

Rufus Glasper
Chancellor

2411W.14th Street, Tempe, Arizona 85281-6942 • T 480.731.8100 • F 480.731.8120 • r.glasper@domail.maricopa.edu

HIGHLY CONFIDENTIAL 1

June 10, 2014

Maricopa Community Colleges
Governing Board
2411 W. 14th Street
Tempe, AZ 85281

Introduction:

President Saar, and Members of the Governing Board, here are my annotations to a plot designed by the Administration to terminate my position after nearly 30 years working for MCCCCD. This entire report was based on facts that are inaccurate and distorted with the purpose of confusing the Board and most readers who are not intimately familiar with the way ITS operates and who was responsible for what in 2011 and 2013. The key points this document fails to address are the following:

- 1. I was never privileged to the Stach and Liu report of either 2011 or 2013. That information was not shared with me. Last week, I requested a copy of the report and I was provided with an 8-9 page Powerpoint that were mostly blank/redacted pages.*
- 2. My hearing was completely rigged from the beginning. I was not allowed to present evidence or bring any of my witnesses. We cooperated with the process until the point where a defense was futile. My representative was replaced without my approval and policy after policy were violated to stack up the committee and keep me from presenting evidence. The entire policy section 15.2 in the MAT employee manual was violated.*
- 3. The 2011 breach involved areas of ITS that were not under my supervision or control.*
- 4. Where is George K. and what is his testimony? Has the Board heard what my supervisor has to say? I reported to him directly. He supervised my performance and gave me marching orders. He reported to the Chancellor directly.*
- 5. I was not responsible for the 2013 systems when they were compromised. I was working for John Webster on other assignments at the time and not even onsite. Has the Board contacted Mr. Webster to obtain his testimony?*
- 6. Even after nearly 30 years with MCCCCD IT and all the knowledge of IT system I have accumulated, no one ever approached me to assist and try to protect MCCCCD when the 2013 breach took place. The plan was to blame me from the beginning.*
- 7. This entire report refers to 'databases' that another Director and the Marketing Department were responsible for. Why am I being blame for a breach on a database that was not my responsibility?*
- 8. None of the systems I managed in 2011 were compromised. Issues with the security of these systems were never mentioned to me.*
- 9. The thieves entered through the front door via webservers managed by another team in ITS. These systems were the ones compromised, misconfigured and mismanaged. These systems were the ones that had to be fixed in 2011 to protect the house. Someone did not follow through with the tasks identified and thieves gained access to every room in the house in 2013. The databases I managed were secure, however the doors that keep people from entering the rooms where those resided were left unlock. Locking those doors was the responsibility of another IT Director. That is the way the VC of IT setup the department and divided responsibilities.*
- 10. The Chancellor is not accepting responsibility and neither is the VC of IT even though they were presented with letter after letter speaking of misuse of funds, mismanagement, morale, security and other issues that will eventually lead to the 2013 incident. All of this is in black and white and you have seem most of the letter.*

The FBI notified MCCCCD in 2011 of a major security breach. The Chancellor and the VC of ITS were informed. It was their responsibility to ask questions, follow through and ensure that MCCCCD was safe. They should have taken the initiative to make sure MCCCCD was safe. They should have talked to vendors, requested reports, do follow-up audits and all necessary due diligence.

My job is on the line after nearly 30 years helping with faculty, staff and students. I am being wrongly accused of doing things I did not do and be responsible areas of ITS that I wasn't responsible for. The top level administration of MCCCCD decided not to accept any responsibility for their negligence, are protecting themselves with millions of dollars of taxpayer money and are using employees as scapegoat.

Please allow me the opportunity to present my evidence to you and bring my witnesses in a fair and level playing field. If the Administration will not allow this, I begged you to please obtain a copy of the sworn deposition of Earl Monsour and either listen to the tape recording or read his sworn testimony. This is the only 'real/untainted' legal accounting of what took place in 2011 and 2013. District lawyers and lawyers from law firms now suing MCCCCD were present and cross examined Mr. Monsour for 3 days. The tape and transcripts are available for purchase and MCCCCD should already have a copy.

I was denied access to public records he needed to establish his defense. Mr. Corzo provided a list of witnesses, most of which would have testified if allowed. MCCCCD told Mr. Corzo that he could only use witness provided by the District. MCCCCD could not prepare a proper defense w/o public records needed for his defense.

In mid-2013, and after the security breach took place, the MCCCCD Administration implemented a new MAT policy (C4) to terminate employees. This policy was not in effect in 2011 and it was not a part of my contract for that year. The administration is using this policy and applying it retroactively to events that took place prior to this policy being in place. This is a breach of contract at the very least and it allows the Administration to fire employees at will.

I respectfully request a private meeting with the Governing Board to present the side of my story and respond to any questions you may have.

In accordance with Section 15.2 of the Staff Policy Manual Appendix C (the MAT Manual), I am forwarding to you a copy of the decision of the hearing committee supporting the recommendation that the employment of Miguel Corzo be terminated. After careful consideration of the hearing record and the evidence, I accept the committee's finding and will recommend termination of Mr. Corzo's employment at a subsequent meeting. This letter provides a monitoring report to the governing board concerning my recommendation.

The following board policies, as interpreted and discussed in detail in Attachment A, apply to my recommendation:

- 2.1 Treatment of Students- Chancellor Limitation (Chancellor holds individuals accountable for failure to meet performance standards which resulted in conditions that were unfair, unsafe, undignified, untimely or unnecessarily intrusive for students)
- 2.2 - Treatment of Faculty and Staff - Chancellor Limitation (Chancellor assures that procedures are fair and holds individuals accountable for failure to meet performance standards which resulted in conditions that are unfair, unsafe or undignified for faculty and staff);

Not true. I never in my entire career failed to meet any performance standards as documented in my employee evaluations. Letter after letter of recommendations from my past supervisors point to my performance between above standards. Please review my personnel file, in particular my evaluations in 2010 and 2011 by George K. You will see that I was performing at or above standards during that period and prior to that. I also urge to compare Mr. George K. evaluations to that of the Chancellor or those I did of my direct reports. You will see how sloppy and inappropriate those evaluations were. The issue of negligence hiring comes into play as I believe Mr. George K. never provided proper supervision of his employees and failed to document goals.

Please see the letters of recommendation from my supervisors before and after George K. that were attached to my email to you.

1 NOTE: THIS DOCUMENT IS HIGHLY CONFIDENTIAL AND SHOULD NOT BE SHARED WITH ANYONE. This document includes highly sensitive information about District IT operations, which if made public, would make it easier for a hacker to obtain unauthorized access to sensitive information we hold. This document also contains advice received from legal counsel, and reflects legal counsel's mental impressions. PLEASE TAKE EXTRA PRECAUTIONS TO KEEP THIS DOCUMENT PRIVATE. Please be aware that a version of this document that is redacted to for legal privilege and to protect the security of Maricopa's network will be provided to Mr. Corzo's counsel and produced as a public record.

1 Ten colleges and two skill centers dedicated to student success.

Chandler-Gilbert | Estrella Mountain | Gateway | Glendale | Mesa | Paradise Valley | Phoenix
Rio Salado | Scottsdale | South Mountain | Maricopa Skill Center | SouthWest Skill Center

- 2.5 - Asset Protection - Chancellor Limitation (Chancellor holds individuals accountable for failure to meet performance standards which resulted in rendering institutional assets unprotected, inadequately maintained or unnecessarily risked); and

Not true. I was never told by my supervisor that I was performing below standards. His evaluations do not reflect this. I took marching orders from my supervisor. None of the ERP systems I was responsible for in 2011 were compromised. The 300 or so identities stolen in 2011 came from systems owned by the Marketing Dept at MCCCCD and maintain by another Director in IT. Neither I nor my staff had access to these systems and could not therefore protect them.

- 2.8 - Communication and Counsel to the Board - Chancellor Limitation (Chancellor holds individuals accountable for failure to meet performance standards which left the Chancellor and the Governing Board uninformed that millions of individuals' data was exposed to unauthorized access for

Not true. I summited multiple letters to the Chancellor and VC of IT raising concerns about morale, employee departures, mismanagement, misuse of fund, MAJOR security risks that were communicated to me and other issues. The president of MAT and PSA presented letters to the Chancellor and the Board hoping that they will take action to protect the District assets. The Chancellor and VC of IT were not left uninformed. The Board was informed. A formal grievance was filed that 'CLEARLY' states that there were security issues that had to be addressed. This was meant to communicate and alert the Chancellor first and the Board next and to protect MCCCCD assets. (see. Grievance letter to the Board attached)

The Chancellor chose to ignore the grievance and every letter he received dismissing it as coming from 'disgruntled employees' rather than recognizing that this employees were all long-time MCCCCD employees who were trying to protect the District and alert him of what could happen. The only failure to meet standards came from the Chancellors unwillingness to take action, respond to the grievance in a timely fashion as establish by MCCCCD policies and accept responsibility. Employees communicated outwards their concerns in writing multiple time (See Chronology of Events attached), the Administration dismissed those concerns and took a chance that nothing will happen. Now, the Administration is using every dime MCCCCD has to protect themselves, avoid accountability and scapegoat the very same employees that tried to protect District assets.

a prolonged period of time).

Based on the hearing committee's report, the full record (which supports the hearing board's employment termination recommendation), and the reasoning discussed below, I respectfully submit that my recommendation of employment termination is in compliance with board policy reasonably interpreted.

I strongly believe that any action short of termination would be inappropriate based on the nature of the conduct at issue and the millions of people who were impacted by it. The impacted individuals and the public we serve deserve the clear commitment of all of Maricopa, acting together as one, to ensure that our employees understand that privacy and security is Job #1, and employees who fail to protect sensitive information will be held accountable.

This employment termination recommendation is a tipping point for Maricopa. I ask you to stand together with me to do the right thing so that the public we serve and our employees understand that we take the privacy and security of sensitive information entrusted to us very seriously.

The following paragraphs provide further detail. Nothing will be kept from the board.

If members wish to review the hearing transcript and exhibits, a copy of the personnel recommendations of independent counsel (which includes the investigative report), and/or the

I have tried to explain who did what in ITS and who was responsible for what. The MCCCCD Administration has turned a blind eye to every document I provided. In every single occasion from the interview with Kroll to the interview with Mr. Bowers, I have offered to provide more evidence if necessary and answer more questions if my innocence was questioned. Neither Kroll nor Mr. Bower nor anyone in this Administration ever cared to follow-up with me after very brief interviews.

My responsibility was to escalate the issues to my supervisor and the Chancellor if necessary. I did that in multiple letters that the Chancellors recognized not having taken any action on (See letter from Kerry Mitchell to the Chancellor in Jan 2014). All issues were escalated to the Chancellor, the VC of IT and even the Board before the 2013 incident took place and with plenty of time to react. Had they taken the time to read any of these letters, they could have prevented the 2013 incident. Not once and to date, did Mr. Glasper care to meet with those of us who filed a grievance in 2012 about mismanagement, misuse of funds, security issues etc. In early 2012, I had a personal meeting with Mr. Glasper as a few people in ITS were getting ready to file EEOC charges. I told Mr. Glasper that 'we had been lucky not to have been compromised'. I encouraged him to help MCCCCD and protect our systems. Mr. Glasper told me during that meeting that I had two choices, 1) Proceed with my EEOC charges and be pushed to the sidelines 2) Work directly for him and not worry about salary or the reorganization. I considered this a bribe and told Mr. Glasper that I would be willing to help MCCCCD as always, but given the nature of the issues I did not want to blind-side him but I had to continue with the EEOC charges. I have been sidelined since that day.

2011 and 2013 reports by security firm Stach and Liu (rebranded Bishop Fox), arrangements can be made to view them in the district office.

This information includes privileged and confidential information, as well as highly sensitive information about our IT operations that, if made public, would make it easier for hackers to break into

our network and obtain information without authorization. Accordingly, this information will not be shared electronically.

The District Could Treat This as a Default Decision, but Has Not

When a party fails to participate in a judicial proceeding, a default judgment can be entered. In a previous case, when the employee who wanted an indefinite postponement failed to continue his participation in the hearing process, I dismissed the appeal and submitted my recommendation as a consent agenda item. However, unlike that case, Mr. Corzo has created a public controversy, proclaiming that he is wrongly accused. It is important to demonstrate that the recommendation is

If that is the case, the Board should obtain a copy of Mr. Monsour's sworn deposition by the courts and review prior to making any decision. Where is George K? Where is his testimony? Has the Board interview Mr. Kahkejian? Is he being held hostage? Is the Chancellor being held hostage? I took direction from Mr. Kahkejian. He was my supervisor and his testimony and cross-examination is critical to my defense.

well founded and consistent with board policy. I encourage you to make a fully informed decision and consider my recommendation as a non-consent item, subject to policy governance principles.

Nothing will be kept from the board.

If members wish to review the hearing transcript and exhibits, a copy of the personnel recommendations of independent counsel (which includes the investigative report), and/or the 2011 and 2013 reports by security firm Stach and Liu (rebranded Bishop Fox), arrangements can be made to view them in the district office. Because of their legal confidentiality and data security sensitivity, they will not be shared electronically.

The Committee Followed the Prescribed Procedure

I note at the outset the Committee's finding that Mr. Corzo knowingly waived his right to appeal the recommendation by refusing to participate in the hearing.

PLEASE request a copy of Mr. Monsour sworn deposition that was made a couple of months ago to preserve his testimony for the courts. If you want to make a fully informed decision, I encourage you to listen to the recording where Mr. Monsour was cross examined under oath by District and other lawyers. This is the only real sworn testimony to date. This is where you will hear what truly happened in 2011.

I was forced to go to the press by the injustice taking place at MCCCCD. I have never done that in my entire career at MCCCCD. This time the Administration left me no choice. They were wrongly accusing me of doing things I did not do while stacking committees and testimony in their favor while denying me of due process. The future of my employment and my family was in the hands of people who were trying to avoid responsibility and conceal the truth. I had no choice. To this date, I sought to find an amicable solution to this issue. I have not filed any lawsuits and I have tried to protect true confidential information that could seriously damage MCCCCD. The message to the press was simply 'the Administration was fully informed of security risks. They did nothing and here are the letters. They are now trying to scapegoat employees'. The information we disclosed pales in comparison to what MCCCCD disclosed to the state attorney generals and it is now public in the Internet. The information we disclosed is now dated and no longer can be used to hurt MCCCCD. MCCCCD has publicly stated that their systems are now secure.

I have yet to see any of the documents that MCCCCD is using to raise accusations against me. None of these documents were made available to me.

I have never seen a copy of the Stach and Lui report of either 2011 or 2013 (see signed testimony from Martin Gang attached to your email) I requested a copy via public records of the 2011 report and I was given 8-9 pages of mostly blank and redacted information that appear to be a PowerPoint presentation. This information was not presented to me in 2011. My communication with Mr. Liu in 2011 only extend to a meeting where all the work that had to be done in systems managed by another IT Director were discussed. There was never any discussion of a compromise or security issues with our ERP systems in particular SIS in 2011. It was determined in 2011 that SIS was not compromised. SIS was one of the databases I managed back them.

This was no surprise: his attorney Richard Galvan told the press more than a week earlier (Arizona Republic, March 23, 2014) that he would not attend the hearing unless the district provided a huge volume of records, including documents he had reason to know were confidential by law.

Not true. We requested a series of document that were CRITICAL to establish our defense. We provided a list of witnesses to be crossed examined (See list of witnesses attached). We name the reason why these individuals and their sworn testimony was needed.. MCCCCD denied us access to records we required for our defense. MCCCCD denied us our right to interview and cross-examined key witness under oath (including Dr. Glasper). MCCCCD finally provided records in July 2014, months after our hearing and 1-2 days after I received a termination letter. We are yet to go over most of these documents and the Chancellor is recommending my termination. MCCCCD has taken months to gather documents, review information and interview people. The huge volume of information they are referring to is simply a 'SUBSET' of what other companies like the AZ Republic and Gallagher and Kennedy has requested. MCCCCD was forced to generate these documents even before we made our request. They used excuse after excuse to keep these documents from us until a judge recently 'FORCED' MCCCCD to yield those documents. These are critical documents needed to establish a proper defense (See letter from Richard Galvan attached)

(For your information, the court did not decide that the District's rejection of this or any other request was unlawful: under the judge's supervision, we were able to establish a realistic schedule for disclosure, and just as important, an agreement protecting against the disclosure of legally confidential records)

Not true. This is very misleading. While MCCCCD may not have been penalized for keeping the documents from the public when they were requested, MCCCCD is now being FORCED to provide this document on a schedule. MCCCCD has no right to deny public document and a judge had to intervene to enforce this. MCCCCD broke the law. If G&K did not file a complaint in court, MCCCCD would have continued to keep records from everyone. Mr. Galvan was not involved in this complaint and I have no idea what documents MCCCCD has deemed confidential or not. To date, MCCCCD has failed to provide me with a list of documents and their reason for claiming confidentiality (See letter from Galvan asking MCCCCD to explain confidentiality attached)

Mr. Galvan claimed to the hearing committee that the records requested were necessary for Mr. Corzo's appeal. At the same time, Mr. Galvan was working with members of the Arizona Hispanic Community Forum to submit documents and make statements to the board on Mr. Corzo's behalf. At the February board meeting, one of these advocates claimed the documents provided were "all the board needed" to reject the recommendation to terminate Mr. Corzo and another colleague. Mr. Corzo's advocates to the board insist the available evidence is sufficient for the board but not the hearing committee. The two positions cannot be reconciled.

The committee found that there was no basis in policy or law to further extend the date when the

I disagree. I cannot defend myself without critical documentation and witnesses. See letter from my lawyer attached (Exhibit 100). It is not July 2014 and the very first time that I am able to see 'a small set' of the documents I requested. Nearly 90% of the critical documents needed for my defense are still being kept from me. I was provide with a bunch of useless and unrelated documents. Once of such documents is information on the equine program at MCCCCD. This goes to show the intention of MCCCCD.

hearing would begin. I agree.

The documents were provide show enough evidence that the Chancellor and VC of IT knew about the situation in ITS, the mismanagement issues, misuse of funds, security issues, treatment of employees etc. These documents should have been sufficient to show the Board a pattern that would ultimate led to massive exodus of IT employees, EEOC charges, massive hiring of consultants and ultimately the security breach of 2013. These documents were enough to show the Board one critical point 'THE CHANCELLOR and VC of IT were told about the risks and the problems in ITS prior to the breach in 2013 and with plenty of time to react'. The responsibility of anything that took placed in 2013 was passed on to the Chancellor and VC of IT when employees filed a grievance. They should have taken action. They could have avoided the entire incident. These documents were enough for the Board to understand who was to be held accountable.

There were however, other critical documents that were need to establish a proper defense. These documents belong to MCCCCD and had to be retrieved via public records. The accusations raised by Mr. Bowers were very technical in nature. These documents were necessary to prove all allegations wrong. The Kroll report was necessary to determine how Kroll reach their conclusions and validate their finding. The Stach and Liu report was necessary to prove who was responsible for fixing the issues found in 2011. These and many other documents we requested were necessary to show that I did nothing wrong as stated by Kroll in his recording. See: <http://rickgalvanlaw.com/employment-law-blog/kroll-finds-employee-nothing-wrong-mcccd-blames-employee/>

The two positions reconcile. The first position was to prove who was ultimately responsible. The second position was meant to prove that I was innocent and the investigation was flawed due to what appears to be lack of knowledge and understanding in the part of Kroll of how ITS works and is organized.

When I was denied access to witnesses and public documents, I was in fact denied due process.

Then, Mr. Corzo's appointee to the hearing committee resigned just prior to the scheduled hearing date, after speaking with an unnamed attorney. The procedure does not address this situation. The hearing committee applied Robert's Rules and appointed a member who had been Mr. Corzos advocate and to whom Mr. Corzo stated he had no personal objection. Nonetheless, Mr. Corzo claimed he should have been consulted on the appointment. Mr. Galvan and Mr. Corzo used this issue as a pretext to do what his attorney had previously announced he would do: they left the hearing room, refusing to offer testimony under oath and subject himself and other witnesses to cross examination.

The committee did not prevent Mr. Corzo from having his written evidence, including his written response to the charge, entered into evidence and considered.

Since the recommendation to terminate was made, Mr. Corzo and his advocates, including his counsel, have waged an extensive public relations campaign to persuade the board to pre-empt the appeal

Not true. Please interview my appointee and you will find out why Mr. Landagora resigned. He could not ethically and morally comply with what the District asked him to do. He refused to sign an open ended non-disclosure agreement that will forever seal any documents or information he may need for a future defense if the District tried to go after him.

I never approved of the appointment of Mr. Mitchell as my representative. Mr. Mitchell was one of my key witnesses that needed to be cross-examined. MCCCCD tampered with my witnesses when they decided to appoint Mr. Mitchell to the committee. MCCCCD decided to deny me the opportunity of appointing a replacement for Mr. Landagora and failed to notify me of the situation days before the hearing. When I questioned the committee Chair if he knew about this, he testified under oath that he did not. When I asked him why he replied under oath that 'he had not read his emails'. In follow-up conversations with Mr. Landagora, document exists that proves that not only Mr. Dan Huston knew about Mr. Landagora situation but that he had been in contact with him and knew he was going to resign. When I questioned Lee Combs when he learned about Mr. Landagora resigning from the committee, his response was 'on Friday'. Hearing was the following Monday. Documentation exists that show that his is not the case either. Both of this individuals lied under oath. Mr. Lee corrected himself later. Mr. Huston did not. This is a violation of policy as MCCCCD basically created their own excuse to name a representative on my behalf.

I strongly urge the Board to get a copy of the transcript from the 1st day of the hearing and listen my conversation with Mr. Combs and Mr. Huston.

Without witnesses, without public records, without my representative in the committee, with legal counsel and the Chair of the Committee lying under oath, I had no choice but to leave the hearing. How could I defend myself?

process and decide this matter without input from the independent investigator, advocacy from counsel for the administration, or the findings of a hearing committee. Mr. Galvan and his clients have made many unsworn statements and shared with the board, the press,

Not true. See memos attached. We were prevented from entering witnesses and accessing records needed for our defense.

and the public many documents they claimed exonerated Mr. Corzo. Some of these documents do not exist in any MCCCC system. The person who claims to be the author, Mr. Earl Monsour, wiped his computer before he went on medical leave. In their publicity campaign, Mr. Galvan and his clients have published information that is legally confidential because it jeopardizes the security of district data.

Not true. Most of these documents exists in our email system and can be retrieved. Documents like the ITS Grievance where the Chancellor is CLEARLY told in several paragraphs that we have major security issues. Documents like the letters sent to the Chancellor warning him of risks, employee attrition, mismanagement, morale and other issues. Documents like the Security Oversight Report where the VC of IT is clearly informed of security issues that had to be fixed. Many documents do exist that prove MCCCC negligence. All these documents have been shared with the Board. The information we provided is dated and no longer of any significance. MCCCC has publicly stated that all systems are now secure. The information the District provided to the State Attorney Generals around the country contains significantly more confidential information that anything 3-4 years old that we provided. MCCCC disclosed the type of firewall, the fixes implemented, the location of the issues and other information that could be used by hackers to compromise MCCCC again. In addition, MCCCC has disclosed in public Board minutes that it will take 18-24 months to fix their systems. It also goes on to state that this does not include the college systems. The two statements CANNOT be truly reconciled. On one hand, they are saying all is safe. On the other they are denying it.

I strongly urge the MCCCC Board to look into the security of the systems at MCCCC today, in particular, the college systems. MCCCC may still be very vulnerable.

The board should not condone Mr. Corzo's attempts to circumvent the hearing process and make a political decision, in which he can avoid giving sworn testimony and facing cross examination. If the board cannot hold accountable the IT employees who failed to maintain a secure system and failed to

This is not a political decision. This is simply scapegoating of employees to protect an Administration that should be held accountable. Extensive documentation exists where the Chancellor and VC of IT were told that there were security issues that had to be addressed, misused of taxpayer dollars that had to be looked at, mismanagement that will lead to attrition etc. All of this has transpired since it was reported. Now, the Administration is in denial. The future of MCCCC and education in our community depends on the Board holding those in position of power accountable.

respond appropriately to the situation in 2011, it will send a message to regulators that it does not share my commitment to reforming the District IT Department. The public, and the regulatory

agencies that are currently investigating the District, should not and I believe will not accept a political decision in this or any other action.

I find that the Committee's procedural rulings were compliant with board policy, reasonably interpreted.

Not true. Here are a few Board policies and other violations of the law that have taken place:

- *Untimely response to grievances*
- *Untimely notifications to employees*
- *Tampering with witness and personnel records*
- *Tampering with evidence*
- *Negligent hiring and supervision of employees*
- *Intentional infliction of emotional damage*
- *Wrongful termination*
- *Defamation*
- *Tortious interference*
- *Discrimination*
- *Retaliation and harassment*
- *Untimely response to hearings*
- *Denial of due process during hearings*
- *Denial of public records*
- *Breach of contract*

I am yet to file a lawsuit against MCCCCD and I have always sought to find an amicable resolution to this problem. Contrary to what appears to be the process with Mr. Kahkejian, the Administration has not made any attempts at trying to resolve this situation without further involvement of the courts. The resolution of this case could have been easy and painless for everyone, however the Administration prefers to continue wasting millions of dollars in taxpayer money to protect themselves rather than to seek an agreement with those being wrongly accused. For example, Mr. Monsour sworn deposition that was ordered by the Courts had over 10 lawyers present, 2 from MCCCCD and took 3 days to complete. This deposition generated a nearly 700 page document with facts of what took place in 2011. If you do the math, the cost to MCCCCD is nearly \$100K for the deposition of just one individual and that does not include the time MCCCCD has invested internally in protecting the Administration against my case and others. The future of MCCCCD is in your hands and like a well-known Maricopa supporter ('Paul Pair') used to say 'there has to be a better way'. Specially, when people are willing to cooperate. Bullying and harassing employees cannot be the answers. It will create an army of lawyers that will bankrupt the organization.

The Committee's Findings and Conclusions are supported by Substantial Evidence

Not true. The committee findings and conclusions are supported by the MCCCCD interpretation of their evidence. I was not allowed due process in the hearing. I was not allowed to inspect any evidence. I was not allowed to present any witnesses. I was not allowed due diligence to defend myself in a fair and equitable manner.

The Committee quotes from the testimony and the documents extensively, and review of the record demonstrates that they do so accurately. Their interpretation and application of my administrative regulations and other documents is reasonable, and is supported by expert testimony.

It seems clear from the evidence presented, and I agree, that Mr. Corzo failed to work in collaboration with the other members of the IT team to assure that his and the



Not true. Besides heavy redaction that barely allows me to respond, these statements are not true. I worked closely with my staff and others at the time of the 2011 incident as documented in Mr. Monsour log of events during this incident. My staff checked SIS and other ERPs under my supervision. As pointed out in this document, Mr. Monsour initially contacted me to verify that SIS had not been compromised. I directed my team to change passwords as a precaution in all ERPs and worked with the CIMS team to make sure that system had not been compromised. In addition, I was asked to name a 'technical' representative to work in the investigation team to represent the DBA team. I appointed the most qualified person in my team and worked with that person to implement any recommendations related to the ERP systems. As a side note, I have never seen the Stach and Liu report. All I heard was that web servers had been compromised. All I knew is that Mr. Monsour and Mr. George K. were in the loop and aware of the situation. There was nothing to report upwards at that time. The VC of IT was informed and aware. The person in charge of strategic security was involved. The person responsible for the web servers and databases that were compromised (Rod Marten/Marketing Dept) were involved and working on the issue. Executive leadership did not remain ignorant. Letters sent by the VC of ITS to MCCCCD show the extent of their knowledge, which was more so than the extent of mine at the time. It was the responsibility of the VC of ITS to report to the Chancellor. It was only in 2012, that after issues went unresolved for months, I filed a grievance pointing to security issues and escalated security and other concerns to the Chancellor and the Governing Board. The Chancellor had "PLENTY" of time to address this issues 'BEFORE' data was exposed. I DID NOT FAIL to communicate or perform any of my duties.

PLEASE obtain a copy of Mr. Monsour's deposition before making any decisions. This is a huge cover up by an administration trying to avoid responsibility.

He knew or should have known that the---

-----and should have insisted as far up the chain of command as necessary, that this was unacceptable. Once he heard the preliminary findings of Stach and Liu, he should have insisted that they be allowed to investigate his - which was reportedly advertised for sale on the internet. Also, he should not have allowed executive leadership and the board to remain ignorant of Stach and Liu's specific findings of-

----- or to accept that only a few hundred

individuals' data had been exposed. By failing to do these things among others, he failed to perform duties that had been communicated to him.

I agree with the testimony and the committee's finding, that his failure to provide accurate, reliable, and timely information of this kind to executive leadership was motivated by a desire to protect his job: he would certainly have faced serious questions about his performance if the true condition found by Stach and Liu in 2011 were disclosed to his supervisor, or higher. The finding that his

As VC of ITS Kahkedjian knew everything. He was the one making decisions to hire Stach and Liu. He was the one supervising the investigation of 2011. He was the one aware of the content of the Stach and Liu report. That report was never shared with me as mandated by Mr. Kahkejian (see letter from Martin Gang attached to the email you received). He was the one who officially communicated with MCCCCD. It is ludicrous to believe that he was not aware of the extend of the problems and actions necessary to correct a breach where the FBI was involved. If that was the case, he should be the one being held accountable for non-performance.

conduct was willful is supported by the evidence.

Mr. Galvan and his clients suggest that Vice Chancellor Kahkedjian had actual knowledge that our system was wide open to intruders in 2011. They claim that I had an opportunity to know all

about data security issues, if only I had investigated reports of poor morale in IT, and a grievance seeking to rescind Mr. Kahkedjian's reorganization of the department.

Not true. The Chancellor was told about serious security issues in the ITS grievance. This grievance was filed as part of an employee complaint, as part of an Internal EEO complaint and as part of a Federal Government EEOC charges. It was sent to him repeatedly by PSA and MAT Presidents in 2012.

As VC of ITS, it was Mr. Kahkedjian's responsibility to be aware of issues in the department, to meet with his direct reports and understand issues at hand. In 2012, Mr. Kahkejian stopped meeting with his direct reports for months. Seldom did he visit the Emeral Building where members of his leadership reside. He never provided any feedback in his employee evaluations. Mr. Kahkejian was an absent leader. It was Mr. Kahkejian responsibility to report issues to the Chancellor as needed. Mr. Monsour, myself and others reported back to him. It was his failure to escalate and the Chancellor's failure to respond that lead to the security breach of 2013. As Chancellor and VC of ITS, these members of the leadership had full knowledge of a security incident where the FBI was involved. Messages sent to CEC and other members of the leadership attest to this.

The breach of 2011 was small in nature, however things had to be repair and corrected to avoid a bigger breach. Those responsible for these changes did not follow-through with the recommendations made to them. The individual in charge of making these changes was an IT Director, responsible for the webservers compromised and the database residing on it. It was not Miguel Corzo responsibility to fix this problems. It was the lack of follow-through by Mr. Kahjkejian and Dr. Glasper that ultimately led to the security breach of 2013.

I can attest that I sent Dr. Glasper ample documentation to make him aware of the risks and employees issues that ultimately led to the 2013 breach. I can attest that Mr. Kahkejian was well aware of what had to be done based on communications readily available between him and his direct reports.

The Hearing Committees findings to the contrary are supported by the record. I can attest that Mr. Kahkedjian denied such knowledge when I asked him, and that I had no such actual knowledge.

Mr. Corzo and his advocates make much of statements that were made to me by internal and external advocates, which culminated in an informal grievance that was submitted to me informally by MAT and PSA leaders in fall of 2012. The documents to which they refer demonstrate that the concerns focused on work environment and morale issues and their alleged effects, not data security.

FALSE. The grievance was a document warning the Chancellor that failure to address morale, mismanagement, wasteful spending, AND DATA SECURITY issues could have significant financial risks to MCCCCD. These same concerns were communicated to him in writing by others in ITS. The grievance is VERY CLEAR and the SECURITY statements are very bold. This should have never been ignored. It is not just the lack of follow-through that led to the 2013 incident. It is a compilation of issues all listed in the grievance. The Chancellor is choosing to minimize the significance of the paragraphs in the grievance warning him of security concerns. The massive exodus of staff, the morale, the lack of follow through, the wrongful spending, the mismanagement etc... all created 'THE PERFECT STORM' that ultimately led to the issues ITS faces today. It is ludicrous for the Chancellor to say that we did not report concerns about data security. It is in black and white in the grievance. It is in black and white on the S&L report that his direct report George K. was privileged to in 2011. If there was ever a communication failure, it was between the Chancellor and the VC of ITS.

The informal grievance was the response of the MAT and PSA leadership to Mr. Kahkedjian's reorganization of IT: the express, primary purpose of that grievance was to restore the affected employees to their former positions. The principal substantive reason for reversal of the decision was the employees' charge that the action amounted to unlawful discrimination. I immediately had this complaint investigated by an independent law firm, which found nothing unlawful.

There is nothing voluminous about an 11 page report. Voluminous is what this Board is being presented with as a result of negligence. The purpose of the grievance as documented in the grievance itself was to bring all the items to the attention of the Chancellor not just the items he felt compelled to address. Its purpose was for the organization to look into mismanagement, morale, discrimination, retaliation, security, misuse of fund etc. The issues dealing with the reorganization was only a portion of the grievance not the entire grievance. The Chancellor never ONCE asked to meet with me or any of those filing the grievance. Instead, the approach he took was to alienate me and others he thought were behind the grievance. To my benefit, he removed me or directed that I be removed of all database responsibilities as early as October 2012. As such, I no longer was responsible for the MCCCCD database when the 2013 incident occurred.

I accepted the firm's recommendations for policy changes in the area of reorganization. The voluminous grievance contained an 11-page addendum listing examples of alleged poor management of

Not true. This was a formal grievance. A grievance that should have been responded to in the timely manner as identified by Board policy. It is a grievance that was submitted over and over again to the Chancellor and MCCCCD. It is a grievance that we begged () be responded to. The primary purpose of the grievance was to show the Chancellor that the 'OVERALL' state of the department was so chaotic that it put MCCCCD at great risks. Nothing was done about it even as late as 2014.*

The external investigator found no age discrimination basis in our internal EEO complaint. THAT IS ALL. As documented, the company the District hired to 'represent the District', did not look into any of the policy and non-policy violation listed in the grievance. They made recommendations such as sending Mr. Kahjkejian to management training but they never investigated any of the ITS operational complaints. It was the Chancellor's responsibility to do so and he never did or at least never released.

IT resources. Its purpose in the grievance was not to call for an audit of all the issues, but to challenge the Vice Chancellor's reorganization decision by attacking his overall credibility as an executive leader, offering examples.

Everyone always asks why. Only Chancellor Glasper can answer that question. Perhaps the Chancellor thought that we were disgruntled employees. Perhaps he thought our issues had no merit. Perhaps he wanted to conceal information from the Board. Perhaps the truth was so painful that it was worth taking a chance at ignoring the grievance. Regardless, MCCCCD was compromise and he is ultimate responsible for acting on information presented to him by top leadership in his organization. The people who brought this to his attention had been serving the District for years and had what's best for MCCCCD at heart.

One document described some of these examples as consequences of the reorganization, but again the focus was on the then-proposed reorganization's effect on employee morale and its effect on organizational performance, not data security or any other particular concern.

An investigation into the merits of the reorganization would not likely reveal the true condition of the database, especially if the witnesses were inclined to conceal it to protect their jobs.

None of the specific concerns in the addendum was a proper subject for a grievance under our procedure. Nonetheless, I inquired about these concerns. Among them was a brief statement to the effect that data security had been jeopardized by Mr. Kahkedjian's partial neglect of recommendations in a "security oversight report" that were intended to address unspecified "security risks and deficiencies."

Not true at all. The grievance covers myriad of issues that we felt will ultimately lead to the current outcome. Since then the Chancellor cancelled a 2 million project (CFS) that we reported in the Grievance. Since then, nearly 50% of the department has resigned, quit or retired. Since then, the largest security breach in the history of an educational institution took place. The grievance was not just about the reorganization, it was about ITS and the current state of affairs. It was a tool to communicate with the Chancellor and the Board that we had serious issues. The Chancellor told over a year to respond when by policy he should have responded in 10 day. He held the grievance until it was finally escalated to the Board in 2014. He failed to follow policy. MCCCCD employees were forced to follow process and chain of command to raise their issue. They did everything they had to do to alert the organization. The Chancellor kept information from the Board, failed to respond to employees in a timely fashion and we believe he is ultimately responsible for what took place. What else could we have done? We were encourage to follow the chain of command and we did. The Chancellor decided he could simply ignore our grievance and failed to even meet with us personally to discuss the merit of our allegations. This was dismal failure of the Chancellor and the MCCCCD organization to follow their own processes and listen to employees.

The grievance did not suggest that immediate action was required to notify and help people because there was no security and their data had been exposed since January 2011. Instead, it suggested that

Not true. The grievance did not seek to notify people (students) about security issues. The grievance was meant for the Chancellor to help expedite resolution of unresolved security issues so people did not have to be notified that their information was compromised. In letters from Mr. Kahkejian to Mr. Monsour, it was clear that nothing was being done. Risks were never addressed before or after his leave. Mr. Corzo had absolutely nothing to do with any of the issues that had to be resolved. There wasn't a single item in the to do list identified that pertained to the team Mr. Corzo was leading. All Mr. Corzo was asked to do is change passwords in the ERP systems as a precaution and to make sure the data had not been compromised.

delayed resolution of the recommendations represented a "high risk to the organization" that "could expose personal information" presumably at some time in the future. Mr. Kahkedjian was on extended Family Medical Leave at the time of the grievance, and we do not normally contact employees in that status for legal reasons. However, when we were able to contact him, he assured me that he had not ignored any security recommendations or security issues and that to the best of his knowledge known

Where is George K. today? Where is his testimony? He was my supervisor and reported directly to the Chancellor. Why is his assurance all that is needed to prove his innocence? It is obvious by now that the security risks he mentions were in the process of being addressed were never resolved. Given that timing of this conversation with the Chancellor (2012), it is clear that Mr. Kahkejian knew about the security issues that had to be addressed and those were communicated to him.

risks were in process of being addressed when he went on leave.

Had the Chancellor looked at the merits of all the issues mentioned in the grievance he would have discovered the condition of the data security at MCCCCD. It was all in the grievance in black and white for him to act upon.

First of all, the database that was hacked in 2011 was not SIS. It was not a database that Mr. Corzo managed. It was a database that resided on the compromised webserver. The issues with this database were disclosed and the steps necessary to make corrections identified. This was a database managed by the Marketing Dept at MCCCCD in conjunction with the MCCCCD server team.

An investigation into the security issues raised in the grievance would have revealed that none of the agreed upon changes to keep the system safe were completed. It would have revealed that the system was still vulnerable to hacker attacks. It would have revealed everything Stach and Liu discovered in 2013. I asked the Chancellor to look into the reorganization of ITS, however that is not the only thing that the grievance contains. That is just a small portion of that complaint. The grievance if acted upon could have safe MCCCCD millions in consultant and lawyers. The grievance if acted upon could have safe MCCCCD reputation from being tarnished.

I stress that the examples in the addendum were not listed by the grievance among the "non- policy" issues the employees wanted me to address. Nor were they the focus of the MAT and PSA leadership or the Office of Public Stewardship.

Not true. We met with the Office of Public Stewardship to bring these issues to light and to the attention of the Chancellor. Mrs. Teresa Toney sent a letter to the Chancellor asking him to address these issues as they could create significant problems for MCCCCD. His response to Teresa's message and she sent at least two, was 'Thanks'. Nothing ever took place. So if the committee feels that I am entitled to whistleblower protection by having done so, I therefore claim whistleblower protection for raising the issues with the Office of Public Stewardship.

These issues were focused on the IT reorganization and the alleged mistreatment of the employees. The remedy sought was not immediate action on the alleged consequences but rather on the alleged cause - the reorganization.

Not true. The grievance sought to find a solution or address a broad range of issues including the reorganization. It was not its sole purpose to focus on the IT reorganization. This grievance was repeatedly brought up to the Chancellors attention.

To be very clear, no one informed me at any time before 2013 that ... access to our systems, that our system was "wildly misconfigured and very insecure," that no

, and that because of this over two million people already had their data exposed. This information was known to the MAT employees I have recommended for termination. They did not report it to me.

I reported to Mr. Kahkejian. The unresolved security issues that led to the 2013 security breach were reported to the VC of ITS by his direct reports, Earl Monsour and Rod Marten, the two individuals in charge of the 2011 investigation. Mr. Kahkejian should have reported back through the chain of command. Please interview Mr. Kahkejian. He was the person reporting directly to the Chancellor at the time. My role in this investigation was to provide support and my teams did so. The security issues and related details were known to others not me at the time of 2011 incident. I never communicated with the FBI or was privileged to a lot of information regarding this incident. Details were not known to me. When security incidents happen, ITS policy was to keep as few people involved as possible. Since the information I was responsible for was not compromise, I was kept at a distance. I was made aware over time that repairs and recommended steps were not being taken to protect MCCCCD from further attacks. I made this known to the Chancellor via the ITS grievance in 2012. I was copied on emails from Mr. Monsour that made it clear that steps were not being taken. Mr. Kahkejian was also copied on these emails and should have taken necessary action. It was not my responsibility to do his job.

What did come forward to me is consistent with Earl Monsour's e-mail report to George Kahkedjian dated February 3, 2011, which you will find in the record. This is the only self- authenticated document I have seen, showing what Mr. Mansour actually reported to Mr. Kahkedjian about the condition of data security in 2011. Here is his reassuring conclusion:

"At this time, we have no evidence that any MCCCCD data has been breached. Services have been restored in general. A few minor changes or delays have been realized due to some - made to protect our environment, and there is a possibility that a few more may result as we move forward. However, we don't anticipate anything major. We will make every effort to resolve these as soon as possible when encountered We have now extended our investigation into other-, to ensure the attacks have not spread. We are moving forward with the development of a new standards, processes, and-

The Chancellor was CLEARLY told that security issues were still unresolved that could expose data and bring great financial consequences to the organization. I kept no information from the Chancellor or the VC of IT. Even though I was not in charge of security or the systems that were compromised, I use the grievance and many letters sent to the Chancellor to communicate the situation. It was the responsibility of the VC of ITS

capabilities will be implemented "

This is correct. In 2011, there was no evidence that any MCCCCD data had been breached other than the identity of 300 or so individuals who were notified. That is what the investigation concluded and what I was told as well as the message that was sent to all MCCCCD by Mr. Kahkejian. The SIS system was secured and we had no evidence of any breach on our ERPs. As the Director over the ERP databases in 2011, I was performing at or above standards. The security of our ERPs was not compromise.

It is my understanding today that the Stach and Liu report speaks of vulnerabilities and misconfiguration of the webservers at MCCCCD and the databases residing on these servers. These servers WERE NOT my responsibility. These servers HAD to be replaced and rebuilt to reduce risk and avoid further intrusion. Those responsible for this effort did nothing. Most of the agreed upon remedial actions were ignored and never completed. The risk and consequences were communicated to the Chancellor of MCCCCD and the VC of ITS,

Mr. Monsour reported directly to me and General Counsel Lee Combs that although there was no evidence that information had been accessed, a small number files containing old personal data from a few hundred faculty members was in a position that was not protected from hackers. He informed me that these individuals would be notified citing a past precedent. I recall that Mr. Kahkedjian

I have no doubt that this is probable the way things were when Mr. Liu looked into the MCCCCD webservers. Problems were identified by Stach and Liu in 2011 and never addressed. However, NONE of these issues had to do with the systems I was responsible for and I was never told of ANY security issues with the databases I managed. The system was exposed for 2 years or more b/c no one took action on our grievance or Mr. Monsour Security Oversight Report. This report contained no indication of any security issues dealing with the areas that Mr. Corzo had oversight and responsibility for as indicated to him by those in charge of the investigation at the time and documented in the ITS Security Oversight Report.

I knew about the general issues with the webserver as reported by Mr. Monsour and communicated to MCCCCD. The details of the misconfiguration and security issues resided with the Director over the servers that were compromised not me.

broadcast a notice to the MCCCCD community containing a similar message. From that point on until 2013, my understanding was that the incident had been effectively addressed and that steps were being taken to address known vulnerabilities. I was, as Mr. Liu testified to the committee, shocked to learn that the system was wide open, that over two million people had their data exposed, that this condition had existed for at least two years and probably more, and that Mr. Monsour and his colleagues knew about it.

The committee correctly interpreted and applied district regulations and the board's employment

Mr. Corzo had never seen the Stach and Liu report. This was never given to him. Mr. Corzo relied on others in the organization that were tasked with the responsibility to report the condition of the data exposure to move this information forward. Mr. Corzo's understanding of the condition of the exposure in 2011 was that only 300 people were compromised and the servers had to be replaced. This was communicated to the VC of ITS by Mr. Monsour who was the person in charge of this process. Mr. Monsour communicated with Rod Marten the tasks that had to be completed. Many of these tasks were never completed and it was in 2012 that Mr. Corzo and Mr. Monsour wrote the ITS grievance to raise awareness and alert the organization. Neither Mr. Corzo nor his staff had access to fix or even understand the true condition of what Stach and Liu found in the Maricopa webservers. Communication took place from those in charge of it. What happened is that there was no follow-up. The lack of follow up was reported in the grievance and the Security Oversight report in early 2012.

standards. Mr. Corzo failed to meet his responsibility to protect data before and after 2011 by allowing conditions to exist that resulted in exposure of sensitive information from the - for which he was responsible, and also by failing to make sure that executive leadership in 2011

understood accurately and completely the true condition of data exposure as Stach and Liu found it.

The District's dramatically different response to the same Information from Stach and Liu in 2013 demonstrates the dramatically different state of my knowledge.

When IT received a report from Stach and Liu in 2013, John Webster, Interim CIO consultant conveyed the information to me immediately.

The company was authorized to perform a complete examination, and I directed the situation be investigated and remediated. I initiated an internal audit, and as the scope and seriousness of the situation began to emerge I directed that the investigation must be independent of the District. We retained the exceptionally well qualified Lori Nugent and her Wilson Elser legal team to investigate the matter through Kroll, Inc, an industry leader in data security.

It is unclear how long the District took to respond to the 2013 breach. According to records, MCCCCD took nearly 7 months to notify the people impacted. Contracts with Kroll and those involved in the remediation efforts do not appear to have been issued until May/June 2013. Given the size of this contracts (millions), it is safe to assume that MCCCCD knew how extensive the problem was and decided to hold back public notifications. Ironically, the Chancellor's 1 year extension was granted a day before the press was notified in November 2013 of the security breach. Seven months is a long time to wait to notify the public. This cannot be in the best interest of faculty, staff and students or the community we serve. The personal and financial information for over 2 million people was left unprotected for 7 months while MCCCCD 'investigated', hired consultants instead of using internal staff and more importantly while the Chancellor had his 1 year contract renewed.

We exercised no control over their inquiry, as Mr. Caouette testified to the committee. Ms. Nugent's team applied MCCCCD policy to Kroll's factual findings. They recommended that the employment of several people be terminated, including Mr. Corzo. We initiated all the recommended actions.

I am yet to see what basis they use for that recommendation. No facts have been shared with me. It is clear that neither Kroll nor Mr. Nugent had a good understanding on how the ITS organization worked, who was responsible for what and how it was organized.

This entire process is riddled with attempts by the District trying to influence the outcome of the security incident. They hired a law firm whose motto is 'representing management' to look into the EEO charges. They denied us access to public records. They refused to accept our witnesses some of who were willing to testify in our defense. They violated grievance and hearing Board policies. They replaced our representative in the hearing committee. They did not care for anything that has been written. They wrote a termination recommendation knowing full well that I was neither in charge nor responsible in 2011 for security at MCCCCD. They raise several accusations some of which they have dropped in the final report. The list goes on and on. How can anyone believe that this was a 'fair and independent' investigation when those being accused have been denied of every opportunity to defend themselves?

Three individuals who were charged have resigned, and we accepted the resignations. Neither they nor the District agreed to "settle" any claims. In addition to Mr. Corzo, one person has requested a hearing. The procedural and substantive issues in that person's case are different from the MAT employees and we have attempted unsuccessfully to resolve them by agreement. I will propose a path forward for that person at a subsequent meeting.

This recommendation is not based on any hunt for scapegoats by me or my staff. An independent

This is nothing more than a witch hunt and scapegoating of employees. All you have to do is review all the evidence I have provided. All you have to do is review all the evidence provided by the press after careful consideration of facts, testimony from witnesses and access to records.

investigation determined the facts, and independent recommendations resulted in all the Personnel actions we have taken. The independent parties were given free rein to exercise their professional judgment, as the hearing record reflects. Neither my staff nor I sought to influence their recommendations.

When the Chancellor first learned of this incident, he failed to contact me. He never approached me for my help or advice, a person who has been running his ERPs systems for years. Instead, he brought consultants in whose first job was to learn about the system before they could investigate. This left the public and MCCCCD systems exposed longer than necessary. It is ironic that the lead investigator from Kroll told Mr. Corzo in a recording during his interview that 'he did nothing wrong but he could have done more'. Even after statements like this, the MCCCCD Administration is still trying to prosecute Mr. Corzo. It is also ironic that the lead lawyer for Wilson Elser left the organization shortly before the board decided to hire a local lawyer. Little did anyone know that this lawyer went to work for the very same local firm that the Board hired to handle its security affairs?

Dr. Glasper's response to the breach was to delay notification and leave the public exposed for months rather than rely on staff that knew about the system to begin remediation effort and protect MCCCCD data .

For several years the Chancellor has been made aware that this was the case. All you need to do is follow the money trail and do a financial investigation of all ITS projects he had recommended that this Board approve. You will see a pattern of failure after failure. A pattern of the Board being misled. A pattern of the same projects with different names being presented to the Board for approval over and over again. A pattern of overspending and projects being over budget and/or never completed. A pattern of a Board being misled by an Administration for years. A pattern of wasteful spending of millions of dollars in ITS. The Chancellor has done very little to resolve this and wasteful spending continues to date. Look at the recent projects approved by the Governing Board in 2013. What is the Chancellor doing with the Identity Management Software he purchased from Oracle?

I made the Chancellor aware of these issues years ago and little or nothing was done. A project like the CFS upgrade costs MCCCCD over \$2 million dollars and there as little or nothing to show for. Look at the ITS grievance carefully. It is more than just a document regarding the reorganization.

My Effort to Assist District IT to Address its Challenges

For several years I have been working to address the operational performance of District IT, which was not producing satisfactory results. Projects were not completed timely or as expected. Employees had difficulty functioning as a team. I supported Vice Chancellors as they used a variety of methods to improve IT results. I relied on qualified and trusted executives to manage their resources effectively and produce the expected results in this highly technical area

There should be no question that I support executives who make the case that additional IT resources are needed. When John Webster sought substantial additional funding to increase staffing, replace

Yes, and it is too little too late. The Board should interview Mr. Webster. All of this could have been avoided. Millions of dollars could have been saved had the Administration taken necessary actions when the information was presented to them. Even today, they deny receiving documents that are readily available. The lives of many loyal and committed employees has been ruined. Over 50% of the ITS department has left the organization. People have been forced to quit, resigned or retire against their will. Now the Chancellor is asking the Board for millions to outsource IT. That may very well be the only solution given that nearly all institutional knowledge is gone, however it did not have to be this way. I urge the Board to hire their own IT, Financial and Legal counsel to conduct an investigation.

equipment and software, and provide training, I supported his request.

The board approved it at the meeting of February 2013, two months before the hacking incident. My support for IT solutions after the incident also is a matter of public record.

The IT solutions after the incident came too late. The Chancellor had every opportunity to avoid what happened and save the District millions had he read our grievance and take time to understand the scope of the issues that were presented to him in early 2012. The actions taken by the Chancellor after the hacking incident are reactionary in nature. ITS has lost an incredible amount of irreplaceable institutional knowledge. ITS now has to outsource nearly all its ITS systems b/c there is little or no expertise left in house and no one trust the organization to protect the systems. Yes, the Board has approved millions in spending in 2013 but ask yourself how much of that was necessary and how much of that could have been avoided and redirected towards the classrooms, scholarships and community projects.

Before he left, Vice Chancellor Darrell Huish expressed frustration with his staff, whose continuous infighting, fueled by egos and ambitions, divided IT into factions that lowered trust and cooperation. This would have made it difficult for anyone to manage the Department effectively.

His successor, Mr. Kahkedjian, engaged in "team building" exercises intended to address this problem,

That is correct as others have reported but I was never disrespectful to Mr. Kahkedjian to his face. My evaluations by Mr. Kahkejian show that I was performing my job at or above standard both in 2010 and 2011.

with no result. Staff members openly expressed disrespect for his authority, to his face

I was in the process of addressing this situation when Mr. Kahkedjian unexpectedly needed to take medical leave. I continued to work on these issues with IT leadership, initially with John Webster, and

When Mr. Kahkejian arrived in the organization, one of the very first things he did was to invalidate a Strategic and Operational plan that was developed by his predecessor Darrel Huish. This plan called for an Information Security Officer to be put in place and for security to be the cornerstone of everything we did. I worked with Mr. Huish in the development of this plan. Instead of taking action as outlined in the plan and as developed by long time MCCC employees who knew about our strength and weaknesses, Mr. Kahkejian embarked in a year long process that generated a very superficial and high level plan with not operational details. Had Mr. Kahkejian accepted and implemented some of the recommendations from his predecessor to strengthen the security of our systems, 2011 and 2013 could have been avoided. This plan is available for the Board to review.

now with Ed Kelty and Sasan Poureetezadi.

This employment action is a necessary part of the pathway for improving IT performance by holding employees accountable for their conduct. Your support of this employment action is needed to make clear to all Maricopa employees, as well as the public we serve and regulators who are charged to protect the public that Maricopa takes seriously its obligation to protect the privacy and security of the information entrusted to us.

Conclusion

The board has the statutory authority and responsibility to "Remove any officer or employee if in its judgment the interests of education in this state require the removal." It also has the statutory authority and responsibility to "Adopt policies for the government of the community colleges under its jurisdiction" and to " ... set standards for the ... administration (and) operation ... of community colleges in the district."

The board has chosen to set the standards for determining whether the interests of education require removal. For the reasons set forth above, I believe the hearing committee's application of the board

When employees escalate a grievance to a supervisor, when employees write multiple letters of raising issues and risks to an organization, it is the responsibility of those in receipt of this information to take action or be held accountable for the consequences. The MCCCC Administration decided to take a chance and ignored serious issues being raised by employees. I strongly urge the Board to consider where the failure to follow process and standards took place. We were asked to follow process and we did. It slowed things done but we never gave up in our attempts to raise awareness. Our efforts were met with indifference and negligent behavior that ultimately led to where we are today.

standard to Mr. Corzo was appropriate, and the best interests of education require termination of his employment.

The board has also chosen to establish policies that govern the board's exercise of the power to remove. It has established a process that I must follow to reach a final recommendation. For the reasons stated, I believe I have followed that process. The board also requires me to comply with board policy as I reasonably interpret it. For the reasons stated above and in the detailed discussion

I was never given any indication by my supervisor that I was performing my job below standards. I have never been given a poor evaluation in my entire career at MCCCC. I have letters of recommendation from all my supervisors that speak of my commitment to MCCCC before and after Mr. Kahkejian. Many of the systems in place at MCCCC today were implemented by teams I led. None of the systems under my supervision were ever hacked including SIS. My teams received several Innovation of the Year awards. I brought in vendors like Microsoft to assess the security of our systems. Security was at the forefront of everything my teams did and none of the systems I supervised were ever compromised. The 2011 incident did not involve any of my systems. The repairs needed after 2011 did not have to be completed by my staff.

provided in Attachment A, I believe my interpretations are reasonable and that I am in compliance with

applicable board policy. Accordingly, I recommend that the board vote to terminate the employment of Miguel Corzo.

Respectfully,

Rufus Gasper
Chancellor

My case is a serious case of complete obliteration of Board policies to scapegoat employees and avoid responsibility. Board policies were broken during the notification process in the IT reorganization, the timing of events during the hearing, due process during hearings, responses to grievances and the application of termination based on a new policy being applied retroactively to events in the past. There has been no compliance with any applicable board policy being used to handle this case.

While others decided to resign and move on with their lives, I have spent an entire career at MCCCCD and I am committed to the success of the organization. I decided to fight this wrongful termination b/c I detest this Administration's attempts at intimidating and scapegoating employees. It is time to start holding our leaders accountable if they don't want to accept responsibility. If other organizations like Target Corporation can hold their CIO and CEO accountable for a major security breach why is MCCCCD trying to blame low level employees who were the ones trying to protect the organization in the first place? How can MCCCCD move forward when employees are treated this way? How can a Chancellor go after an IT Manager to protect his job? What kind of leadership is that? How can this behavior encourage others to come forward? Fear in the workplace is not something this Governing Bboard wants. An IT Manager in my position doesn't an organization make. The behavior of a Chancellor can make or break an organization. MCCCCD is facing billion dollar lawsuits b/c that behavior has been allowed to prevail for years.

ATTACHMENT A: DISCUSSION OF APPLICABLE BOARD POLICIES

Policies that Apply to the Recommendation

This is, in effect, a monitoring report. I submit that the following board policies apply to my recommendation:

2.1 - Treatment of Students - Chancellor Limitation

With respect to treatment of students, or those applying to enroll as students, the Chancellor shall not cause or allow conditions that are unfair, undignified, unsafe, untimely, or unnecessarily intrusive.

Interpretation: As applied to this recommendation, I interpret this policy to require that I hold individuals to account in a meaningful way when I believe their failure to meet board standards of performance has resulted in conditions that were unfair, unsafe, undignified, untimely, and unnecessarily intrusive for students: namely the exposure of student personal data to unauthorized access for a prolonged period of time,

Policy Compliance: Based on the hearing committee's report and the record supporting it, and the reasoning below, I respectfully submit that this recommendation is in compliance with Board policy, reasonably interpreted.

Board Policy 2.2 -Treatment of Faculty and Staff- Chancellor Limitation.

With respect to the treatment of faculty and staff, the Chancellor may not cause or allow conditions or procedures that are unfair, unsafe, or undignified.

Interpretation: As applicable to this process, I interpret this policy to require me to assure that the hearing committee in each case followed board approved policy and procedure according to its terms. As applied to my recommendation, I interpret this policy to require that I hold individuals to account in a meaningful way when I believe their failure to meet board standards of performance allowed conditions to develop that were unfair, unsafe, and undignified for faculty and staff: namely the exposure of their personal data to unauthorized access.

Policy Compliance: Based on the hearing committee's report and the record supporting it, and the reasoning below, I respectfully submit that this recommendation is in compliance with Board policy, reasonably interpreted.

Board Policy 2.5 - Asset Protection - Chancellor Limitation

The Chancellor shall not cause or allow institutional assets to be unprotected, inadequately maintained, or unnecessarily risked.

Interpretation: As applicable to this process, I interpret this policy to require that I hold individuals to account in a meaningful way when I believe their failure to meet board standards of performance failed to maintain data security and risked the exposure of individual community members' personal data and other digital access to unauthorized access.

Policy Compliance: Based on the hearing committee's report and the record supporting it, and the reasoning below, I respectfully submit that this recommendation is in compliance with Board policy, reasonably interpreted.

Board Policy 2.8 -Communication and Counsel to the Board - Chancellor Limitation

The Chancellor shall not allow any practice, activity or condition that causes the Board to be uninformed or unsupported in its work.

Interpretation:

As applied to this recommendation, I interpret this policy to require that I hold to account in meaningful way individuals whose failure to meet board standards of performance, I reasonably believe, left me and the governing board uninformed that millions of individuals' data was exposed to unauthorized access for a prolonged period of time.

Policy Compliance: Based on the hearing committee's report and the record supporting it, and the reasoning below, I respectfully submit that this recommendation is in compliance with Board policy, reasonably interpreted.

MARICOPA COUNTY COMMUNITY COLLEGE DISTRICT

In the matter of Miguel Corzo, Appellant

HEARING COMMITTEE'S
FINDINGS OF FACT AND Appeal of Involuntary Termination
CONCLUSIONS OF LAW PURSUANT TO SECTION
15.2 OF STAFF MANUAL APPENDIX C

(MAT POLICIES, DISMISSAL)

Summary of the Proceedings and the Evidence

This appeal of the involuntary termination of the employment of Miguel Corm (Appellant) came on for hearing pursuant to section 15.2 of Staff Policy Manual Appendix C ("the Manual") on March 31, 2014, at 9:00 am in the Offices of the Maricopa County Community College District ("MCCCD"), 2411 West 14th Street, Tempe, Arizona, before a Hearing Committee ("Committee") duly constituted under the above section. In accordance with section 15.2.8, the above hearing date was set by agreement of the parties and the committee. The original appointed members of the Committee were Daniel Huston, Chair; Dustin Landagora: and Irene Kovala, Ed. D.

Section 15.2.6 Manual charges this Committee with responsibility to "render written findings of fact and conclusions of law and forward same with its recommendation regarding retention or dismissal to the Chancellor." This document represents the unanimous decision of the Committee, and the chair is authorized by the members to execute it on their behalf.

Appellant Miguel Corzo appeared at the hearing with his attorney, Richard Galvan. The MCCCD Administration was represented by attorney James T. Tucker. The proceedings were transcribed by a court reporter.

This is an appeal of the recommendation to terminate the employment

Before the hearing, Mr. Tucker had informed the committee and Mr. Galvan that the evidence would include information about the security of MCCC'D's network, that state statute [A.R.S. §§ 13-2316.02(0), 13-2301(E)(8)] and MCCC'D policy (Governance Policy 5.6; Administrative Regulation 4.4) required everyone with access to such information to keep it confidential, and that he could share it with those involved in the hearing if they agreed to maintain that confidentiality. This would include Mr. Corzo, his attorney (Mr. Galvan), and the committee members. Agreement to maintain confidentiality

We were not willing to sign the confidentiality agreement for numerous reasons. First, on the face of it, the agreement was over the top containing numerous unnecessary provisions. As previously outlined above the information the District sought to protect was no longer confidential due to the passage of time and measures the District claims to have made to secure the information on its network. Also, we did not wish to enter into an agreement at the hearing level which might be adopted by a court in subsequent litigation.

Would be indicated by signing the proposed agreement. Mr. Huston and Dr. Kovalahad already signed the proposed agreement.

Before the hearing, Mr. Galvan had requested an extension of the time for the hearing in this matter, stating that MCCCCD had not responded to his request for records he considered necessary for his client's appeal. The Chair denied the request for extension because it did not meet the standard under Manual Section 15.2.8 and because Mr. Corzo's advocates previously stated to the Governing Board that she and others had submitted all the evidence necessary for the Board to decide the matter in Mr. Corzo's favor.

The District bullied us into thinking that all hearing representatives had signed this agreement and we were the only ones left. When we asked for copies of the signed agreements, the District failed to provide them.. We later learned that our representative had never signed such agreement. The District lawyers lied when they told us that everyone had signed except us.

With three work days available, the District had plenty of time to contact us and ask us to select another member for the Hearing Committee.

Notwithstanding his request, just before the hearing Mr. Galvan submitted a pre hearing statement with a substantial number of documents attached.

Three working days before the hearing, Mr. Landagora informed the chair that he had spoken with an attorney he did not name, and he resigned as a hearing committee member.

MAT Policy does not address this circumstance. The employee is merely required to appoint a member to the committee, and Mr. Corzo did so. According to MAT Policy, Mr. Landagora had accepted Dr. Kovala as a member, and the committee was duly constituted. Once duly constituted, the committee's duty is to conduct a hearing so that the Chancellor and the Governing Board can act in a timely manner concerning the employee's appeal. The resignation of a member cannot be allowed to cause the process to fail and bar any decision.

The Chair applied Robert's Rules of Order, which states that a deliberative assembly like the committee is competent to transact its business if half or more of its members are present, in the absence of a contrary rule.

Whatever Robert's Rules of Order says is not relevant here because the hearing committee/Mr. Combs had plenty of time to ask us for another selection.

The Chair asked Mr Kerry Mitchell to stand by to serve as the committee's third member in the

The appointment was made on the day of the hearing? And at no time before the appointment did the District/Committee/Mr. Combs think to tell us about the appointment before the appointment How to remove all footers in a Word document. Wow.

event Mr. Landagora failed to appear for the hearing. The Chair believed Mr. Mitchell, having been president of MAT and having advocated for Mr. Corzo and others under the grievance procedure could serve without bias or prejudice. When Mr. Landagora did not appear, the chair

The Board is relying on third party hearsay of individuals who are not representing Mr. Corzo and who are not formal advocates for Mr. Corzo. These "advocates" are neither lawyers nor are they aware of all of the issues and facts involved in this matter.

The evidence presented the Board was very limited in nature compared to what is available via the public records we requested. There is no reason whatsoever for the hearing committee to deny me access to information requested via public records request that I need for my defense. Most of the documents presented to the Board were meant to prove that the Administration was informed and knew about the security risks. They were therefore to be held responsible. Most of the documents requested via records requests were meant to defend myself against the allegations of wrongdoing made by Kroll. People who went in for of the Board did not speak on my behalf. They spoke on the topic and issues concerning my termination. This hearing committee has no right to determine what information I can and cannot use for my defense. I have every right to review most of the public documents I requested. I never stated that I had submitted all evidence necessary for my defense. The District denied me of that opportunity when they refused to provide me with records that were readily available at the time of my requests. It was not until July 16th, 2014 that I was finally able to start reviewing some of these records. I am not even done with my review and the District is recommending my termination and denying me of due process. In addition and as stated before, I was not allowed to bring any witnesses for my defense. The District indicated () that the only witnesses I could use where*
37
those provided to me by the District.

proposed to seat Mr. Mitchell as a committee member, and he was duly seated with the unanimous consent of the other members. He signed the confidentiality agreement.

When the committee replaced my representative with a representative named by someone other than myself, the committee not only violated policy but it lost an incredible amount of knowledge of how ITS works. The committee does not have a single member of ITS that could speak to the complexities of the organization and help them understand who did what. This shows in many of the wrongful assertions made by the committee throughout this document. It is obvious that members of this committee are not familiar with the Security of IT system, the complexity of ERPs, the responsibilities for webservers and operating system access and a myriad of other technicalities that make a significant difference of the outcome of their findings. The committee instead opted to simplify a very complex technology organization and use a broad brush to blame me for things I was not responsible for. Even the consultants are not able to grasp some of the complexities and that is shown in some of their testimony. I strongly feel that w/o an ITS expert in the hearing committee, this committee was not equipped to render a decision in such complex matter. Mr. Landagora was a long time ITS employee who was very much aware of the inner working of ITS.

Mr. Corzo stated that he had no objection to Mr. Mitchell and that he knew the committee was trying to be fair. However, Mr. Galvan stated that he objected to the Committee seating Mr. Mitchell as a new member because the chair had not consulted Mr. Galvan and his client about the appointment. Mr. Corzo then left the hearing room with Mr. Galvan.

Not true. I urge the Board to review the transcript. The opportunity to name a replacement to Mr. Landogora was offered to us at the start of the hearing. We were not prepared to name a representative and decided to leave when District Counsel indicated that we had no choice but to either accept Mitchell, leave or name a replacement on the spot. As offered by the Chair of the Committee, we decided to leave and made it very clear that we did not agree with the way the hearing was being carried on. We made it absolutely clear that we objected to this hearing process. We could have contacted another resource had we been given the opportunity. This is yet another example of the District violating policy, creating new policy on the fly and denying us due process. Mr. Mitchell was one of our witnesses not my representative in the hearing. Had I want Mr. Mitchell to represent me, I would have asked him to do so. My comment in the meeting did not imply by any means that Mr. Mitchell was to be my representative or that I agreed to that appointment. In addition, I am represented by counsel in that hearing and my counsel's decision was final. The use of Mr. Mitchell as my representative is yet another attempt from the District to tamper with my witness and eliminate his testimony.

The hearing commenced, in open session. District Administration exhibits 1 through 17 (D-1 through D-17) and appellant's exhibits 1 through 36 (A-1 through 36) were admitted into evidence without objection.

Nearly the entire section regarding dismissal in the MAT Policy Manual was violated. I was denied a fair hearing.

15.2. Dismissal

Upon the recommendation of the Chancellor and approval by the Governing Board, a MAT employee may be dismissed for cause. The employee shall have access to the following due-process procedures.

15.2.1. A written statement of charges, formulated by the college president or appropriate vice chancellor, shall be forwarded to the Chancellor. After review of the charges, the Chancellor may recommend to the Governing Board that good cause exists for the dismissal of the MAT employee. The Chancellor shall simultaneously advise both the Governing Board and the MAT employee, in writing, with a copy of the recommendation. This written notice shall be sent via U.S. Postal Service certified or registered mail to the MAT employee at his/her place of residence as recorded in the District records. The Chancellor's recommendation will give notice to both the Governing Board and the MAT employee of his/her intention to recommend that dismissal take place not sooner than thirty (30) calendar days from the date of the letter.

2. **15.2.2.** A written statement of charges specifying in detail the basis for the dismissal recommendation shall be provided to the Governing Board and the MAT employee as an attachment to the notification outlined in the preceding paragraph. The statement of charges shall, if applicable, state the statutes, rules, or written objectives of the District that the MAT employee is alleged to have violated. The statement of charges shall be of such specificity that the MAT employee will be able to prepare a defense based on the statement.
3. **15.2.3.** The MAT employee shall have the right to a hearing by filing a written request with the Vice Chancellor for Human Resources or designee within five (5) working days after being served with a notice of intent to dismiss. The filing of a timely request shall suspend the dismissal procedure, pending the completion of the hearing.
4. **15.2.4.** **Upon a request for a hearing, a hearing committee shall be constituted by the Chancellor or his/her designee within ten (10) working days. The committee shall be made up of three (3) members. The charged MAT employee shall select a MAT employee of his/her choosing. Another committee member shall be a MAT employee selected by the MAT Executive Council President or his/her designee. These two (2) committee members will approve of the third member named by the Chancellor or his/her designee. The third member shall be a College President or Vice Chancellor from a college or area other than the one in which the charged MAT employee works. In the event a decision cannot be jointly reached on the third member, the MAT Executive Council President will then be included in the decision making process. The employee subject to dismissal may attend the hearing; present any testimony, evidence, or oral and written statements in his/her behalf; cross-examine witnesses; and be represented by Legal Counsel and/or a non-lawyer personal representative.**

5. **15.2.5.** The hearing committee shall conduct the hearing no later than twenty (20) working days after the appointment of the committee. The hearing committee findings and conclusions shall be completed with ten (10) working days.
6. **15.2.6.** Within five (5) working days after completion of the hearing, the hearing committee shall render written findings of fact and conclusions of law and forward same with its recommendation regarding retention or dismissal to the Chancellor.
7. **15.2.7.** Within fifteen (15) working days, the Chancellor will review the hearing committee's findings, conclusions, and recommendation. The Chancellor will make his/her own recommendation to the Governing Board and forward same with a copy of the findings of fact, conclusions of law, and recommendation to the Governing Board. The Governing Board shall render the final decision for retention or dismissal. A copy of the final decision shall be sent via U.S. Postal Service certified or registered mail within twenty-four (24) hours to the MAT employee at his/her place of residence as recorded in the District records.
8. **15.2.8.** The time limits in this section may be extended only by the mutual written agreement of the parties or as the result of unforeseeable circumstances.
 9. **15.2.9.** No adverse personnel action shall be taken against any employee, representative, or other participant in the Hearing.
 10. **15.2.10.** The pay of the employee shall continue during the Hearing Process

15.2.1 I was notified 3 times of my dismissal in 2014. My termination never happened as it as supposed to have 30 days from the day of the letters. This is a violation of policy.

15.2.2 None of the statements were specific enough for me to establish a proper defense. MCCCCD claimed confidentiality of information and did not provide me with a single document, confidential or not prior to my hearing. This is a violation of policy.

15.2.4. I was not allowed to name my representative in the hearing committee. The Chancellor and the committee following advice from counsel replace my representative with one of their choice. This is a violation of policy.

15.2.5 The committee was supposed to complete the hearing and report their findings in 30 days after the appointment of the committee. It has been months since this committee was formed and met to discuss my case. This is yet another violation of policy.

15.2.5 – 15.2.7. These were all violations of policy as I finally heard about the findings in July 2014, months after the committee was formed.

and not end prior to the date of the decision of the Governing Board.

The administration called Mr. Vincent Liu, CISSP, as a witness. Mr. Liu is a recognized international expert in the field of cyber security and a principal in the security consulting firm Bishop Fox (formerly Stach and Liu). His work history includes services to Honeywell International, Ernst and Young Advanced Security Centers, and the National Security Agency. He has spoken on this topic at all

major conferences. Mr. Liu testified as to his work for MCCCCD in 2011 and 2012, and what he observed during that work.

The administration next called Mr. Gregory Caouette, EnCE, CFE. Mr. Caouette is certified in the use of EnCase software for computer forensic examinations. He is also a certified fraud examiner presently working for Kroll, Inc. His previous work includes service conducting internal fraud investigations for the Postal Service. Mr. Caouette testified concerning his independent

We have little knowledge of what witnesses testified to at the hearing because we were not present. There is a transcript of the hearing purchased by the District which would tell the tale.

investigation of the condition of MCCCCD's system, his investigation of the cause of that condition, and his findings and conclusions about what happened.

The administration called former Interim Vice Chancellor of Human Resources James Bowers, J.D., (Currently District Director of the Human Resources Solutions Center) who testified as to the content, interpretation, and application of district policies, procedures, and job descriptions in general and as applied to Mr. Corzo. He also testified as to his final recommendation (as interim VCHR) for termination of Mr. Corzo and the proceedings leading up to it.

The Committee conducted an open hearing whenever possible to honor Mr. Corzo's request. However, at Mr. Tucker's request the hearing was closed when questions began to address the condition of MCCCCD's computer systems and/or steps taken to secure the system.

It was Mr. Gregory Caouette who was recorded during a preliminary meeting with HR and Kerry Mitchell stating that 'You (Miguel Corzo) did nothing wrong'. It was Mr. Caouette is recorded during a meeting stating that 'he had nothing to do with the accusations' raised against me. Some of these accusations lead me to believe that Kroll didn't have a complete understanding of how ITS was organized and who did what in the department. One of the allegations against me was that I did not know anything about the state of a network device. I am not in charge of networking at MCCCCD and never have been. This along with other accusations lead me to believe that this investigation was rushed and unmeritorious. Allegations are being raised by consultants with little knowledge of the organization and who was responsible for what.

I requested an open meeting but it is my understanding that the media was asked to step out nearly 15 times on the first day. This was not an open meeting. This was a meeting controlled by the District with the pretext of security as an excuse. This was again a violation of my rights and Board policy.

At the conclusion of the sworn testimony, the Committee recessed to read and study the exhibits submitted by Mr. Corzo In light of the other evidence. It reconvened to deliberate, and to approve these findings, conclusions, and recommendations. A transcript of the testimony and exhibits was prepared for the committee's use, and the committee has had an opportunity to review it. The committee also considered proposed findings, conclusions, and recommendations submitted by the parties.

In my preliminary meeting with Mr. Bowers, I offered a lengthy explanation both verbally and in writing regarding all the allegations against me. I urge the Board to read a copy of that report to Mr. Bowers (exhibit 107). At the end of my presentation, I asked Mr. Bowers to contact me if he had any additional concerns or any doubts of my innocence. I also told Mr. Bowers very clearly that I was only given 2 business days to respond to a very grave set of accusations and I have had no time to prepare and explanation. Mr. Bowers never contacted me again. Instead, he proceeded to recommend my termination to the Chancellor without removing a single allegation. He did not even remove allegations that made me responsible for issues with the network at MCCCCD, an area of the department that I was not responsible for or trained to oversee.

The Committee takes administrative/judicial notice of: (1) MCCCCD rules, regulations, and official policy statements and guidelines; (2) the official minutes of Governing Board meetings In which presentations were made and/or documents submitted by Linda Brown, Rosie Lopez, and Beto Soto on behalf of Mr. Corzo and his colleague, Mr. Monsour, among others; and (3) the public statements, actions and recommendations of senior administration and the Governing Board, following the incident of 2013.

The Committee, having heard the testimony of the witnesses, read and considered the exhibits admitted into evidence, and heard the arguments presented by counsel, makes the following findings of fact and conclusions of law:

Findings of Fact and Conclusions of law

The Committee finds and concludes as follows:

A. THE PROCEEDING WAS CONDUCTED PROPERLY IN ACCORDANCE WITH APPLICABLE LAW AND POLICY

1. We find that Mr. Corzo was provided with sufficient notice of the charges and the hearing and was afforded a full and fair opportunity to participate in the hearing.

Not true. I was denied access to documents I needed for my defense, denied the opportunity to present witnesses, had my representative replaced without noticed and I was asked to return documents I had obtained via public records in the past prior to my hearing. I was clearly denied due process in a one-side, District-slanted hearing.

2. We find and conclude that each member of the committee is required to serve not as an advocate but as an impartial judge or juror. The record supports our conclusion that the Constitutional mandate for a hearing before an Impartial tribunal has been met. This would be true, even if the committee had decided to proceed with only a quorum of Its members present.

Not true. My representative views were not considered

3. We find and conclude that Section 15.2 of the MAT Policy Manual does not give the employee a right to choose a replacement hearing committee member after the committee has been formed, and that the law does not establish such a right independent of the MAT Policy Manual. We find that the seating of hearing committee member Kerry Mitchell, former MAT President, who previously represented Mr. Corzo in an employee grievance proceeding and advocated before the Governing Board on his behalf, is appropriate, lawful, and consistent with the requirements for disciplinary hearings under MAT Polley, which has been approved by the Governing Board. We find and conclude that there was no breach of contract or violation of Board policy involved in his seating.

4, We find that the refusal of Mr. Corzo and his counsel to participate in the hearing under these circumstances was not justified. The hearing was still Mr. Corzo's opportunity to confront and cross-examine the witnesses against him, to offer his own testimony under oath, and to persuade the hearing committee to accept his proposed findings and conclusions. He would not have waived his right to contest the procedural issues by such participation. We find and conclude

Not true. With all the defects identified about the hearing participating in it might have itself waived Mr. Corzo's right to a fair hearing. Moreover, the hearing might have been a ploy to obtain Mr. Corzo's testimony for use in other legal processes it may have intended to initiate against Mr. Corzo. We know of at least one case where after a hearing the District abandoned the hearing process and instituted other sanctions against the employee who had hired an attorney costing her a lot of money to represent her at the hearing thereby rendering the attorney's efforts a costly waste of time and money.

Without the specifics, cannot respond other than to say that the Chancellor and VC for IT had knowledge of the risk of another security breach. For the committee to deem this information irrelevant is incomprehensible.

that Mr. Corzo's failure to participate constitutes a knowing waiver of his right to a hearing and further appeal of the recommendation to dismiss him. Nonetheless, we find and conclude that the committee must complete its obligation to report to the Chancellor its findings,

There is no process allowing the appointment either. Again the committee failed to solicit another selection from us although there was plenty of time to do so. Further, it seems strange that the committee selected one of Mr. Corzo's witnesses as the replacement members who could speak to a variety of issues including the Chancellor's knowledge of and his failure to process the heretofore identified employee grievance.

conclusions, and recommendations so that he can complete the recommendation process in accordance with the MAT Policy Manual.

5. Mr. Corzo's unsworn statements and unattested documentary evidence were considered by the Committee notwithstanding his absence. District Administration introduced into evidence all of the exhibits provided by Mr. Corzo's counsel, some of which were separately produced by District Administration as part of its proof of the charges. Most notably, District Administration has produced Mr. Corzo's full statement to Mr. Bowers in response to the charges. District Administration stipulated for purposes of the Committee's consideration that any witnesses Mr. Corzo may have produced would have testified consistent with the exhibits designated by Mr. Corzo.

After the hearing, Mr. Galvan was afforded an opportunity to submit proposed findings and conclusions, and he did so.

Not true. We were not allowed to present our evidence. It is ludicrous to think that a MAJOR IT grievance played no role in the charges before the committee. This entire incident is about accountability at the top and about a condition that existed in ITS which ultimately led to the 2013 security incident. The organization is in denial and statements like this make it very clear that scapegoating of employees is what this organization and this committee is after. Every single member of this hearing committee was appointed by the Administration. This is against Board policy.

We submitted a very small subset of what should have been made available to us for our defense. The Administration refused to provide us with a single document prior to our hearing. Even documents that were readily available to us and the committee that had nothing to do with security of information were kept from us.

6. District Administration has contended that many of Mr. Corzo's exhibits have no relevance to these proceedings, and the Committee agrees. In particular, the Committee finds that any grievances, charges, complaints, or other disputes previously raised by Mr. Corzo played no role in the charges before the Committee and do not refute the charges as stated.

7. Mr. Corzo presented no witnesses before he left the hearing, and no witnesses appeared during the hearing other than those presented by District Administration. No one requested an opportunity to testify on Mr. Corzo's behalf during the testimonial session of the hearing.

*Not true. I was not allowed to use any of my witnesses. The District stated in writing * that I could only use witnesses they were providing. There were people willing to testify some gladly and others reluctantly (Dr. Glasper, Mr George K. etc). We had plenty of witnesses that if allowed would have testified to what truly happened in 2011 and 2013. Some of our witnesses were even willing to fly from out of town to provide testimony. These witnesses are still available and ready to talk to the Board if they are allowed.*

Mr. Corzo's witness were not only those in support of Mr. Corzo but others like Dr. Glasper, George K. and many other individuals who needed to be cross-examined under oath. The District denied us the opportunity to obtain testimony and interview critical witnesses for our defense. It is ludicrous for the hearing committee to predict testimony they have not heard and deny us the opportunity to interview witnesses with the pretext that this witnesses would have testified consistent with the exhibits we present. In addition, the exhibits we presented were only a small subset of what we intended to present once public records were made available. This is again another violation of Board policy.

8. We find and conclude that the hearing was conducted in compliance with the terms of the Manual and in compliance with all legal requirements.

Not true. There were multiple policy violations as mention throughout this document.

9. We also find and conclude that Mr. Corzo failed to establish grounds to reschedule the

Not true. The grounds to reschedule the hearing was MCCCCD unwillingness to provide us with "ANY" documents before the hearing, confidential or not. The ground for an extension was the fact that there was Court Complaint filed by G&K to resolve the issue of public records. We requested a delay until a judge decided if/when records requests should be provided by MCCCCD. Eventually, the judge ruled in favor of those requesting records and set a schedule for MCCCCD to provide public records. It is only now, 6 months later, that I am being allowed to review the records that I needed for my defense.

Our grounds were simple. We made a record request to defend ourselves and the District failed to provide a single document prior to our hearing. This includes documents like the ITS Oversight Report or the ITS grievance that were readily available. This proves malfeasance in the part of the District and an attempt to deny Mr. Corzo with due process.

hearing to another date, and we affirm the Chair's decision and rationale as described above.

B. STANDARDS OF PERFORMANCE PROVIDED TO MR. CORZO IN WRITING REQUIRED HIM TO MANAGE HIS AN IN COLLABORATION WITH OTHERS SO AS TO SECURE AND PROTECT THE DATA IT CONTAINED, AND TO PROPERLY IDENTIFY AND MANAGE RIS(S RELATED TO THAT DATA.

10. Governing Board-approved employees who have successfully completed their initial probationary period may only be disciplined for just cause as provided in the Staff Policy Manual. Under the "just cause" standard, any discipline recommended for a Board-approved employee must meet the following criteria: (1) The employee knew or reasonably should have known that the employee's conduct could lead to disciplinary action; (2) The disciplinary action is the result of job performance, violation of law, violation of established MCCCCD policy or procedure, and/or a violation of established college/division/department policy or procedure; (3) Management conducted a fair and objective investigation in accordance with MCCCCD policy and the law; (4) The investigation produced sufficient evidence or proof to reasonably support

the failure of performance or violation as alleged; (5) The disciplinary action taken was consistent with disciplinary action for similar or comparable conduct or was otherwise reasonable under the circumstances. [MCCCD Exhibit 5, MCCCD Policy C-4(C)(S)] Management, Administrative & Technological ("MAT") policies apply a "for cause" standard that is consistent with the "just cause" standard. [MCCCD Exhibit 6, MCCCD MAT Policy 15.2) We find that all of these criteria are satisfied in this case.

11. Employees are notified of their expected job performance and the penalties for unacceptable conduct through training, policies, counseling, and other measures, [MCCCD Exhibit 5, MCCCD Policy C-4(C)(3)]. The job duties in question here are based on job descriptions, policies, and directives that pre-date the conduct in question.

12. Violations of generally expected job performance standards and specific rules of conduct are grouped into three separate categories by type of offense: Conduct, Performance, and Attendance. Each of these offenses is separated into two groups based on the seriousness of the offense: Group One (more serious) and Group Two (less serious). [MCCCD Exhibit 5, MCCCD Policy C-1.J.(C)(4)(a)]

13. Examples of the categories and groups of offenses are provided in Policy A-4. [MCCCD Exhibit 7] Mr. Corzo was charged with "willful and intentional failure to perform job duties that were communicated to the employee and are within the scope of employment." This is a Group One Performance-based offense. Although recently consolidated with other policies, this Governing Board-approved standard long pre-dates any of the acts and omissions that serve as the basis for the charge,

Not true. See above regarding a new policy (C-4) used to recommend my termination and being applied retroactively. This is a breach of contract that existed back in 2011 when this policy was not in effect. I was not present or responsible for any of the systems compromised in 2013.

14. Multiple policy infractions which are closely related in time, even 'if unrelated or in different groups, may be combined to result in corrective action which is more or less than the severity of the total-sum of the separate offenses. [MCCCD Exhibit 5, MCCCD Policy C-4{C}(7)(d)]

15. Group One performance-based offenses are corrected under a progressive corrective action schedule and a first offense may result in "any disciplinary action, including dismissal." [MCCCD Exhibit 5, MCCCD Policy C-4{C}{4}(b)]

MCCCD created a new policy (C-4) in 2013, shortly after the security incident and is now applying it retroactively to severely punished employees for past non-performance. This is similar to establishing a new law that states that killing of cows is now punishable by the law and going back in time to punish anyone who had broken the law. This new policy did not exist in 2011 and employees were operating under a different employee manual and set of rules/policy. Are all new policies approved by the Board now allowed to be retroactively applied? Are employee actions today subject to all future policies?

I am innocent of everything I am being accused of, however, the Board must understand that this organization has done everything possible to create new laws to allow them to scapegoat employees and avoid accountability. Use of policy C-4 for an event that took place prior to this policy being in effect represents a breach of contract.

16. Maricopa Governance Policy Manual section 6.16- Public Stewardship and Ethics: "The Governing Board of the Maricopa Community College District recognizes the responsibility to demonstrate ethical and professional conduct. In order to demonstrate this commitment to public trust and accountability to the communities the District serves, all Governing Board Members and all employees shall be required to participate in training that focuses on public stewardship and 'institutional ethics. All MCCCD employees, Including those assigned positions

classified as Management, Administrative and Technological (MAT), are required to complete the training annually and certify their completion of the training." [MCCCD Exhibit 8] This policy also predates any of the acts and omissions that serve as the basis for the charge against Mr. Corzo.

17. Section 6.12 of the Online Policy Manual, under the heading "Management Responsibility," mandates that MCCCD managers (specifically defined to include all MAT employees) are charged with the responsibility for "establishing a system of internal controls, risk management and organizational processes over the operations of MCCCD in a manner which provides the MCCCD Governing Board reasonable assurance that:

- A. Risks are appropriately identified and managed.
- B. Interaction with the various organizational groups occurs as needed.
- C. Significant financial, managerial, operational information is accurate, reliable and timely.
- D. Employees' actions are in compliance with policies, standards, procedures and applicable laws and regulations.
- E. Resources are acquired economically, used efficiently and protected. F. Programs, plans and objectives are achieved.
- G. Significant legislative or regulatory issues impacting MCCCD are recognized and addressed appropriately." [MCCCD Exhibit 8]

18. The Online Policy Manual further provides that the "system of Internal controls over the operations is a function of management and is an integral part of the overall process of managing operations. As such, it is the responsibility of managers at all levels of the organization to:

- A. Identify and evaluate the exposures to loss which relate to their operations.

B. Specify and establish plans and operating standards, procedures, systems, and other disciplines to be used to minimize, mitigate and/or limit the risks associated with the exposures identified.

C. Establish practical systems of internal control processes that require and encourage employees to carry out their duties and responsibilities in a manner that achieves the seven (7) control objectives outlined in the preceding paragraph.

D. Maintain the effectiveness of the systems of internal control processes that they are responsible for." [MCCCD Exhibit 8]

19. In 2007, the Office of the CIO for MCCCD published a statement of which we take notice, the Best Practices for Data Security, Acceptable Use, and Access Management. It states, "All employees and agents of MCCCD and anyone working on behalf of MCCCD are charged with the protection of MCCCD data."

In September 2010, ITS published "IT Operational Principles" stating, "If Maricopa is to be truly successful in achieving its information and instructional technology Vision and accomplishing its IT strategic objectives, it is not sufficient to do things right; Maricopa must do the right things. ITS stated seven principles n ... to help ensure that everyone involved in the delivery of information and instructional technology solutions, as well as those served by Information and instructional technology within MCCCD share a common understanding of the role and mission of information and instructional technology in achieving Maricopa's future:

Information Technology

- Facilitates strategic usage of technology to enhance teaching and learning
- Delivers technology to support efficient, effective, and secure operations across the district
- Collaborates with internal and external customers to understand and respond to their needs
- Plans In a responsible manner which includes effective use of resources and specific performance measures
- Makes decisions that are
 - o Clear and concise
 - o Aligned with our strategic plans

o Reflective of broad participation and accountability o Defined by a shared governance structure

- Adapts to meet the evolving needs of the District

- Balances innovation with operational activities to meet the changing needs of our customers

We take notice of these statements as well.

At all relevant times, these performance standards applied to Mr. Corzo, and they were provided to him in writing. Mr. Corzo acknowledged his understanding and agreement to meet these standards by affirming during the relevant time period: 111 will fulfill my responsibility for internal controls, risk management and organizational processes in a manner which provides the MCCCDC Governing Board reasonable assurance that risks are appropriately identified and managed."

20. At all relevant times, Mr. Corzo's job description provided, in pertinent part:

"Job Summary: Plans, Directs, and Administers the Database Administration team and assures there is effective database support for multiple database applications. Assists in making strategic decisions relating to enterprise database technology, design, and management."

"Representative Duties: ... develops, designs, refines and/or implements integrated database systems; researches, tests and supervises implementation of innovative database technologies; participates in budget preparation, monitoring, needs assessment and procurement; confers with users and implements-procedures, methods, technical concerns and budgets; fosters the professional Development of assigned staff ... "

"Knowledge and Abilities: Knowledge of enterprise database architectures; enterprise database management systems currently used and supported; latest database design and management tools; database security; ... principles and practices of management and leadership."

C. THE CHARGES AGAINST MR. CORZO ARE SUPPORTED BY A PREPONDERANCE OF THE EVIDENCE.

21. In its essence, the charge against Mr. Corzo is this: that the above job responsibilities were communicated to him in writing, and that his conduct leading up to and following the 2011 incident constituted a willful failure to perform those responsibilities.

The only mention of security in this document refers to database security. There was absolutely nothing wrong with the security of the SIS database in 2011. The only security problem was with the servers supporting the main Maricopa webservers. The security of the webservers is completely different that security of SIS databases. The security of these servers were under the control of another ITS Director not Mr. Corzo.

55

In addition, database that were under the control of the Marketing Department were residing on the main Maricopa webservers. The security of these database was the responsibility of the marketing department and another Director in ITS not Mr. Corzo.

Not true. The organization has recognized my commitment for MCCCCD before and after the 2011 incident by awarding my teams multiple innovations of the Year awards for their contributions to the organization. All my employee evaluation in nearly 30 years with the institutions reflect that I have been performing at or above the standard at the time. Never in my career at MCCCCD have I've been told that I was failing to perform my responsibilities. That responsibility rested with my supervisors. Had I been told that, I would have initiated corrective actions or MCCCCD would have done so for me as it is customary. If this statement was true it would constitute a failure of my supervisor to monitor and assess my performance as required by MCCCCD.

The factual allegations are that before the 2011 incident, Mr. Corzo failed to do his job with respect to data security: that is, to work in collaboration with the other members of the IT leadership. As a result the personal data of individuals that was entrusted to his care was exposed to unauthorized access. The District Administration 'claims Mr. Corzo turned a blind eye to the lack of security of the data he managed both before and after January, 2011, failing to identify and manage this risk effectively so as to protect the information in his care. In this, he was one point of failure among several, but the District asserts that he bears responsibility for his part in allowing these conditions to develop and continue to exist. When the 2011 investigation by Stach and Liu revealed to Mr. Corzo (among others) explicitly that his

Not true. Mr. George K. setup the department so those responsible for the webservers had the staff and training necessary to support that technology and those responsible for the ERP databases we staffed and trained accordingly. I collaborated in many projects in ITS during my career. Many of these projects were done in conjunction with college IT people like CIMS and others in cooperation with members of the ITS leadership and there were other tasks done by individuals as part of their job. The responsibility of protecting the main Maricopa webservers relied with another Director of ITS. My staff was neither trained nor had access to these servers. My staff collaborated constantly with other member of the IT leadership, attended weekly meetings, and coordinated many efforts over the years. The breach of 2013 was a direct result of a breach in 2011 that was not corrected for nearly 2 years. I communicated my concerns to the District Executive Leadership many time in 2012. Those responsible for implementing changes simply did not follow through. This had nothing to do with collaboration with members of the IT Leadership. A job had to be done to secure MCCCCD and it was not done.

, tie failed to alert

Not true. The databases I was responsible for in 2011 according to my job description were secure and never compromised in the 2011 incident. There was no willful failure to perform my responsibility because I was not responsible for the systems that were compromise. I urge the Board to ask questions and contact people like Margin Gang, John Webster and others that could testify to this regard. This is a critical concept because either investigators do not understand who did what in MCCCCD or there is a willful attempt at scapegoating Mr. Corzo.

Not true. I never turned a blind eye on any of the security issues at MCCCCD. I engaged Microsoft every year to do a security assessment of our identity management system (CIMS). I conducted daily audits of the security for the systems I was responsible for. When I learned of the delays in the fixes that had to be put in place, I sent filed a grievance. The responsibility to follow-up with the fixes was not mine. The responsibility to implement the security issues that were found in 2011 was not mine. Had that responsibility been assigned to me the outcome would have been different. The job of pointing out security risks was not officially and it was my understanding that all risks had been clearly pointed out to Mr. Kahkejian in the ITS Security Oversight Report. I urge the Board to look at this report. Mr. Monsour make every effort to both identify the fixes and get those in the department responsible for the corrections to do their job. None of the fixes had to do with my teams. There was little more I could do other than wait and then file a grievance to alert the Chancellor. Never in my entire career have I turned a blind eye on security. As the Director over ERPs, security was my number one priority. As a Director over CIMS, the MCCCCD identity management system, security was my number one priority. None of these systems were ever compromised while I was in charge and responsible for day to day operations. What happened to MCCCCD is very unfortunate but I had nothing to do with it.

LASTLY, and more importantly, Mr. George K or others in the department who were privileged to the Stach and Liu report never shared it with me. The Stach and Liu report of 2011 appears to be nothing more than a high-level 8-9 page Powerpoint presentation pointing to problems with MCCCCD webservers and the code and databases residing there. Again, none of this technology was my responsibility.

executive level leadership to that fact. Again, he was allegedly one point of failure among many, but he is charged with responsibility for his part. Among other senior leaders who were aware that the-

..... after 2011 his failure to communicate accurate, complete, reliable and timely information to executive leadership allegedly allowed executive leaders and the community to believe that a thorough investigation had revealed only a limited intrusion that had been effectively

addressed, and although steps would be taken to prevent future-here was no urgent need to act. In fact, Mr. Corzo and others knew that the and everyone's data was exposed. By analogy, the charge is that he and others advocated that steps be taken to prevent a burglary when he knew the house had already been broken into and ransacked on his watch. By protecting his job in this way, he deprived senior management and the Governing Board of the crucial information that came forward in 2013 -that the personal data of millions of individuals was actually exposed to unauthorized access and that immediate and effective action was required to protect them.

For the following reasons, we find and conclude that the charge, that Mr. Corzo engaged in willful and intentional failure to perform job duties within the scope of his employment that were

Not true. No data other than that for 300 or so individuals was exposed in 2011. An oversight report was developed by Mr. Monsour and presented to the VC of IT. Mr Corzo did not participate in the creation of this report and there were no action items in this report for Mr. Corzo's attention. This report was created independently by Mr. Monsour as it was the desire of Mr. Kahjkejian. It is my understanding that this report was given to George K. and next steps identified. Mr. George K. was in the loop as documentation and emails reveal. I had no knowledge of any SIS data being exposed. There was no indication that anything like that took place in 2011. The house had not been ransacked under my watch. This is consistent with the report from Mr. Monsour as to the state of affairs in 2011. I was not privileged to any additional information or conversations with the FBI at that time. My job was to make sure that SIS was not compromised and checks of the system at the time revealed that nothing had been taken even though the house (Maricopa webservers) was broken into. The Database for SIS reside in a completely different set of servers and were protected by firewall and other access methods that made it much harder for people to break into them. Senior Management was not deprived of anything. Letters were sent to the Administration, a grievance file and communication with the VC of IT took place.

communicated to him, is supported by a preponderance of the evidence, This is a Category One performance-based offense that justifies immediate dismissal without progressive discipline.

21. SUMMARY OF THE TESTIMONY

Mr. Corzo's position as we understand it is as stated in bold below. Evidence and findings addressing each statement follows in plain text.

"These accusations deal with security and - in Maricopa, areas I have never been responsible for (and for which I received no training)"

Not true. I have never been disciplined in my entire career at MCCCCD and my performance evaluations show an employee consistently performing at or above standards. I never engaged in willful or intentionally failed to perform any job duties. There is no document to attest to that in the form of supervisor evaluations or comments. The feedback from the VC of IT in 2011 is that I was doing an excellent job as document via email available upon request. I object to this action and ask the Board to continue the investigation and allow me to testify, review public documents and present witnesses.

The evidence supports the committee's finding to the contrary. In a November 15, 2010 memorandum, Mr. Corzo described one of his goals for 2011 as placing "heavy focus on security around

- [MCCCCD Exhibit 10]. Mr. Corzo also was designated to respond to security issues by the

I was assigned once by Mr. Monsour to take care of things for him while he was out b/c the person responsible to be his backup was also out.

The ITS organization is very complex and there is a huge misunderstanding about security and who does what and who was responsible for what in this report. I don't expect the hearing committee to understand all of this but I do hope that I am given an opportunity to explain.

The main Maricopa webservers were compromised in 2011. There were database residing on these webservers. Mr. Corzo was not responsible for the security of these servers or the database residing on it.

security director, Mr. Earl Monsour, when they were out of the office. [MCCCCD Exhibit 11].

Moreover, -

••• was not the cause of the 2011 incident. Mr. Liu's testimony was that although he found in 2011

W&Js also lacking, " ... no amount of

could have prevented (the

The hearing committee clearly does not understand roles and responsibilities in ITS and how security works. There are several layers of security in ITS depending on the application. As organized by Mr. Kahkejian the responsibility for operational security was divided among members of the department. While this is not ideal, it is the way Mr. Kahkejian wanted it. There is application security, database security and operating system security. In MCCCCD, Mr. Corzo was responsible for database security. Mr. Creswell dealt with application security and Mr. Marten had responsibility for server and operating system security. The first layer of security was Mr. Marten's responsibility – server and operating system, the door to the house. The second layer of security is Mr. Corzo's responsibility - databases, the room in the house. That said and again as desired by the VC of IT, Mr. Corzo did not have responsibility for ALL the database and their related security at MCCCCD. The third layer of security was Mr. Creswell, what you can do in a room. If you break into the house, there is little or nothing that can be done over time to keep the thieves from stealing. What happened in 2011 is that the thieves broke into the house and the lock was never fixed. They stayed in the house until something major happened in 2013. Mr. Monsour tried to get those responsible for the entry door to fix things but it never happened.

•••••••••• Moreover, "If you'd even taken just like five minutes to see how it was set up, you can see how (the data) was not being well maintained, it was not being well taken care of." "(If I were a database manager responsible for security of the data) I would never have allowed it to be placed (where it was) in the first place because it's....."

There is so much being redacted that I am unable to defend this statement.

(Paraphrases in parenthesis)

Both Mr. Liu and Mr. Caouette stressed that data security is a critical function of a database administrator; that security requires a team effort; and that Mr. Corzo was clearly a member of that team- It cannot be maintained by people who see themselves as working in silos. The committee believes that this is an obvious application of a major principle of management and leadership In Maricopa that Mr. Corzo was responsible to know and follow.

I would have never allowed that to happen either, however the webserver at MCCCCD and the databases residing on it were not my responsibility as assigned by Mr. Kahkejian. These databases use software that my staff was not trained to support. We had no idea how they were being configured. I was not the database manager over this system. This were the property of the Marketing Department and their staff maintained them.

The IT Organizational Principles and Best Practices documents support this finding.

My teams supported a piece of a big puzzle in ITS. We supported the databases, authentication and enterprise reporting. We worked in collaboration with everyone at both the District and the Colleges. There was no way in the world that our ERP systems would have operated for years without that level of collaboration. This statement is ludicrous. The Board should simply look at all the awards my teams received for collaborating in projects with other members of the department and the colleges.

Testimony of all witnesses supported by MCCC documents referenced above supports the committee's finding that working with others to assure proper.....

The witness provided were those in support of the District's testimony only. They were merely consultant who while highly respected in industry had spent only a few months looking at a very complex set of technologies that has been in place for years. The true experts were the witnesses I had planned to present, some of them still working at MCCC and others who had left the system. These were people intimately familiar with MCCC systems.

..... it served so that it would protect the data was among Mr. Corzo's

specific security responsibilities as a member of the leadership team.

uding.....

"Security for Maricopa systems,

..... was

Not my responsibility."

incl

Mr. Corzo's job description at all relevant times included specific responsibility for management best practices and security of the databases. As such, and as a member of a team assigned to deliver secure IT services across the District through decisions that reflected broad participation and accountability, he was responsible for assuring the secure configuration, administration and maintenance of the databases he managed - including assuring the use of strong passwords.

Security is the responsibility of all IT staff, working as a team through shared governance and sound planning, and as a senior leader of the IT staff Mr. Corzo had significant responsibilities in this area to communicate and coordinate with other members of the management team to assure that personal data was adequately protected as it Mr. Corzo's list of accomplishments and goals (District Exhibit 10) clearly indicates that his duties were not nearly so narrow and ministerial as he claims: they encompass

This is again a matter of understanding how things work. In addition to the databases at MCCCCD, I was also responsible for CIMS, our identity management system still in use at MCCCCD. This system is still being used today to gain access to all our Enterprise Applications. It provides usernames and password used to access most MCCCCD and college systems. Any time there was a problem dealing with security, Mr. Monsour referred people to me, that is correct. However, that referral was meant to solve issues related to CIMS most of the time and dealing with end-user access to our systems. It WAS NOT security issues dealing with the configuration and access to the Maricopa web servers that were compromised. Neither I nor my staff had the knowledge and training to manage the security on these servers. I am glad to meet with the Governing Board to answer any questions. My security responsibilities are not clearly understood by either member of the hearing committee or the investigators. I can see how they could be confused and think that I was responsible for security at MCCCCD when indeed I was not. Please allow me the opportunity to explain or answer any of your questions.

responsibilities including security, according to witness testimony and supporting documents. Indeed, Mr. Earl Monsour, identified in the record as the Vice Chancellor's "security officer," referred all questions on security issues to Mr. Corzo in his absence.

Mr. Corzo was the first person Mr. Monsour contacted for assistance when notified of the 2011

I agree. The passwords in our database were very strong both for our administrators and end-users as implemented in CIMS via LDAP authentication.

FBI report. See testimony of Liu, beginning on page 66 of the transcript, and testimony of Caouette beginning on page 121]]

"There were no security breaches of the ••••• during the 2011 incident"

According to the witnesses, Mr. Corzo ignores the fact that his was listed for sale (District Exhibit 12), and he argues for a compartmentalized, ministerial view of his duties.

I was never involved with the FBI. I was never told that the SIS database was listed for sale. The only thing that was found to be exposed in 2011 were approximately 300 users that did not come from the SIS database. That was the conclusion of the 2011 investigation and the message sent by Mr. Kahkejian to MCCCCD. That was my only understanding as well. The fact that someone claims to have a database for sale does not mean that the database was indeed stolen. I was told that this was not the case in 2011. My staff confirmed that there was not unauthorized access to SIS or any of the ERP systems in 2011. I do not argue for a compartmentalized view of my duties. I am simply stating that my duties did not involve the security and configuration of the data that was stolen in 2011.

Not true. The data that was breach came from a database residing in the main Maricopa webservers. That database was the responsibility of the marketing department and another ITS Director. My staff participated in the 2011 investigation and was part of a team working together to assess the situation and provide remediation services. It is hard for me to decipher what is being said here as it is heavily redacted.

He fails to account for his leadership role, working as a team member to design, administer, and maintain systems that protect data. While It is true that his and that Stach and Liu made no finding that the was breached, the witnesses believe his argument is untenable. Testimony of the witnesses showed that Mr. Corzo was a part of the team that worked directly with Stach and Liu in 2011.

I believe that is true. Mr. Monsour wanted to know if the SIS database had been compromised.

It was data from his [redacted] that was reported to be exposed and the compromise of data from his [redacted] was the principal original focus of the investigation by Stach and Liu, which was restricted from examining his [redacted]. Security can only be accomplished by people working as a team.

Among others, Mr. Corzo was responsible for assuring the security of his data as it He was informed directly of the firm's findings about the security of the data from his [redacted] which included: "Everything was on the-- everything was on the same [redacted]. There was so much information contained within [redacted] [redacted] they were so [redacted] you know that they were compromised. We have evidence that the entire- [redacted] was compromised ... we are talking in the order of over a thousand instances of issues [redacted] [redacted] on that- ... it was about as bad as it could get.," "It was clear that the folks with

Not true. My staff worked with every team in the District and many in the colleges to implement and protect many systems. If anything, this statement shows that I collaborated with the investigation of 2011 and that the Stach and Liu report made no finding that the ERP SIS database was breached. I did not work directly with Stach and Liu. I attended a meeting in 2011 where work to be done in the Maricopa web servers was outlined and that was the extent of my personal engagement with Stach and Liu as far as I can remember. Work was assigned to a Director in ITS to fix the servers compromised and little or nothing was assigned to my staff. We changed passwords as a precaution and proceeded to assist with the investigation. I was asked to nominate a highly technical member of my team to assist and I did so. I worked with this individual to make sure that all ERPs database were protected and all work was done as requested.

hands on the keyboards had no knowledge about what to do in response or even the hardening of the

- In every possible aspect, the- the- the- none of it was being taken care of." "There was no security program. Period." "One of the biggest challenges was that there were no

•.. just basic, basic computer administration, is having so you know what's going on in ." In response to a committee question as to the magnitude of the security problem he found in 2011 analogized to the stages of a house fire, Mr. Liu stated, "I think the building has burned down at that point, okay? And everyone was kind of looking the other way ... the message we delivered was that there was evidence of everything." After Stach and Liu made these preliminary findings, they were prevented from examining Mr. Corzo's even though his was reportedly for sale. There is no evidence that Mr. Corzo pressed Mr. Monsour for an investigation of the condition of his- to determine the extent to which it was compromised and get security experts' recommendations about it.

It is nearly impossible to decipher what's being said here.

Mr. Monsour lead a comprehensive investigation into the breach.

It was determined that the SIS data was not compromised.

Mr. Monsour planned among other things to do a comprehensive security assessment of ITS.

The plans for this effort did not materialize.

Mr. Corzo brought in experts from Microsoft to do security assessments of CIMS, two years in a row. This was MCCCCD identity management system. Later in 2013, it is my understanding that John Webster also requested another security assessment of CIMS and little or nothing was found to be a problem.

I never prevented anyone from examining any of the databases I was responsible for. Mr. Monsour had full authority over the investigation to do and go wherever necessary. There is absolutely no evidence that I kept anyone from investigating or accessing any of our systems. Access to these systems is yet another area that the hearing committee and the investigators needs to understand. The computers where the databases for SIS resided on were not managed by Mr. Corzo's team but by another ITS Director. Access to these computers was granted by Rod Marten's team not Mr. Corzo. Mr. Corzo only managed the databases residing on these computers not the computers themselves. If anyone ever prevented the investigators from accessing these computers it was not Mr. Corzo as he had no authority or access to do so and neither did his staff.

"Maricopa was made aware of risks in 2011 by the report Earl M. shared with George 1<. Maricopa was made aware of all the risks associated with the 2011 (incident) in the Grievance complaint filed by several members of ITS in 2012 (see attached)" I followed processes to bring important matters like the 2011 incident to Maricopa's attention and avoid both the 2013 Incident and many others that followed."

This grievance was crystal clear. Its purpose was to bring multiple items, not just the reorganization of ITS to the attention of the Chancellor. It called for an external investigation by a mutually agreeable 3rd party. The grievance was ignored and dismissed. In the process of doing that, MCCCCD violated their own policy when it comes to timelines to respond to a grievance. This was so blatant that the Chancellor held to this grievance for nearly two years and to this date has not responded to it as acknowledge as recently as Jan, 2014. According to the MAT policy manual the following policy violations took place.

Level III – Chancellor.

i. Within 10 days of the reply at Level II, or if no reply is received, within 20 days after the submission at Level II, the grievant may submit the grievance, using the District's grievance form, to the Chancellor.

d. Level III – Chancellor.

i. Within 10 days of the reply at Level II, or if no reply is received, within 20 days after the submission at Level II, **the grievant may submit the grievance, using the District's grievance form, to the Chancellor.ii. The Chancellor may hold a meeting to discuss the grievance within 15 days after receipt. The Chancellor shall reply in writing to the grievant within 15 days after the meeting.**

iii. If the grievant is not satisfied with the written answer of the Chancellor, the grievance may be submitted to Level IV of the grievance procedure.

e. Level IV – Governing Board.

- i. **Within 10 days of the reply at Level III, or if no reply is received, within 20 days after the submission at Level III, the grievant may submit the grievance, using the District's grievance form, to the Governing Board.**
 - ii. The Governing Board may, at its option, review the evidence and issue a final written decision within 30 days after receipt. The written decision shall be forwarded to the grievant.
 - iii. The Governing Board's decision shall be final and binding. If the Governing Board elects not to consider the grievance, the decision of the Chancellor at Level III shall be final and binding.
-

Mr. Corzo appears to be referring first to steps that he and others took in response to a reorganization of District IT staff that Mr. Kahkedgian announced in Spring 2012. However, this

Not true. The Chancellor was told that a security oversight report existed and that corrective actions had not taken place leaving MCCCCD at risk. The Board should obtain a full copy of that report. The condition and the risks to MCCCCD are clearly spelled out in both the ITS grievance and the Security Oversight Report

response was not a clear call for action on data security, made necessary because millions of people's data was at that very moment exposed to unauthorized access because the system that included his ●●●

was Their unaddressed letter of complaint dated June 25, 2012 (Appellant's Exhibit 13C) does not address security. It complains the personnel actions affecting them are unfair and discriminatory. It makes no reference to the 2011 incident or to data security in general. Nor does the undated request of Mr. Mitchell and Ms. Quiroz (Exhibit 98). The single focus of all the requests directed to the Chancellor, whether by Mr. Corzo or others, is the adverse effect of the reorganization on personnel. The only request for action by the Chancellor is that the personnel decisions made in the reorganization be postponed or reversed and that the "work environment" be investigated. In a ten page statement in support of the personnel grievance submitted on his behalf, a single short paragraph mentions that among many other alleged shortcomings, Mr. Kahkedgian allegedly ignored a "security oversight report" submitted a few months earlier, representing a "high risk that could expose

Not true. That report contains several paragraphs stating high risk, high impact if security issues continue to go unresolved. The grievance report was truly a call to action on the Chancellor's part to investigate many things in addition to the reorganization.

personal information." The grievance suggests there are security risks to be managed: It does not convey that the data is actually exposed and the Institution ●●●●●●●●●●

The intent of the grievance was to restore the positions Mr. Corzo and Mr. Monsour (among others) had lost through reorganization. The nature and extent of the information available to the Chancellor through the grievance statement and other statements about working conditions in IT contrasts sharply with the information the Chancellor received and acted upon in 2013, when he acted decisively to assure a thorough investigation and make data security and protection of individuals the top priority for MCCCCD. Mr. Corzo has offered no evidence that he told the Chancellor or anyone else the true condition of data security as described to him by Stach and Liu in 2011, and the disingenuous grievance statement

about security "risks" undermines any sentiment to give the benefit of the doubt on that subject. Mr. Liu testified that in 2011, his investigation was cut short ("... they started very quickly putting boxes around what we were looking at...if you really wanted to find out what the problem was, you would not run an investigation this way.") and his requests to speak directly with the Vice Chancellor were ignored. He was not surprised that there was a second identical report in 2013. That year, Mr. Liu found the same conditions he found before. However, with different people in charge of IT in 2013 Liu's treatment was very different. He was allowed not only speak with CIO Webster and Security Officer Williams, but also the Chancellor himself. In contrast to Mr. Monsour and Mr. Corzo, "They treated it like it was a real issue and ... the attitude was much more receptive to wanting to solve and remediate the issue." Mr. Liu testified that the Chancellor was taken aback that the conditions Stach and Liu found in 2013 had existed for several years. "He had no idea how bad it was until 2013.¹¹ When asked why he would not know, Mr. Liu stated, "... we knew in 2011, the behavior of the team was unusual, and we just assumed it was because there was CYA going on." This, in reference to the MCCC managers who prevented Stach and Uu from examining the - containing the that was advertised for sale.

Not true. I had absolutely nothing to do with the way Mr. Liu was treated. He dealt directly with Rod Marten and other directors in the department. I never prevented Mr. Liu from accessing any of the systems I was responsible for or treated him disrespectfully. I never utter such words to Mr. Liu. I could not have kept him from accessing anything even if I wanted to. The authorization to access servers in ITS was not granted by my department. I did not know that he was denied access to the VC of ITS but I do know that historically the VC of ITS has refused to speak to vendors. There was not CYA going on at all with my teams. I urge the Board to find any information or witnesses that will testify that I tried to prevent Mr. Liu from doing anything. I met Mr. Liu once and he went on to work with Mr. Marten, Mr. Monsour and Mr. Martin at the time. The comments mentioned above did not come from me.

22. Information was provided to the committee that other ITS employees similarly situated, who were found by Mr. Caouette to have engaged in acts and omissions that the Chancellor VCHR believed were a failure to perform to the above standards, have similarly been charged and recommended for dismissal. We make no findings on the merits of those charges, but we note that three of the five who were recommended for termination have resigned, and that all who have resigned are peers of Mr. Corzo- Direct reports to the VCIT at the relevant times, with team responsibilities for data security. As Mr. Liu testified, in 2011 he found several points of failure. The sole question before the Committee is whether the evidence supports a conclusion that Mr. Corzo was one of those points of failure. Our decision is not contingent on the outcome of the other personnel actions.

23. The Committee finds and concludes that we need not find Mr. Corzo solely responsible, or even primarily responsible, for the 2011 incident or the subsequent failure of others to meet the above standards, In order to uphold the charges against him.

24. Based on the evidence, the Committee finds that MCCCCD has proven facts sufficient to support the charges against Mr. Corzo. After evaluating the evidence, the Committee concludes that Mr. Corzo's denial of having any responsibility to protect personal data on any- other than when it resides in his and that there was no breach of his lacks credibility and misses the point of the charge. The Committee concludes that Mr. Corzo had security responsibilities in his role as the- data administrator and in his role as the administrator; that the data and the ••• were completely unprotected because ••• among other things; and that Mr. Corzo failed to report these facts to executive leadership even after he was expressly informed. [MCCCCD Exhibit 12, at 50-51]

To this date, I am yet to examine any evidence supporting the findings. To this date, I have been denied the opportunity to defend myself, provide expert witness testimony and present evidence from public records request.

I am unable to defend myself against exhibits presented here. I was not provided with access to those exhibits. I was never told that SIS data or any other data I was responsible was completely unprotected. Nothing could be further from the truth.

It is important to understand how hackers broke into the system and who was responsible for keeping these hackers out. My responsibilities did not allow me to protect the ERP databases once hacker broke into the webservers. The security of our network and the security of the servers where our database reside was the responsibility of another ITS Director. This does not mean that I worked in isolation but it does mean that for my systems to be protected others had to be doing their job. This is the way Mr. Kahkejian organized the department.

This coincides with the recorded statement from Kroll that "I did nothing wrong". For a person who wasn't solely responsible or even primarily responsible or even yet not responsible at all, the recommendation for termination seems to be excessive.

I was asked to attend a meeting in 2013 with very short notice and no indication of what the meeting was about. I was superficially involved in the 2011 incident and completely unaware of the details of the 2013 incident other than what was disclosed to the MCCCCD community. The Chancellor and others in the leadership of ITS decided not to involve me or tap into my expertise to investigate the 2013 incident. I was basically sidelined and my input and expertise was never requested. My job at the time was to do research and development for John Webster. I can understand Mr. Caouette reaction but other than what was reported in the grievance, I was pretty much unaware of what ITS was doing in 2013. I was sidelined by the MCCCCD leadership after filing the grievance and the EEOC charges against MCCCCD. I told Mr. Caouttee what I knew at the time. I also gave him the names of the people he should contact for additional details (Martin Gang and Joyce McQueen). I told the investigator that I would like to go back to my email and document to review. I also told them that I would be glad to interview with them again. They never called me back. They never called any of the individuals I gave them as a reference. One of them was my appointee to the 2011 investigative team. The document that have been provided to date where documents that I either obtained from Mr. Monsour or found after searching through the 2011 emails.

25. · Mr. Corzo gave an example of his attitude in the investigation, when he initially denied to Mr. Caouette having any knowledge of the 2011 Incident. Mr. Caouette testified that he was shocked: the overwhelming evidence, including documentation that Mr. Corzo himself has provided, establishes that Mr. Corzo was aware that his [redacted] was reported for sale: he was also aware of the breach

Not true. I reported these facts to the leadership in multiple letters, the grievance and other documents. Mr. Monsour did the same. It is nearly impossible for me to decipher the accusations here due to redaction, however, I can only be responsible for what I am being assigned responsibility for. I have always try to collaborate and assist others, however, ultimately, they need to do their job as part of a team. I had no security responsibility for the marketing database that was breach in 2011. I was not the database administrator at that time and technically in 2011, I was a Director of Strategic Information Technology not a database administrator

investigation and Stach and Liu's finding that the- data he managed was
- He was one of the first people informed about the 2011 incident. He participated as a member of the internal investigation team and knew the results of the Investigation; that the.....
- were that there was and that all the data was exposed. Mr. Monsour would not allow Stach and Llu to examine the- containing Mr. Corzo's and there is no evidence that Mr. Corzo demanded such an examination to be sure his was not compromised as had been reported.

With respect to Mr. Monsour's action or inaction, there is no credible evidence that the draft documents in his name, submitted to the committee as Appellant's Exhibits 2 and 3, were created contemporaneously with the events in question, that they were reduced to final and

Not true. I was contacted by Mr. Monsour to ensure that the SIS databases were not compromised. I DID NOT directly participate in the investigation. I appointed an expert from my area as requested by Mr. Monsour to participate in the investigation. I was made aware of the ITS Oversight Report in 2012. I am unable to decipher the rest due to redaction but I would be glad to explain if necessary. I was never told or made aware or found any of the SIS data to have been exposed.

signed versions, and that they were transmitted to anyone at the time the events occurred. Mr. Corzo could have offered testimony to support these propositions, but did not do so. We cannot give significant weight to these documents. If Mr. Corzo was aware of their contents and aware that they had been ignored by the Vice Chancellor, he should have shared the full content and its true significance with the Chancellor and/or the Governing Board. There is no evidence that he did so.

26. More than that, if he was monitoring security procedures to protect the data, Mr. Corzo had to be aware that the.....
. This was the case both before and after the 2011 incident. There is no record that he protested this risky practice on behalf of the people whose data he was assigned to protect. To the extent Mr. Corzo claims that

Not true. I was denied access to public records that could have supported the propositions listed above. I was not allowed to bring witnesses that could have testified to the existence of these documents. I was not aware of the full content of many of these reports as they were not share with me until later in 2012 when the grievance was file and 'after' they had been shared with Mr. Kahjkeian. It was Mr. Monsour role to report these finding to the VC of ITS and it is my understanding that he did so. I ENCOURAGE the Board to listed to Mr. Monsour sworn testimony. This should be now available for purchase.

his staff regularly
he could not reasonably have relied on review of
88-89) knowing the

the committee finds and concludes that

27. The committee finds and concludes that Mr. Corzo had a duty under the above performance standards to do more than report generally and prospectively that neglect of security improvements could create a risk of data exposure, in support of a grievance requesting restoration of his position. The report finding that there was containing personal data and

•••••• could and should have been presented to the

It is nearly impossible to decipher what it is being said here. We had daily monitoring reports running in our ERP systems. I wasn't personally responsible for reviewing these reports by both the Assistant Director for the ERP system and the Database manager at the time were. These reports were reviewed and signed daily by the Database Manager or Assistant Director. It is important to understand that this reports did not monitor any of the servers or database that were compromised in 2011. The responsibility to monitor that environment relied with another ITS Director. When I interviewed with Kroll on their allegation against me, I pointed out to them that we had many monitoring reports/tools in place. I also told them that I would be glad to share those if necessary. They never followed up or contacted me to review the reports that were available in 2011.

Governing Board directly If other members of senior management failed to act on it immediately; this is why the District has whistleblower protection. The information could have been presented to the Office of Public Stewardship confidentially, for due diligence inquiry. [The only complaint to that office appears to concern the "workplace climate," according to Ms. Taney's report to the Chancellor). It is easy to see why the information was not so reported; leaders whose job it was to protect data would have faced serious questions as to how these conditions came to exist on their watch.

28. There is no better evidence that senior management and the Governing Board were unaware of the true condition of the institution's data after the 2011 incident than the stark contrast in Stach and Liu's experience in the two events: obstruction, obfuscation, and "CYA" by

*Not true. The information was presented to the ITS VC of ITS by Mr. Monsour, the person responsible for escalation of these issues. It was also shared with the Chancellor as part of the grievance and it was recently shared with the Board. Those in charge who received the grievance should have escalated it further or taken action. In addition, Mr. Monsour and I talked to Teresa Toney about all the issues in ITS * and she brought up this information to the Chancellor. The Chancellor responded 'Thanks' to the second message she sent and we have not heard from him since. This took place in 2012. In a letter of resignation sent to the Chancellor in 2012, the Manager of the Database team after resigning due to hostile environment brought up a myriad of issues to the Chancellor and the Governing Board. This employee never received a response other than dismissal of her concerns *. The MCCC Administration has known about the security issues and risks since 2011. They were later notified by the FBI. They were bombarded with complaints of all sorts having to do with IT and treatment of employees. They experienced first hand the departure of nearly 50% of the department in 2012 and 2013. The Chancellor received letter after letter and a grievance warning him and the Administration of tremendous financial risks to the organization. The Administration opted to turn a blind eye and the 2013 security incident happened.*

senior IT leaders in 2011; serious attention and vigorous action to investigate, remediate, and protect people in 2013: We find that Mr. Corzo willfully and intentionally failed to perform the above duties by allowing the risk to arise

and exist before 2011 and by failing to disclose to executive leadership fully and accurately participating in the cover-up of the known true condition of data security after the 2011 event.

Not true. I was the person who brought this up to the attention of the Chancellor and others in the Administration. The administration opted to ignore and dismiss the issues we raised. I made every attempt to protect our systems and even order a security assessment of a critical MCCCCD systems I was responsible for two years in a row. The webserver and operating system security of ALL ITS servers resided with another Director in ITS. It was his responsibility to perform all necessary checks and balances on those servers. I made every effort to make sure this was getting done and escalated when I realized nothing was being done. My job was not to watch over the job of every ITS Director reporting to Mr. Kahkejian. It was the job of the VC of ITS to do so and ensure that data in all systems that he was responsible for was fully protected. We all had responsibilities for certain parts of the ITS organization. I did not willful, intentionally or unintentionally failed to perform my duties. Others in the department apparently did.

29. The Committee finds and concludes that the charges against Mr. Corzo are based solely on the independent results of the Kroll Investigation by Mr. Caouette and the recommendation of Independent counsel. Mr. Caouette interviewed ITS employees {including Mr. Corzo}, former employees, and consultants and reviewed the documentation those individuals submitted about security issues relating to the [redacted]. Testimony by Mr. Caouette supports our conclusion that he was objective, and that he had free access to any evidence and any witness he wanted to interview, and that he applied his independent judgment as an experienced Investigator to

Not true as already explained multiple times.

investigate and evaluate the evidence.

30. The 2012 IT grievance's general references to data security risks fail to disclose the critical information that Mr. Corzo knew at the time: that there was no effective security program in place to protect his data and In fact it was..... The Committee asked Mr. Liu to assess the significance of his 2011 findings as reported to IT managers, including Mr. Corzo. Was this the equivalent of a piece of paper on fire, or was this more serious? Mr. Liu responded, "I think the building has burned down at that point, okay? And everyone was kind of looking the other way the house had been ransacked. I mean, there was evidence everywhere this had occurred." There is no question that reports and recommendations were made to the Vice Chancellor about the incident and that plans were reported to [redacted] But the information conveyed did not hint that the [redacted] security house had burned down and that.....

- No crisis was reported: improvements were needed and would be made in due course. The failure of senior managers like Mr. Corzo to report upward accurately in 2011 the findings of Stach and Liu left the personal information of well over two million people exposed for two more years.

The contrast between 2011 and 2013 is compelling evidence of the above described failure to report fully the information they held. In 2013, different people were in place in IT. In response to another FBI report similar to 2011, they shut down the website and initiated an investigation. Stach and Liu (subsequently rebranded as Bishop Fox) found the same conditions they found two years earlier: none of their recommendations had been implemented. But in contrast to the 2011 response, the CIO and the Chancellor treated the situation as a serious problem. Experts were brought in to assess what had happened. Protecting Maricopa's data and people became top priority. Resources were shifted and changes were made. Millions of people were notified and offered meaningful protection, and resources were allocated to support the protection of district data.

I was not involved in the 2013 investigation but it does not surprise me to read this comment. This comment from Stach and Liu was the basis of the grievance we filed and submitted to the Chancellor. The Chancellor knew about this condition in 2012 when he was told the exact same thing. Please read the text of the grievance regarding security.

We find and conclude as Mr. Caouette did, that Mr. Corzo did not report fully and accurately what he knew because his job was more important to him than the protection of the people whose data it was his responsibility to secure. This was a willful decision on his part, not an inadvertent one. Had Mr. Corzo reported to senior management accurately what Stach and Liu found, he would have faced then the questions he faces now, as to how such disastrous lack of security could have existed on his watch if he were doing his job. But the information would have protected the

Not true. An information security program was created in 2011-2012. The responsibility to create that program for MCCCDC was placed in Mr. Monsour's plate by Mr. Kahkejian. He created such program and with direction from Mr. Kahkejian proceed to create a committee for implementation. I was not asked to participate in the committee or task with implementation by my supervisor. I was not asked to create such program for MCCCDC.

data of the people of Maricopa
from further.....

Not true. After the 2011 incident I contracted with Microsoft twice to conduct to do a security assessment of our identity management system. In addition, I also contracted with IBM after the 2012 incident to give Maricopa a proposal to partition the SIS data so if it was ever breached, only a small subset of that data was compromised. This project was scrapped by Mr. Kahkejian and never implemented. This is the same project implemented at VCCCS to protect their system. There was no disastrous lack of security. The SIS database was secure and never compromised in 2011. I have yet to see any evidence to support the statement above.

Failure of the MCCC administration to act on the myriad of issues not just security mentioned in the ITS grievance and the Security Oversight Report is what led to this fiasco. Instead of accepting responsibility, the Administration has hired expensive lawyers, rigged hearing and violated policy to protect itself and fire employees.

D. SUMMARY CONCLUSIONS AND RECOMMENDATION

As a MAT employee and as a member of the IT leadership team, Mr. Corzo had a responsibility team to operate systematically in collaboration with other team members, in a manner that helped the organization to identify and appropriately manage risk; to provide accurate, reliable, and timely information to executive leadership; to protect resources including data, and to help to identify and address issues of regulatory compliance. He had a responsibility to Identify and evaluate the risks related to his I to help to mitigate those risks, and to establish and maintain the effectiveness of controls, standards, procedures and other means available to help him carry out those responsibilities. At all relevant times, Mr. Corzo was specifically assigned responsibility for security. He was a designer and implementer of] who was to work in conference with other team members, applying principles and practices of management and leadership. All these responsibilities were communicated to him, and he acknowledged these responsibilities.

We cannot agree with Mr. Corzo's point of view, that his responsibility to protect data was limited at best, that they ended when the data moved to else, and that he fulfilled such limited responsibilities as were assigned.

Taken together, the charges against Mr. Corzo supported by substantial evidence, and they constitute a willful and intentional failure to perform job duties that were communicated to him and are within the scope of his: employment. See Online Policy Manual 6.7(3). This is a

Please note that the 4 allegations raised against me in Nov 2013 are different than the charges listed in this document. This document appears to go all over the place to protect the Administration, justify the hearing process and blame me for sub-standard performance. The original charges that led to this hearing are not specifically mentioned anywhere in this document. As a matter of fact, one of the charges alleging that I was responsible for networking in Maricopa (IDS/IPS devices) has been completed left out.

The following charges were the reason this committee was constituted. I do not agree with any of them. At times, the committee touched on some of these charges but some of them have been completely ignored and I am confused. I urge you to review the document I provided to Mr. Bowers with my response to all these charges. The way these charges are being presented reflect a complete lack of understanding of the ITS organization, how things work and who was responsible for what.

- You did not monitor or audit the security procedures for the databases for which you were responsible. If you had done so in a reasonable and competent manner, you would have identified existing system vulnerabilities before the first known security incident in January 2011. – FALSE. There were many monitoring tools in place in my area.*

- You were responsible for the SIS database which contained student tax information including Social Security Numbers that was accessible through the public facing web server in the 2011 security incident. – FALSE. The database was not accessible through a public facing webserver.*

- Even after the 2013 security incident, you acknowledged that you did not know whether there was an IDS/IPS device on the Maricopa web server that was working or properly configured. - FALSE. I was not responsible for any network devices at MCCCDC.*

- Although the 2011 security incident included databases for which you were responsible, you did not assist in the investigation or take any remedial steps, which ultimately contributed to the 2013 security incident. As one of Vice Chancellor Kahkedjian's senior managers, you should have been actively involved in the 2011 investigation and been proactive in identifying the network vulnerabilities, communicating those vulnerabilities to senior management, and taking steps to resolve them. - FALSE. I supported the investigation and performed all tasks assigned.*

Category One performance-based offense. See MCCCDC Policy A-4(C), Performance-Based Offense, Group One Offense.

Mr. Corzo knew or reasonably should have known that his actions and inactions could lead to disciplinary action because they were the result of poor job performance and violated established MCCCDC policies or procedures.

This conclusion was reached by District Administration after a fair and objective investigation conducted in accordance with MCCCDC policy and the law, which included a pre-disciplinary

interview of Mr. Corzo for his version of the events and a review of pertinent e-mail correspondence. As discussed above, the investigation has produced sufficient evidence or proof to reasonably support the failure of performance or violation as alleged.

Group One offenses provide that a first offense may lead to "disciplinary action, including dismissal from employment." MCCCDC Policy C-4(6). The exposure of the- data to unauthorized access in 2011 and 2013 was a direct result of Mr. Corzo's willful non-performance of his duties.

The events described here are unprecedented, so it appears that there is no directly comparable precedent. However, the committee is informed and finds that MCCCDC recommended dismissal of other Individuals whose performance failed to meet the above standards, and that three resigned rather than appeal the charges. We find on that basis that the standards have been consistently applied.

The consequences of Mr. Corzo's performance failure are significant. MCCCCD faces lawsuits and possible regulatory sanctions as a result of his (and others') failure to take reasonable steps to secure personal data. Given these serious consequences, the Committee finds that the proposed disciplinary action, termination, is reasonable and permissible under MCCCCD policy.

Therefore, the Committee recommends that the charges against Mr. Corzo should be sustained, and that he should be dismissed from employment based on his willful nonperformance of assigned duties.

Respectfully submitted,

Daniel Huston

As long-time MCCCDCD employee, I have been denied due process to defend myself. The Board has been denied access to critical information such as Mr. Monsour's testimony and other pieces of information. The Board has yet to hear from Mr. George K. and his account of events. Record requests made months ago and needed for my defense are now being provided after a judge forced MCCCDCD to do so. A Letter of termination is being sent to individuals 2 business days before the Board is to vote on this topic and with absolutely no time to respond. Even the name of the employee being targeted is being kept from the Board agenda. Wrong assumptions are being made that I had access and responsibility for information that I did not. Statements in this document from the hearing committee and even investigators show a lack of understanding of the complexity of IT system and who was responsible for what. Lastly, multiple Board policies and breaches of contract has taken place as outlined above.

My role in ITS was not to play GOD and look over everyone's department. If anyone had overarching responsibility for ITS and MCCCDCD, that was the VC of ITS and the Chancellor respectively. I followed process as advised and communicated upwards, not once, not twice but over 12 times in 2012 alone. The Administration had plenty of time to take action but chose to turn a blind eye.

My supervisor had every opportunity to evaluate my performance and provide feedback prior to 2013. He never reported any issues to me as documented in my yearly evaluations. On the contrary, a letter of recommendation from my last supervisor, Mr. John Webster paints a completely different light that what is being depicted here. I urge the Board to contact Mr. Webster, Mr. Darrel Huish, Mr. Ronald Bleed and others CIO/VCS of ITS regarding my performance if they have any questions for my commitment to MCCCDCD faculty, staff and students. I have letters of recommendations from all of them.

In my entire career at MCCCDCD, I have never been given a poor evaluation and I hold several letters of recommendation from nearly all my past supervisors.

The Administration was notified by the FBI. The VC of ITS was notified by his direct reports in charge of operational and strategic security that there were significant issues that will lead to great financial impacts. No information was intentionally kept from anyone. I did not work at MCCCDCD for nearly 30 years to end up my career like that. The early warnings were ignored and the Administration has chosen to break Board policies, create new policies, go back in time and break multiple laws in Arizona to protect itself at the expense of taxpayers and MCCCDCD employees, faculty and students.

I still remain committed to the success of MCCCDCD and to continue fighting this injustice.

I respectfully request that all these charges be dismissed and that the Board considers additional testimony to hold those at the top of this organization accountable. If the Board does not do this, law firms and our community will eventually do so.