



SUSANA MARTINEZ  
Governor

Duff Westbrook, Chair  
Roger E. "Bart" Bartosiewicz, Vice-Chair  
John Bledsoe, Member

STATE OF NEW MEXICO  
PUBLIC EMPLOYEE LABOR RELATIONS BOARD

2929 Coors Blvd. N.W. Suite 303  
Albuquerque, NM 87120  
(505) 831-5422  
(505) 831-8820 (Fax)

THOMAS J. GRIEGO  
Executive Director

November 23, 2015

New Mexico Dep't of Health  
Office of General Counsel  
1190 St. Francis Dr.  
Santa Fe, New Mexico 87502  
Attn: Maura Shuttleworth, General Counsel

CWA Local 7076  
c/o Rosenblatt & Gosch, PLLC  
8085 E. Prentice Ave.  
Greenwood, Colorado 80111  
Attn: Stanley Gosch, Esq.

Re: ***CWA Local 7076 v. N.M. Dep't of Health; PELRB No. 116-15***

Dear Ms. Shuttleworth and Mr. Gosch:

This letter constitutes my decision regarding the Respondent's Motion for Summary Judgment filed November 16, 2015. The Union did not respond to the Motion by the scheduled response date, November 20, 2015. Therefore, the factual allegations set forth in the Employer's Motion for Summary Judgment are not refuted and are established as facts in this case. Despite the absence of a Response, after considering the movant's arguments, affidavits and other evidence submitted I have determined that the Motion should be **DENIED** for the reasons set forth below:

**STANDARD OF REVIEW:**

The PELRB has long followed New Mexico Rules of Civil Procedure, Rule 1-056 when deciding a motion for summary judgment. See *AFSCME Council 18 v. New Mexico Department of Labor*, 01-PELRB-2007 (Oct. 15, 2007). Applying that rule the movant shall set out a concise statement of all material facts about which it is contended there is no genuine dispute. The facts set out shall be numbered and the motion shall refer with particularity to those portions of the record upon which the party relies. See N.M. Rul. Civ. Pro. Rule 1-056. Summary Judgment will be granted only when there are no issues of material fact with the facts viewed in the light most favorable to the non-moving party. The movant has the burden of producing "such evidence as is sufficient in law to raise a presumption of fact or establish the fact in question unless rebutted." If that threshold burden is met by the Movant, the non-moving party then must "demonstrate the existence of specific evidentiary facts which would require trial on the merits." *Summers v. Ardent Health Serv.* 150 N.M. 123, 257 P.3d 943, (N.M. 2011); *Smith v. Durden*, 2012-NMSC-010, No. 32,594; *Blauwkamp v. Univ. of N.M. Hosp.*, 114 N.M. 228, 231, 836 P.2d 1249, 1252 (Ct. App. 1992). An award of summary judgment is proper if there are no genuine issues of material fact and the movant is entitled to judgment as a matter of law. *Koenig v. Perez*, 1986-NMSC-066, ¶16 104 N.M. 664. ¶10 (citing *Westgate Families v. County Clerk of Los Alamos*, 100 N.M. 146, 667 P.2d 453 (1983) and *Meeke v. Walker*, 80 N.M. 280, 454 P.2d 762 (1969)).

**MATERIAL FACTS NOT IN CONTROVERSY:**

1. On May 14, 2015, the Employer served a Notice of Final Action on one of its employees, Tony Escudero, suspending him for five days for violations of the Department's Code of Conduct, and other employer policies. (Affidavit of Kimberly Souders, ¶ 2, Exhibit 1.)
2. On Escudero's behalf, his collective bargaining representative CWA Local 7076 invoked arbitration, which was set for September 2 and 3, 2015. (Souders Affidavit, ¶ 3.)
3. While the arbitration hearing was pending, the Public Health Division ("PHD") Human Resources Director, Kimberly Souders ("Souders") received a verbal report alleging misuse of the state email system by Escudero other than those pending arbitration. (Souders Affidavit, ¶ 4.)
4. PHD Human Resources commenced an investigation into those new allegations. (Souders Affidavit, ¶ 5.)
5. As part of that investigation, the Information Technology Bureau downloaded for review approximately one month's worth of Escudero's emails from the state email system pursuant to NMAC Rule 1.12.10.8. (Souders Affidavit, ¶ 5.)
6. On September 3, 2015, at the arbitration hearing, the Department's Assistant General Counsel used one email from the group to impeach Escudero on cross-examination. (Souders Affidavit, ¶ 6.)
7. As a result of the Employer's use of the e-mail for impeachment the Department's Labor Relations Bureau Chief (Elona Cruz), PHD Human Resources Director and its Assistant General Counsel grew concerned that Escudero would realize that there was an ongoing investigation into his use of the state email system and that he might attempt to destroy potential evidence by deleting his emails). (Souders Affidavit ¶ 7.)
8. Cruz consulted with the Information Technology Resources Bureau on the evening of September 3, 2015 and decided to temporarily disable the state email accounts of Escudero and another employee, Julie Maes ("Maes"), because many suspected violations of the Internet, Intranet, Email and Digital Network usage were between Maes and Escudero (Souders Affidavit, ¶ 8.)
9. Both Escudero and Maes have signed an "Acknowledgement and Consent" form acknowledging:
  - a. Their receipt of the Executive Branch Information Technology Resources Policy regarding Internet, Intranet, Email, and Digital Network Usage;
  - b. That they fully understand the terms of this policy and agree to abide by them;
  - c. That the electronic mail system is Department of Health and State property, intended to be used primarily for business purposes and that any message they send or receive may be recorded and stored in an archive file for management use; and,
  - d. That the Employer may access, review, and disclose information obtained through the email system at any time, with or without advance notice and with or without consent.
10. I take Administrative Notice of the following:
  - a. Executive Branch Information Technology Resources Policy: Internet, Intranet, Email, And Digital Network Usage 8.3:



“The State of New Mexico may undertake all prudent and reasonable measures to secure the systems it uses for Internet communications and the data transmitted by these systems and services, at the direction of the Governor or his designee(s)”;

- b. Executive Branch Information Technology Resources Policy: Internet, Intranet, email, And Digital Network Usage 8.6:

“Staff shall have no expectations of privacy with respect to state IT resource usage. Employees are advised that serious disciplinary action up to and including termination of employment may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving state IT resource usage may be referred to appropriate authorities for prosecution”;

- c. Executive Branch Information Technology Resources Policy: Internet, Intranet, email, And Digital Network Usage 11.1:

“Violations of this policy shall be investigated promptly and efficiently by objective and appropriate staff to be designated by the Agency Secretary or Director.”

- d. Executive Branch Information Technology Resources Policy: Internet, Intranet, email, And Digital Network Usage 11.2:

“Staff suspected of violating this policy shall be given notice of an investigation and an opportunity to present any relevant, exculpatory evidence or mitigating circumstances regarding the charge of the violation.”

- e. Executive Branch Information Technology Resources Policy: Internet, Intranet, email, And Digital Network Usage 11.3:

“If the investigation shows the staff member violated this policy, the staff member may be subject to suspension or termination of access to IT resources, as well as disciplinary action up to and including termination of employment. If the investigation shows the staff member to have engaged in any of the activities prohibited in Sections 9.6, 9.9, or 9.12, disciplinary proceedings will commence in accordance with the State Personnel Act and Rules, and shall include a written reprimand and suspension without pay for at least one week or up to one month, or termination for cause.”

- f. NMAC 1.12.10.8, which provides:

“The internet and other information technology resources are important assets that the state can use to gather information to improve external and internal communications and increase efficiency in business relationships. To encourage the effective and appropriate use of the state’s IT resources, the following policies govern the use of the state’s IT resources:

A. State agencies shall provide all users with a written copy of this rule.

(1) All users shall sign and date a statement indicating they have received and read this policy.

(2) Each user’s signed statement shall be kept on file for as long as the user is employed by, has a contract with or otherwise provides services to the agency.

B. For the purposes of this rule, IT resources usage includes but is not limited to all current and future internet/intranet communications services, the world wide web, state intranets, voice over IP, file transfer protocol (FTP), TELNET, email, peer-to-peer exchanges, and various proprietary data transfer protocols and other services.

C. The state of New Mexico may undertake all prudent and reasonable measures to secure the systems it uses for internet communications and the data transmitted by these systems and services, at the direction of the governor or his designee(s).

D. The state of New Mexico and/or its agencies may install software and/or hardware to monitor and record all IT resources usage, including email and web site visits. The state retains the right to record or inspect any and all files stored on state systems.

E. State IT resources shall be used solely for state business purposes (except as described in Section 1.12.10.10 NMAC) and users shall conduct themselves in a manner consistent with appropriate behavior standards as established in existing state policies. All state of New Mexico policies relating to intellectual property protection, privacy, misuse of state equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality shall apply to the use of IT resources.

F. Users shall have no expectations of privacy with respect to state IT resource usage. Serious disciplinary action up to and including termination of employment or contract may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving state IT resource usage may be referred to appropriate authorities for prosecution.”

g. NMAC 1.12.10.9, which provides:

“State IT resources shall not be used for anything other than official state business unless otherwise specifically allowed by the agency head or as permitted under Section 1.12.10.10 NMAC.

A. No software licensed to the state nor data owned or licensed by the state shall be uploaded or otherwise transferred out of the state’s control without explicit authorization from the agency head.

B. IT resources shall not be used to reveal confidential or sensitive information, client data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Users who engage in the unauthorized release of confidential information via the state’s IT resources, including but not limited to newsgroups or chat rooms, will be subject to sanctions in existing policies and procedures associated with unauthorized release of such information.

C. Users shall respect the copyrights, software, licensing rules, property rights, privacy, and prerogatives of others, as in any other business dealings.

D. Users shall not download executable software, including freeware and shareware, unless it is required to complete their job responsibilities.



- E. Users shall not use state IT resources to download or distribute pirated software or data, including music or video files.
- F. Users shall not use state IT resources to deliberately propagate any malicious code
- G. Users shall not use state IT resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the state's IT resources.
- H. Unauthorized dial-up access to the internet is prohibited from any device that is attached to any part of the state's network. The state's IT resources shall not be used to establish connections to non-state internet service providers without prior authorization in writing by the office of the chief information officer or the state chief information technology security officer.
- I. Users shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using state IT resources.
  - (1) In agencies or offices where the display or use of sexually explicit or extremist materials falls within legitimate job responsibilities, an agency head may exempt a user in writing from the requirements of this subsection. The agency issuing the exemption letter shall keep the letter on file for as long as the user is employed by, has a contract with, or otherwise provides services to the agency.
  - (2) The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through email, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored nor forwarded to other parties.
- J. Users are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
- K. Users shall not use state IT resources to override or circumvent any security mechanism belonging to the state or any other government agency, organization or company.
- L. Users shall not use state IT resources for illegal activity, gambling, or to intentionally violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation."
- h. NMAC Rule 1.12.10, which provides:

"Occasional and incidental personal use of the state's IT resources and internet access is allowed subject to limitations. Personal use of the internet is prohibited if:

  - A. it materially interferes with the use of IT resources by the state or any political subdivision thereof; or
  - B. such use burdens the state or any political subdivision thereof with additional costs; or
  - C. such use interferes with the user's employment duties or other obligations to the state or any political subdivision thereof; or
  - D. such personal use includes any activity that is prohibited under this rule.

**ISSUE PRESENTED:**

Whether the Employer is entitled to dismissal of the PPC herein as a matter of law.

## **DISCUSSION AND RATIONALE:**

### **I. THE EMPLOYER HAS ESTABLISHED THAT IT HAS THE RIGHT TO MONITOR AND ACCESS USAGE OF THE EMAIL/INTERNET PROVIDED BY THE STATE AT ANY TIME. HOWEVER, IT HAS NOT ESTABLISHED THAT ITS ACTIONS IN THIS CASE ARE CONSISTENT WITH THAT RIGHT AND THEREFORE HAS NOT ESTABLISHED ITS RIGHT TO DISMISSAL AS A MATTER OF LAW.**

It is clearly established that the Employer has both a right and duty to enforce the Executive Branch Information Technology Resources Policy. See the Executive Branch Information Technology Resources Policy regarding Internet, Intranet, Email, And Digital Network Usage and the effected employees' agreement to abide by that policy. There is nothing in that policy or any of the documents or in the affidavit submitted in support of Summary Judgment that establishes as a matter of law that the Employer's actions in temporarily disabling the email access of two bargaining unit employees as alleged in the instant PPC is authorized by that policy.

Even if the employer had established that, as a matter of law it was privileged to temporarily disable the employees' email access as alleged in the instant PPC that would not lead to a conclusion that it is entitled to judgment because the PPC is not premised as a challenge to the employer's right of access to the email. Rather, it focuses on the propriety of disabling access by bargaining unit employees under the circumstances of this case. It is axiomatic that one may not use a legitimate means to achieve an illegitimate end. For example, by analogy, New Mexico recognizes the tort of malicious abuse of process whereby one party legitimately initiates a judicial proceeding against another but misuses the process in a manner other than would be proper in the regular prosecution of the claim, i.e. using the process to accomplish an illegitimate end.

It remains a material question of fact foreclosing judgment as a matter of law whether the Employer has exercised its rights under the above-reference rules to harass or retaliate against bargaining unit members for their participation in their contract's arbitration procedure in violation of the PEBA.

For the same reasons, the fact that there is no expectation of privacy in the state email system does not militate in favor of summary judgment.

## **CONCLUSION:**

Summary judgment is appropriate only if the movant demonstrates by such evidence as is sufficient in law that there are no issues of material fact with the facts viewed in the light most favorable to the non-moving party. Only once that burden is met would the Complainant be required to rebut those facts or otherwise demonstrate the existence of specific evidentiary facts which would require trial on the merits. Here, the undisputed facts do not support the legal conclusions that the New Mexico Dep't of Health wishes the PELRB to reach. Accordingly, judgment as a matter of law in favor of

Letter Decision re: PELRB 116-15  
November 23, 2015  
Page 7

the agency would not be appropriate.

For the reasons stated above I conclude that the Employer's Motion for Summary Judgment is **DENIED**. The case shall proceed to a Hearing on the Merits as scheduled.

Sincerely,

PUBLIC EMPLOYEE LABOR RELATIONS BOARD  
  
Thomas J. Griego  
Executive Director

Cc: Robin Gould, CWA Staff Representative  
Sandy Martinez, SPO Labor Relations Director