, the freedom to use the network properly has been limited by the Department, and reaffirmed by the Office.
    - b. Regarding respect as individuals, the Department has not been responsive to individual emails; it has only been when advisors/other staff get involved, or faculty get involved, that they even respond to

---

emails, let alone make any changes. The Office has not yet demonstrated enough behavior to be fully in violation of this section.

- c. Regarding respect as learners, the Department has not allowed learning using District resources to properly occur; this has been reaffirmed by the Office.
  - d. Regarding respect as independent decision-makers, the Department has not trusted that students have the intelligence to remain safe online, to not threaten the college, or to have the expertise to know when a provided justification is incorrect. The Office shut out the students completely from all discussions, also not respecting students as independent decision-makers.
3. *"To protect students from disparagement, ridicule, or capricious judgment."* **Not followed by the Department, unclear by the Office.** The key violation lies within the definition of the word "capricious"; legal precedent indicates that it is any decision or judgment that is "the product of a sudden, impulsive, and seemingly unmotivated notion or action."<sup>21</sup> Based on this definition, the Department's decisions have generally all been capricious within the context of what has been covered by this investigation. The Office has no direct evidence of capricious judgment, albeit the hiding of reasoning in its closed-door conversations could leave room for it.

---

<sup>21</sup> <https://judddocumentservice.mt.gov/getDocByCTrackId?DocId=73675>

---

4. *"To keep foremost in mind at all times that the District exists to serve students."*

**Not followed by the Department or the Office.** Both of them have not been concerned at all with student interests. The Department avoids students and does not care about their input or concerns, rather just doing what it wants to whether its decisions are logical or not. It is also not "serving" students to be monitoring accesses of websites regarding religion or abortion. The Office has reaffirmed this, making it complicit, and has also kept students out of the loop, which does not help to serve students.

5. *"To foster a climate of trust and mutual support."* **Not followed by the**

**Department or the Office.** Both have made it clear that they do not seek to cooperate with the students, and have been untrustworthy so far in their handling of the situations. The conduct of the Department as demonstrated in the December 5 document also makes them untrustworthy.

6. *"To foster openness by encouraging and maintaining two-way communication."*

**Not followed by the Department, somewhat followed by the Office.** The Department has shunted two-way communication and has sought to do away with student concerns as quickly as possible. Emails go unanswered and tickets ignored. The Office has generally encouraged two-way behavior, albeit with the caveat that it has extremely delayed responses on many things.

7. *"To encourage, support, and abide by the written Board Policies and*

*Administrative Procedures of the District."* **Not followed by the Department**

---

**or the Office.** There have been some contradictions between the actions of the Department (as affirmed by the Office) and the contents of AP 3720. CPRA requests have been mishandled, violating AP 3300. Other unethical behavior has led to violations of this AP 3050. The Board Policies associated with these documents are, through their nature, thus also violated.

8. *"To challenge unethical behavior in a timely manner."* **Not followed by the Department or the Office.** The Department has not sought to correct its own unethical behavior. The Office has also not sought to correct its unethical behavior, nor has it challenged the unethical behavior of the Department.
9. *"To report to the Vice President of Human Resources or designee any concerns with this policy."* **Not applicable.** The furthest applicability would be as described in #8.

Of eight basic ethical codes (discounting #9 as it is procedural), the Department is in violation of all eight, and the Office is in violation of at least six.

## **California Public Records Act (BP and AP 3300)**

AP 3300 has already been covered previously. BP 3300<sup>22</sup> has not, but it merely establishes AP 3300 and states that it must comply with the California Public Records Act. As such, this section will be focused on the Act itself.<sup>23</sup>

---

<sup>22</sup> [https://www.cerritos.edu/board/\\_includes/docs/BP/BP\\_3300.pdf](https://www.cerritos.edu/board/_includes/docs/BP/BP_3300.pdf)

<sup>23</sup> State Legislature copy unavailable at time of writing, used: <https://tinyurl.com/capublicrecordsactpdf>

---

Section 6250 states that (reiterated in the State Constitution as aforementioned) that “access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person in [California].” Section 6251 titles the Act allowing it to be referenced as the California Public Records Act, and 6252 provides basic definitions. Section 6253 begins with the various rights given under the Act. 6253(a) provides that anyone can come in during the business hours of an agency and demand to inspect all public records.<sup>24</sup> 6253(b) requires that the records be provided upon request (fees are ONLY collectible under cases where other statutes list them, not applicable here, or where there are duplication costs, which do not apply to digital transmission) to any member of the public; 6253(c) lays out that this must be in 10 days *from the date of receipt of the request* (implying not business or instructional days as previously mentioned), and that any document-discovering extension must be reasonable and less than 14 days long. 6253(d) prohibits agencies from intentional delay of providing records, as well as from obstructing the inspection/copying of records as provided for in (a) and (b), also requiring that the names and titles of all involved in the denial be provided. 6253(e) allows agencies to make policies which require themselves to be faster, but not slower, than the minimums set. 6253.1(a) provides for previously mentioned services that must be provided to the requestor, and (b) provides where those are satisfied (such as a 6254, but not a 6255, exception being applied). 6253.2-6253.8

---

<sup>24</sup> While not individually verified, reports indicate that the Department requires fees for inspection, and sometimes shuts down inspection altogether.



---

are irrelevant as they pertain only to specific agencies. 6253.9 provides clarification on how to handle electronic records. 6254 and its subsections provide a long list of exceptions from disclosure of information, many of which only pertain to individual agencies; they are too numerous to cover, and no 6254 exceptions were claimed by VP/AS Lopez in his denials.<sup>25</sup> 6255 covers cases where the public interest in withholding the record is greater than the interest in providing it; this was claimed by VP/AS Lopez. 6257.5 (there is no supersection) clarifies that the reason for a record's request is not a valid reason to deny a request. 6258 provides permission to challenge denials in court. 6259 provides procedural information for claims made under 6258. 6260-6270 are not directly relevant to this case.

As explained previously, the CPRA is a binding piece of the Government Code. In denying the requests fallaciously, and continuing to uphold those denials, potentially illegal behavior has occurred. This behavior is also thus certainly unethical and unbecoming of Cerritos College employees. It leaves a bad stain on the college; it shows that transparency is not a key desire among the Department and the Office.<sup>26</sup> These denials could be referred to the President under BP/AP 3300, and this will occur in the future; however, at this point in the investigation, they have not.

---

<sup>25</sup> Caught later: it appears as if VP/AS Lopez attempted to use a 6254.19 denial in CPRA #1. However, he did not cite it as such, and did not quote the reasoning; he also did not put it verbatim. The documents still should have been released as covered in Chapter 2. The December 5 document also should still have matched in the search, so there was *no valid reason to entirely deny the request*.

<sup>26</sup> There are also (not yet independently verified) reports that there were attempts within the Office to subvert the release of the December 5 document, despite it being undoubtedly a public record. If true, these leave an even deeper stain on the Department's record.

---

## Chapter 4 - Statements and Opinions

This section contains various reports and statements from individuals involved with this investigation on the content of it, or of related actions by the Department. It also contains opinions about the gravity of this situation from a variety of sources, including Cerritos College students and others who are knowledgeable of the situation.

While collaborating with Amy in regards to the aggressive censorship, I had helped discover the rather extensive limitations Cerritos has put in place. New domains, potentially spun up from a small business or a new server spun up by enterprises, and domains set up to adjust the A record for dynamic IP addresses often found at homes can cause false positives with network issues, creating workflow and work ethic issues. Another inherent issue discovered with these limitations put in place is less traffic being able to be monitored by the IT staff, thus causing users to discover workarounds using solutions such as VPNs, remote desktop applications, and web desktop applications. These applications are secure by design using the similar trusted certificates that can be found on websites that are otherwise blocked in a “security by obscurity” approach for the network, further emphasized by the lack of records produced when legal public records requests were made. These security approaches fall apart once recognized by users as they are able to relatively easily evade, demonstrating a fundamental issue with the network security as a whole.

– Monica Hanson, Cybersecurity major at Southeast Missouri State University

---

Cerritos College has been in the midst of transformative change for some time. As it could transpire with any entity, there are still roadblocks that speak to a much larger picture. Slowly, but surely, these items will be addressed; and it will continue to take the tremendous efforts put forth by individuals who understand the intersectional inequities that have hindered a multitude of students and other individuals on campus disproportionately, from being able to embrace and manifest their own sense of authenticity. Consequently, potential and individual success may be all the more inaccessible. Sometimes, the conflict or challenge is invisible, but rarely is it non-existent. As we move forward as conscientiously as possible, it will take a village to discern, address, and rectify what has, for some, been socially and/ or culturally canon throughout the history of the institution.

– Nio Lavermon, Cerritos College LGBTQ+ Program Facilitator and Liaison

I think this report has a strong presence within the campus technology. There is a lot of potential change in the future and the more support we get, the better it will be. We can possibly or you potentially work with the student trustee to address this to the campus.

– Jeremy Ramos, Chair of the University Student Board of Trustees at CSULB, Former Student Trustee of Cerritos College, and Former ASCC Court Associate

Justice

---

I do not think that Cerritos College should be monitoring students' activity when searching through medical websites, abortion, religion, advocacy, and other related categories of websites. I believe that this is wrong due to the many ethical policies it violates.

- Anonymous Early College Program Student

The actions of monitoring student activities on certain websites such as religious and abortion websites which are personal matters of students done by the Office of Business Services headed by the Assistant Superintendent Felipe Lopez are very troubling. If Amy Parker didn't contact the Office of Business Services about the issue of blocking outgoing SSH traffic this receipt about the monitoring information of student searches gained from the library may have never been made public. However, the early issue about SSH that involved Amy in this investigation still stands, there shouldn't be a ban on outgoing SSH traffic because of the need to use it for Computer Science/ Computer Information Science students to access online servers. As a student I'm worried about my fellow students' online information being used against them in the future unknowingly when their information from certain sites should be private only. I can only hope that these issues involving the monitoring of student online web data and the blockage of outgoing SSH be resolved soon by the administrators and if not, more awareness is needed to spread awareness of these issues to students on campus.

- Anonymous Computer Science major at Cerritos College

---

I don't think this is a good idea.

- Anonymous Biology major at Cerritos College

You only wanted to be able to access certain online features that would have assisted you in your work. It was silly how they call it a security risk when the resources you wished to access did not fall under the criteria for problems. Yet when you tell the Director and VA [sic], they reaffirm the silliness the system gave you. Then when you use your rights to investigate and dispute their baseless claims, you get ignored and even mistreated. You decide to let it go due to the distress and the notion that you can go on without it. Yet you then are exposed to others who have gone through similar mistreatment and issues such as the librarian or Dean Miller.<sup>27</sup> You have now brought in ASCC as back up... yet the officials repeat their untruthful uses of the law to protect themselves. The cycle of unprofessional mistreatment and stonewalling continues even to this day... you been [sic] advocating for yourself and those in need for almost 4 months. It is crazy how your need of a service spiraled into uncovering the fact that these officials want to be paid for gaslighting, harassing, and ignoring a student's critical concern.

- ASCC Senator Minh Bui

---

<sup>27</sup> I believe Senator Bui was trying to refer here to VP/AS Brammer - likely a conflation between the positions of Dean SS and VP/AS SS.

---

## **Chapter 5 - Summary and Recommendations**

### **Summary**

All in all, the Department and the Office have been engaged in a myriad of unethical behavior which has abridged student freedoms and denied student rights. Starting with looking into and appealing the blocks on SSH and ICMP, I discovered a chain of events which implicate the Department in several unethical and illegal behaviors, all of which further infringe upon student rights and threaten safe student usage of the network. The Office was then demonstrated as complicit in many activities, including the obstruction of legitimate records requests through false denials. These denials were likely the result of bowing directly to the Department, as the falsehoods the Department has presented about security have appeared to make their way into PRA-response memoranda.

### **Recommendations**

As Director of Equity and Diversity, I will be continuing my investigations into these matters. I will be constantly advocating for the removal of unnecessary blocks on the network which stifle student abilities and harm equity and progress. I will also be advocating against the current system of monitoring/logging implemented by the Department. This information will also be sent by me to the President, so that he has knowledge of what has been going on in the Department and the Office.

---

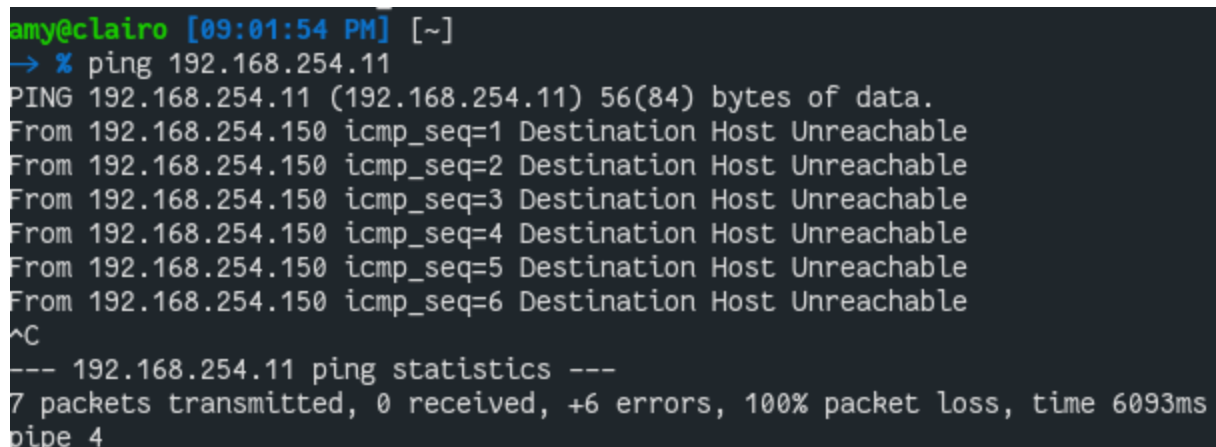
I recommend that we strive for a greater culture of openness and transparency at Cerritos College. In particular, we should begin with eliminating desires to hide information, and immediately ceasing espionage on students except to the degrees required by law. Antiquated systems for controlling students should be rapidly eliminated. A new mindset should be installed to follow AP 3050's principles, and to focus on the needs of students as the first priority. These goals for focusing on students and striving for ethics need to reach into Director O'Donnell and VP/AS Lopez, with the hope that they can become bastions of supporting student rights and freedom.

I also recommend that ASCC continue to advocate for the rights of students. Until the changes it desires are implemented, it should never rest. ASCC should always be striving to bring about change and to eliminate problems like the ones outlined in this article. As students, we have a voice and a responsibility to ensure that our peers are being treated correctly and that their rights are not infringed. It is time that we stand up and perform our duties as the elected and appointed representatives of the students.

---

## Appendix A: Real-World Example Usage of ICMP

After I finished writing the bulk of this report, I was working with one of my servers, trying to diagnose why it keeps crashing. As I went to try and test without physical access to the server, I remembered another common usage of ICMP: testing whether a server being down is really the server failing, or if it's just a broken route. Most of the time, a truly down server will end up causing something on the network to send back an ICMP 3-1, "Destination host unreachable"/DHU (see aforementioned RFC 792). In my case, I was able to verify that my server crashed by receiving DHUs back over the network, as shown in the image below. This isn't just useful on local networks, it's also useful for web and client-server applications; many applications use DHUs to determine if you have a mere connectivity issue, or if something is down entirely. These applications do not function properly (and may even have undefined behavior) when ICMP is blocked.



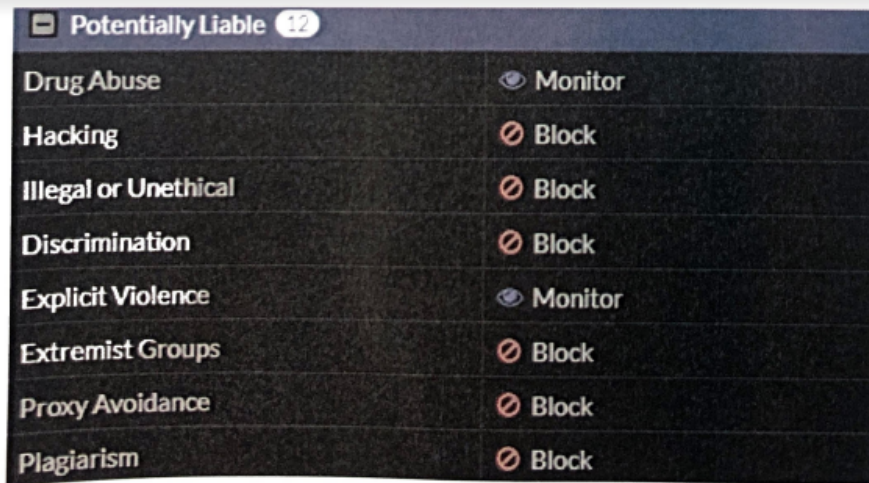
```
amy@clairo [09:01:54 PM] [~]
→ % ping 192.168.254.11
PING 192.168.254.11 (192.168.254.11) 56(84) bytes of data.
From 192.168.254.150 icmp_seq=1 Destination Host Unreachable
From 192.168.254.150 icmp_seq=2 Destination Host Unreachable
From 192.168.254.150 icmp_seq=3 Destination Host Unreachable
From 192.168.254.150 icmp_seq=4 Destination Host Unreachable
From 192.168.254.150 icmp_seq=5 Destination Host Unreachable
From 192.168.254.150 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.254.11 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6093ms
pipe 4
```



---

## Appendix B: December 5 Document

Given the importance of the December 5 document to this investigation, it is important to share it with the public. The document has affixed to it the date it was generated (October 2021, slightly cut off), and the date it was designed to be re-transferred to me (December 5, 2022, also slightly cut off). The document is appended as verbatim as possible; I had to screenshot the pages out of the pdf and paste them here. To the best of my knowledge, the chain of custody on this document is authentic; I see no reason it should not be treated as a fully authentic Department document.



Potentially Liabile 12	
Drug Abuse	Monitor
Hacking	Block
Illegal or Unethical	Block
Discrimination	Block
Explicit Violence	Monitor
Extremist Groups	Block
Proxy Avoidance	Block
Plagiarism	Block

*2/17  
from  
October  
2022*

12/5/22

Child Sexual Abuse	<input type="radio"/> Block
Terrorism	<input checked="" type="radio"/> Allow
<b>Crypto Mining</b>	<input checked="" type="radio"/> Allow
Potentially Unwanted Program	<input checked="" type="radio"/> Allow
<b>Adult/Mature Content 15</b>	
Alternative Beliefs	<input type="radio"/> Monitor
Abortion	<input type="radio"/> Monitor
Other Adult Materials	<input type="radio"/> Monitor
Advocacy Organizations	<input type="radio"/> Monitor
<b>Gambling</b>	<input type="radio"/> Block
<b>Nudity and Risque</b>	<input type="radio"/> Monitor
Pornography	<input type="radio"/> Monitor
Dating	<input type="radio"/> Monitor
Weapons (Sales)	<input type="radio"/> Monitor
Marijuana	<input type="radio"/> Monitor
Sex Education	<input type="radio"/> Monitor
Alcohol	<input type="radio"/> Monitor
Tobacco	<input type="radio"/> Monitor
Lingerie and Swimsuit	<input type="radio"/> Monitor
Sports Hunting and War Games	<input type="radio"/> Monitor
<b>Bandwidth Consuming 6</b>	
Freeware and Software Downloads	<input type="radio"/> Monitor
File Sharing and Storage	<input type="radio"/> Monitor
Streaming Media and Download	<input type="radio"/> Monitor
Peer-to-peer File Sharing	<input type="radio"/> Block
Internet Radio and TV	<input type="radio"/> Monitor

Internet Telephony	Monitor
<b>Security Risk 6</b>	
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block
Newly Observed Domain	Block
Newly Registered Domain	Block
<b>General Interest - Personal 35</b>	
Advertising	Monitor
Brokerage and Trading	Monitor
Games	Block
Web-based Email	Monitor
Entertainment	Monitor
Arts and Culture	Monitor
Education	Monitor
Health and Wellness	Monitor
Job Search	Monitor
Medicine	Monitor
News and Media	Monitor
Social Networking	Monitor
Political Organizations	Monitor
Reference	Monitor
Global Religion	Monitor
Shopping	Monitor
Society and Lifestyles	Monitor
Sports	Monitor

Travel	Monitor
Personal Vehicles	Monitor
Dynamic Content	Monitor
Meaningless Content	Monitor
Folklore	Monitor
Web Chat	Monitor
Instant Messaging	Monitor
Newsgroups and Message Boards	Monitor
Digital Postcards	Monitor
Child Education	Monitor
Real Estate	Monitor
Restaurant and Dining	Monitor
Personal Websites and Blogs	Monitor
Content Servers	Monitor
Domain Parking	Monitor
Personal Privacy	Monitor
Auction	Monitor
<input checked="" type="checkbox"/> General Interest Business 16	
Finance and Banking	Monitor
Search Engines and Portals	Monitor
General Organizations	Monitor
Business	Monitor
Information and Computer Security	Monitor
Government and Legal Organizations	Monitor
Information Technology	Monitor

---

Armed Forces	👁 Monitor
Web Hosting	👁 Monitor
Secure Websites	👁 Monitor
Web-based Applications	👁 Monitor
Charitable Organizations	👁 Monitor
Remote Access	👁 Monitor
Web Analytics	👁 Monitor
Online Meeting	👁 Monitor
URL Shortening	✅ Allow
📄 Unrated <b>1</b>	
Unrated	👁 Monitor

---

## Appendix C: VPN Testing

As previously mentioned, VPNs are a critical tool for circumventing censorship, blocking, and traffic monitoring. This list provides the testing results of several VPN/tunneling protocols, which span the majority of VPN softwares, across the Cerritos College network. Endpoints/gateways were provided for by SEMO cybersecurity major Monica Hanson. The results clearly indicate that all major VPN and tunneling protocols are blocked.

- SSH: **FAIL** (as previously covered, re-tested January 10, tested again over port 60022 on January 17)
- L2TP over IPsec (often referred to as just L2TP or IPsec): **FAIL**
- OpenVPN (most common): **FAIL**
- WireGuard: **FAIL** (protocol is completely blocked)

It should be noted that WireGuard being blocked is a major issue for users of NetworkManager, a common method for \*NIX network management. In my testing (Fedora 35 and Ubuntu 19.10), a broken tunnel to a WireGuard instance causes NetworkManager to hang completely, stopping all network traffic in the process. This does not occur with OpenVPN, SSH, or IPsec. For those who are not technically knowledgeable, fixing this is nearly impossible.<sup>28</sup>

---

<sup>28</sup> For more information, read my report on the FreeDesktop GitLab instance for NetworkManager: <https://gitlab.freedesktop.org/NetworkManager/NetworkManager/-/issues/1183> This issue should tentatively be considered as fixed, although it's more symbolic of the overall problems that blocking protocols can cause.

---

## Appendix D: PRA #3 Response (Direct Falsehoods)

It's official: the Office of Business Services has now submitted to me a direct, undeniable lie with regards to the issue of category blocking/logging. There is no way to attempt to deny the actions of the Department and the Office here now. On January 10, 2023 at 3:51 PM (8 days after submission), VP/AS Lopez returned a response to PRA request 3. He yet again invoked the section 6255 exemption (not cited previously, but cited this time) used on PRA request 1, which alone would be further confirmation as this has nothing to do with "a potential increase for an attack, compromise, increased risk or other vulnerability to the integrity and security of [the Cerritos College] network and computing environment". There's an even more important bit in the response after that, though: "Additionally, we do not have this type of list readily available, and we cannot prepare, compile, synthesize, summarize, or index this information as it is not already existing." The information does already exist, compiled, prepared, and synthesized, through the October 2021 document; replicating a new version, or even sending that one, would be acceptable. They also effectively admit that they are logging student activity in this response, however, by saying the "District cannot share [its] logging methods, monitoring capabilities, technologies used or internal processes for such activity"; I consider this a direct admission. As much as I hoped that this was all some confusion, all good-faith mistakes, this is undeniable; they are hiding information without any legitimate reason, and covering everything up.

---

## Appendix E: Final Update, January 17-18

Prior to the writing of this final update, I received information that VP/AS Lopez would attend the ASCC Cabinet meeting where this report was being disseminated. He was attending to provide an update on gender-neutral bathrooms at Cerritos College, following JR-2223-04 and the applicable board resolution. I was informed that he was not intending to stay for the whole meeting; I have now asked him if he would be able to stay, but have not received a response. I also asked Director O'Donnell if he could attend; he declined, as his vacation consumes the third week of the semester, interfering with his ability to attend the meeting.

On January 17, I came to the Department of Information Technology's office again. This time, I had a pre-prepared written clarification for my request to search documents in-person. Knowing the delays often introduced into these requests, I made sure to clarify that I was making a PRA 6253(a) request. This meant that I should have been able to go in and search records directly - the written clarification was just an *optional* aid I provided to the Department. Instead, Director O'Donnell decided to not let me review the documents; he treated my request as a standard PRA request, and sent it off to Director O'Donnell to view. This directly contradicts 6253(a): "Public records are open to inspection at all times during the office hours of the state or local agency and every person has a right to inspect any public record ..." Director O'Donnell also stated the response would be received within 10



---

*business* days; California law does not specify business days, rather saying “10 days from receipt of the request”.

Later that day, I attended the special Board of Trustees meeting. This was done spontaneously - I didn't know this meeting was going to occur. At this meeting, I spoke more with Dean of Student Services Elizabeth Miller about the upcoming report. I also spoke with an ASCC Senator, encouraging her to come to the meeting. Further, I ran into Dr. Brammer, who I provided access to the in-development copy of this report. I did not speak on the issue to the Board of Trustees; any addressing of it that I do will be at a general Board meeting, and after President Fierro, VP/AS Lopez, and Director O'Donnell receive copies of that report. I hoped to reach President Fierro to speak with him directly about this report; unfortunately, the meeting finished early, and I was not able to speak with him.

As of the morning of January 18, while I am finalizing this report, there are no further updates. I am currently still awaiting a response to my request for the logs of my network activity from Director O'Donnell. I am also still waiting for the in-person PRA request to receive a response; I did send an email to VP/AS Lopez indicating when I gave Director O'Donnell the physical request, as well as the 6253(a) violation that occurred. I have also been gathering my final student comments for chapter 4. This report's content will not be modified beyond 11:59:59 Pacific Time on January 18.

---

## Attributions

- To Dean of Student Services Elizabeth Miller, who has been an excellent advisor for the Associated Students overall (and in particular advisor to the ASCC Senate, and interim advisor to the ASCC Cabinet), and who has aided significantly in my investigation through helping me get responses to emails and connecting with others who have also aided the investigation.
- To Research and Instruction Coordinator Stephanie Rosenblatt, who has provided me with advice during this investigation and who provided the December 5 document, the cornerstone of this investigation and the key item of proof with regards to the actions of the Department.
- To Monica Hanson, current Cyber Security student at Southeast Missouri State University, who has provided technical knowledge and assistance with this investigation, as well as general advice and support.
- To Former Deputy Director of Equity and Diversity Raylyn Lee, who assisted the investigation during her time as a member of the Associated Students of Cerritos College Cabinet and who provided me with advice on how to continue in many circumstances.
- To Student Trustee Hector Ledesma, who provided me with advice on this situation, as well as many others.
- To Vice President Emily Gomez, who assisted me with my attempts to speak in-person to the Department.

---

## Certificate of Affirmation

I, Amy Iris Parker, Director of Equity and Diversity for the Associated Students of Cerritos College Cabinet, as appointed by President of the Associated Students Mohadissa Naqvi, and as confirmed by the 2022-23 Associated Students of Cerritos College Senate, and as sworn in by Associated Students of Cerritos College Chief Justice Bryce Trevino, hereby certify:

That the former is a true and correct, to the best of my knowledge, statement of the facts regarding my investigation, as well as applicable good-faith analysis, regarding the conduct of the Department of Information Technology and the Office of Business Services at Cerritos College, and in particular their respective heads of office Director Patrick O'Donnell and Vice President/Assistant Superintendent Felipe Lopez.

**In witness whereof**, I hereunto set my hand at the meeting of these members of the Associated Students of Cerritos College Cabinet, in Norwalk, California.

---

Amy Iris Parker

Director of Equity and Diversity

---

Date