

**STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS  
RHODE ISLAND STATE LABOR RELATIONS BOARD**

**IN THE MATTER OF  
THE STATE OF RHODE ISLAND  
DEPARTMENT OF CORRECTIONS**

**Employer**

**Case No. EE: 2003**

**AND -**

**RHODE ISLAND BROTHERHOOD OF  
CORRECTIONAL OFFICERS**

**Petitioner**

**DECISION AND ORDER**

This case arises out of a Petition for unit clarification dated July 9, 1996 and filed with the Rhode Island State Labor Relations Board (hereinafter Board) on July 16, 1996 by the Rhode Island Brotherhood of Correctional Officers (hereinafter "RIBCO" or "Union"). The Petition seeks to accrete five (5) positions to the unit certified by EE 2003 on March 23, 1972. The positions sought are: Information Aide, Jr. Electronic Computer Programmer, Sr. Electronic Computer Programmer, Principal Systems Analyst and Chief of Data Operations.

The Board assigned its Agent to investigate the positions. On June 24, 1997, the Board made a preliminary determination that the position of Information Aide was already included in the bargaining unit and that the positions of Jr. Electronic Computer Programmer, Sr. Electronic Computer Programmer, and Principal Systems Analyst were appropriate for accretion into the bargaining unit. Thereafter, formal hearings were held on December 2, 1997 and February 12, 1998. Both parties were present and represented by legal counsel. Upon conclusion of the hearings, the parties submitted written briefs. In arriving at the within decision, the Board reviewed the transcripts and exhibits submitted, and the arguments contained in the post-hearing briefs.

**POSITION OF THE PARTIES**

The Union submits that the computer programming positions in question are the types of positions that have routinely been permitted by this Board to engage in collective bargaining. Further, the Union argues that these positions have never had any access to information pertaining to labor relations or personnel issues; and that these positions are

not “confidential” under the “labor nexus” test enunciated in Barrington School Committee v. Rhode Island State Labor Relations Board, 694 A.2d 185 (R.I. 1992).

The Employer argues that MIS employees are confidential employees, even under the labor nexus test. If however, this Board was not convinced that the MIS employees are confidential under the narrow labor nexus test, the Employer urges this Board to then depart from the narrowly defined “labor nexus” definition of confidential as defined by the Barrington court because these positions are “technologically confidential secretaries to the entire department.” The Employer has also described these employees as having access to every computer byte of information in the department [even more so than the Director of Corrections] and as such they should be considered confidential and excluded from collective bargaining. Finally, the Employer also argues that even though the MIS employees are highly trusted, they nonetheless serve as an integral “choke point” and are able to shut down the entire computer system because of their duties. For their alleged potential to engage in this criminal conduct, the Employer asserts that they are ineligible for collective bargaining.

#### FACTUAL SUMMARY

The Employer first presented the testimony of Mr. Steven F. Chianesi, the Associate Director of the Management Information Systems (hereinafter “MIS”) at the Department of Corrections (hereinafter “DOC” or “Employer”). Mr. Chianesi testified that in 1991 he was interviewed by a Board Agent for a previous unit clarification petition which also sought the inclusion of the position of Senior Electronic Computer Programmer. (TR #1 p. 9) At that time, the Board determined that this position was “confidential” and should be excluded from collective bargaining. (TR #1. p. 9 and Employer Exhibit #1) <sup>1</sup> On cross examination, Mr. Chianesi testified that he had no actual knowledge on what information the Board reviewed when it made its previous determination to exclude the position of Senior Electronic Computer Programmer. Mr. Chianesi also testified that the organization chart submitted as Union Exhibit #1 was missing a section which should show that five lieutenants and two captains (all RIBCO members) also report to Mr. Chianesi. He also testified that the MIS positions of File

---

<sup>1</sup> Both Mr. Chianesi and Mr. Major testified that the MIS unit and the Department had been extensively re-organized since then and that more changes were coming.

Clerk, Clerk Typist, Assistant Supervising Data Entry Operator, Supervisor of Data Entry and the Principal Clerk Stenographer were all positions within the RIBCO bargaining unit certified in EE-2003. (TR #1 p 12)

The Employer's next witness was Kevin M. Major, Program Analyst Manager for the MIS unit. He is responsible for basically all aspects of computerization at DOC. (TR #1 p. 18) He testified that the four positions being sought for accretion report to him on long-term projects and to Michelle Lanciaux, Chief of Data Operations, for day-to-day activities (TR #1 p. 20) In Ms. Lanciaux's absence, they would report to Mr. Major on day-to-day activities. He also testified that the MIS unit is planning on expanding by adding additional Principal Systems Analysts and Senior Electronic Computer Programmers who would also report to Mr. Major on the day-to-day aspects of the job. (TR #1. p. 20-21) He also testified that the work week of the unit is considered "non standard", but that by and large they work from 8:30 am- 4:00 pm. The schedule does vary with the needs of the Department and employees are subject to receiving a call at any hour of any day to report in for a problem. (TR #1. p 22)

Mr. Major went on to testify as to the duties and responsibilities of the individuals holding the positions sought for accretion. He testified that Paul Mattias is a Principal System Analyst who is the administrator of the main WANG system at DOC. (TR #1. 23) Mr. Mattias is responsible to make sure the system is up and running at all times; for assigning IDs and passwords to all users; and to maintain lists of the users; to manage access to the RILETS, a computer system developed for the R.I. State Police (TR #1 p. 23)

Mr. Major testified that Ken Kard, the second Principal System Analyst, is primarily responsible for the operation of the local area network ("LAN") which is located in five buildings. (TR #1 30) Future plans are to expand the LAN to all locations within the Department and to slowly phase out the WANG computer. As the LAN administrator, Mr. Kard is responsible for helping develop these plans, to continue to monitor the LAN and to develop plans on how the expanded network will be utilized. (TR #1. p 31) Mr. Major testified that the Director, the Assistant Director (of DOC), Human Resources, payroll, investigations, legal and finance offices of the Department are on the LAN. (TR #1 p. 32) Mr. Kard's responsibility is to assign passwords and develop

profiles of users. (TR #1. p 32) Mr. Kard also is responsible for occasionally resolving specific user problems. (TR #1 p 33) He also has access on occasion to every office and every computer on the system, to effectuate changes to the system. (TR #1 p. 34-35)

Ms. Peggy Charette, a Senior Computer Programmer, also reports to Mr. Major. She's responsible for making changes to the systems currently in existence. (TR #1 p. She is also the E-mail administrator and sets employees up with E-mail access. (TR #1 p 36) She has also developed a number of Q & A systems over the years. (TR #1 p. 39)

Mr. Frank Pate, a Senior Computer Programmer, is responsible for managing and maintaining an inventory of computer systems located on the Department's computers. ( TR #1 p. 40) He installs and upgrades PCs. (TR #1, p. 40) In this capacity, he must have access to passwords, in order to insure the integrity and the functionality of the new computer. (TR #1, p. 41)

On cross examination, Mr. Major conceded that RIBCO members already have access to information contained in the "records and ID" system, the "RILETS" system, and the inmate banking system. (TR.#1, p. 51-52) He also acknowledged that he has "no role in developing labor relations policies for the Department; in fact, "labor relations" forms no part of his activities. (TR.#1, p. 52) Mr. Major also acknowledged that if a computer was password protected, the user of that computer would have to give his or her password to his employees so that they could access the computer for whatever their duties required.

The Union presented testimony from three of the MIS unit employees, including Ms. Peggy L. Charette, and Frank N Pate, both Senior Electronic Computer Programmers, and Kenneth R. Kard, II, a Principal Systems Analyst.

Ms. Charette testified that she writes programs to print reports, applications that will require input and sets up files for small tracking systems. (TR #2, p. 4) She also assists Mr. Pate in servicing computers and sets up profiles and menus for people using the E-mail system. (TR. #2, p. 4) She does not have user access to the information or data contained in the E-mail system; in order to have access, an individual user would have to set up access within his or her profile for Ms. Charette. (TR. #2, p. 5) She testified that in the seven and one half years that she has been employed at the DOC, no one has ever made his or her files available to her. (TR. #2, p. 5) She does not have any role with or

access to labor relations information; nor has she served with or provided any information to any management negotiating team. (TR. #2, p. 5, 6, 7) She does not supervise anyone and reports to both Mr. Major and Ms. Lanciaux. (TR. #2, p. 6)

Ms. Charette testified that she has user access to the INFACITS (the inmate system) system and depending upon the specific file class, she would have access to either read, write or just display information. (TR. #2, p. 7) There is also a human resources system, but she testified the passwording and security on that system is internal within the application and she does not know how that works. (TR. #2, p. 7) She testified that she would need permission to enter any administrative office to work on the computer systems. (TR. #2, p. 9) She has never been called in on a night or a weekend to perform any work in these offices. (TR. #2, p. 9) As far as access in the legal offices, she has had the occasion to work on an application but not data files. (TR. #2, p. 9)

On cross examination she testified that she had had some training on the LAN, setting up file attributes to give users access to set up IDs and to manage the system, but that she no longer has access to systems administration within the network. (TR. #2, p. 10-11) She also testified that on the E-mail system, she cannot find passwords for individuals, she would have to obtain that information from someone else. (TR. #2, p. 12) She also testified that one of the biggest problems the department has from a security standpoint is that people have their passwords labeled right on the front of their computer. (TR. #2, p. 14) <sup>2</sup> She also testified that when she does work on a computer, she tries to avoid having that person give her the ID or password and instead has that person log onto the system directly and then she takes over. (TR. #2, p. 14) She cannot access anyone else's E-mail. (TR. #2, p. 16) She also testified that when there is a "locked ID" problem, she calls Mr. Major or Ms. Lanciaux at home (where they have computers) and they will go into the system, access the security file and unlock the ID. (TR. #2, p. 7)

Mr. Pate testified that he spends the majority of his time upgrading PC hardware, taking inventory and helping users with the general functionality of their computers. (TR. #2, p. 19) Upgrading a computer consists of "switching a full PC over, transferring their programs, or upgrading, adding components, processors, memory and so forth." (TR. #2,

---

<sup>2</sup> Having passwords in such plain view is an invitation to trouble from every employee in the Department of Corrections and as such certainly poses a great threat.

p. 19-20) He does not have access to the data on individual computers, nor does he have access to passwords. (TR. #2, p. 20) <sup>3</sup> He has never been called in to work in the middle of the night, nor has he ever worked on a computer in the administrative offices without the user or someone else present. (TR. #2, p. 21) He reports to Ms. Lanciaux and supervises two outside MIS consultants. (TR. #2, p. 21) He is not involved with any aspect of the Department's labor relations, nor does he perform any role in adjusting grievances. (TR. #2, p. 21) He does not have access to any personnel or financial information regarding the Department's functions. (TR. #2, p. 21) He does not have access to either security system.<sup>4</sup> After upgrading a computer he checks it by bringing up an application and tests it. For instance, with Wordperfect, he will bring up the program, type in the word "this is a test" and then print the page. (TR. #2, p. 24) He checks to make sure labels print and that the communications port works with the VS system and the Banyan-Vines. (TR. #2, p. 24) He does not need a user's password to perform these checks. (TR. #2, p. 25) If someone is having trouble accessing the systems with their password, he calls either Paul Mattias or Ken Kard. (TR. #2, p. 26) He also testified that for the most part, people keep their data on floppy disks, but that if they've kept data on their Q & A data bases, that information is password protected. (TR. #2, p. 27) He has no unique access to any material of anyone on the Department. (TR. #2, p. 29) He has no systems administration experience. (TR. #2, p. 30) He cannot run inquiries or print any data from the personnel system. (TR. #2, p. 33) He cannot access information about inmate accounts. (TR. #2, p. 33)

Mr. Kard, a Principal Systems Analyst, testified that he is the systems administrator for the Banyan environment and handles all low level security at the network level, providing access to certain files and directories to certain users within the network. (TR. #2, p. 37) When he accesses the system, he can see file names, but he cannot open and read the file itself. (TR. #2, p. 37) He stated that he holds the responsibility of being the most technical person within the unit and that he is occasionally called in to work in the middle of the night to resolve a computer problem. (TR. #2, p. 38) He has also had the occasion to work in specific administrative offices at night to upgrade the network, but

---

<sup>3</sup> This work can be done when the computer is turned off.

<sup>4</sup> There are two security systems, a "VS" system and Banyan -Vines system. (TR#2, p. 21-22)

only with advance notice to the occupants of those offices. (TR. #2, p. 39) Mr. Kard reports to Mr. Major for long term projects and to Ms. Lanciaux for day-to-day activities. (TR. #2, p. 39) Mr. Kard does not supervise anyone, has no responsibility or role in regards to labor relations, has never served on a negotiating committee, has no access to personnel information, is not involved in the grievance process and cannot access any data contained in the financial files of the Department. (TR. #2, p. 40)

On cross examination, Mr. Kard explained that there are many levels of security for the computer systems. He is involved with network security, as opposed to service security. He stated that he has access to the system down to the file level, but cannot see the data stored in the files. (TR. #2, p. 42) Files can be secured with passwords on the Q&A system, Word Perfect and Lotus. (TR. #2, p. 44-45) Mr. Kard cannot access password protected files. (TR. #2, p. 46) If files are not password protected and the file resides on the LAN, instead of a floppy disk, or the individual user's C-drive, Mr. Kard would be able to access the data inside the file, however it would take some extensive programming in order to achieve the access. (TR. #2, p. 51-52) To maintain security at the server level, he meets with groups within the department to determine who is supposed to have access to what. He then provides the access to each individual and sets up the system so that only the proper people can access their files. (TR. #2, p. 55) Mr. Kard testified that he does not have access to the VS system at all and that the only access he has is to his own E-mail. (TR. #2, p. 56)

On re-direct examination, Mr. Major claimed that Ms. Charette had greater access to individual files than she testified. He said that she has a certain level of security clearance that gain access to all the information that may reside in other people's computer files. (TR. #2, p. 64) Mr. Major went on to state that only people in the MIS unit have this unique ability to access information, but that not everyone in the unit has that access. (TR. #2, p. 66) He first stated that every other person in the unit, other than Frank Pate has this type of access. On further examination, he limited this initial statement by saying that he was "not sure about Ken." (TR. #2, p. 66) On re-cross examination, Mr. Major candidly admitted that the DOC has no formal policy or requirement for users of the computer systems to protect their files by using passwords, despite the fact that

such a security device is available to the users. (TR. #2, p. 75) He also admitted that Ms. Charette has probably not accessed a list of passwords in recent years because she had different responsibilities in prior years when the unit had less staff. (TR. #2, p. 78) He also acknowledged that the DOC has a Code of Ethics in lieu of performance standards for his employees. (TR. #2, p. 79)

### DISCUSSION

The issue in this case is whether or not the positions which are sought to be accreted are “confidential” positions which must be excluded from collective bargaining as a matter of law. The current state of the law that defines a confidential employee is found in the Rhode Island Supreme Court’s decision in Barrington School Committee v. Rhode Island State Labor Relations Board, 694 A.2d 1185 (R. 1992). (Hereinafter “Barrington”) In Barrington, the Court adopted the “labor-nexus” test of determining whether a secretary was a “confidential” employee.

“Two categories of employees are recognized as confidential under the test and are therefore excluded from collective bargaining. The first category comprises those confidential employees who assist and act in a confidential capacity to persons who formulate, determine, and effectuate management policies in the field of labor relations. ... The second category consists of employees who, in the course of their duties, regularly have access to confidential information concerning anticipated changes which may result from collective bargaining negotiations. (Barrington at p. 1136, quoting NLRB v. Hendricks County Rural Electric Membership Corp., 454 U.S. 170 at 189)

In Barrington, the Court declined however to adopt the labor nexus test as necessarily controlling in all future instances. In so holding the Court said, “it may be that a broader definition of those employees considered to be ‘confidential’ would be desirable in other circumstances.” Id at 1137.

In this case, the Employer first urges this Board to find that the “systems administrators of computer systems at DOC should be considered confidential and excluded from bargaining.” In the alternative, the Employer argues that the DOC’s MIS unit employees serve as a “choke point” and have an ability to shut down the entire computer system because of their systems administration duties. Therefore, the Employer argues that this capability conflicts with the Director’s statutory ability to run a safe and secure prison system. Finally, the Employer argues that because MIS employees protect computer property and rules, they should be considered “guards”; and therefore, it is



inappropriate for them to be included within the proposed unit. (Employer's brief, p. 20)  
We shall address these arguments one by one.

First, there was simply no evidence set forth that the MIS employees assist and act in a confidential capacity to persons who formulate, determine, and effectuate management policies in the field of labor relations. Likewise, there was also not a shred of evidence that any of the employees in question, *in the course of their duties, regularly have access* to confidential information concerning anticipated changes which may result from collective bargaining negotiations. Any access that might be obtained to this information would be as unauthorized and unlawful as if they had broken into a locked filing cabinet and stolen the files or the information contained therein.

The next argument we take under consideration is the State's insistence that the facts presented in this case warrant an expansion of the labor nexus definition of confidential employee. This Board is mindful of the Barrington Court's reservation to apply the labor nexus test in all cases and we have carefully reviewed the facts of this case against arguments set forth by the Employer to determine whether or not this case does represent the type of circumstance in which the definition of "confidential" employee should be expanded beyond the narrowly defined "labor nexus" test. If the MIS employees truly have regular and uninhibited access to every "byte of information", including labor relations information, within the Department, *with no way for the Department to protect itself from unauthorized access to information*, then we might well indeed be persuaded to find that such employees stand in a confidential capacity and should not be permitted to engage in collective bargaining. Although the testimony on this subject was somewhat conflicting, for the following reasons, we are not persuaded that the employees in question have regular and uninhibited access to information that by its nature would make the employees "confidential."

Mr. Major testified that the employees in the MIS unit have a unique ability to gain access to all information contained on the computer systems. He also testified that Ms. Charette had the ability to obtain passwords, but has not had the occasion to do so in recent years because she has different responsibilities than she did in past years when there were less employees within the unit. (TR. #2, p. 78). In response to an inquiry on whether Ms. Charette has access to a list of all passwords, he replied "I'm only indicating that,

because she is what I call a systems administrator, or she has to be logged as a systems administrator to perform her normal duties.” When asked when was the last time she had the occasion to access a list of passwords, he replied “ I don’t know. As mentioned, that is not part of her normal daily process.” (TR. #2, p. 78) This Board is not convinced by this testimony that Mr. Major has first hand personal knowledge on what access Ms. Charette actually has. It appears to this Board that Mr. Major was engaging in some speculation or was actually testifying to her access in earlier years, prior to the Department’s reorganization.

In contrast to this testimony, Ms. Charette testified that she no longer has any access to systems administration within the LAN network and that on the E-mail system, she cannot find passwords for individuals, she would have to obtain that information from someone else. In fact, when she runs into a “locked ID” problem, she has to call Mr. Major or Ms. Lanciaux (even at home, where they have computers) so they can fix the problem. (TR. #2, p. 10-12). This testimony was unrebutted. This Board is convinced by Ms. Charette’s unwavering testimony that she does not have access to a list of passwords of DOC employees or that she can access other employees’ pass-worded files. In so holding, we do not mean to suggest that Mr. Major’s testimony was in any way untruthful, only that he believed that Ms. Charette’s potential access was greater than it actually is.

As for Mr. Pate, Mr. Major acknowledged that Mr. Pate did not have the security clearance to obtain passwords. (TR. #2. P. 66) Further, Mr. Major was not sure whether Ken Kard had that capability. (TR. #2. P. 66) In contrast, Mr. Kard testified that he cannot access password protected files, although if files are not password protected and the file resides on the LAN, instead of a floppy disk, or the individual user’s C-drive, Mr. Kard would be able to access the data inside the file. (TR. #2, p. 46, 51-52) He also testified that he does not have access to the VS system at all and that the only access he has is to his own E-mail. (TR. #2, p. 56)

The State’s next argument suggests and argues that the broad statutory authority of the Director of the Department of Corrections to run a safe and secure prison system, as well as management’s confidence in the computer system would somehow be compromised by the inclusion of these positions within the bargaining unit. Such an argument also implies that the computer system is safe from malfunction, if and only if, the

computer experts are excluded from collective bargaining.<sup>5</sup> This Board finds such an argument to be convoluted and highly speculative.

Furthermore, concomitant with the broad statutory powers of the director to run a safe and secure prison system are the director's duties to "direct employees in the performance of their official duties"; make and promulgate necessary rules and regulations regarding communication; and supervise the operations of the Department. The testimony established that the Department as a whole has not adopted any mandatory security measures to protect sensitive data. Employees tape their password to the front of their computers; they have been observed yelling a password across a room to other employees; they do not utilize passwords which would protect their individual files. Mr. Major acknowledged that the Department hasn't even discussed *the possibility* of requiring passwords as standard procedure. (TR. #2, p. 75) Further, sensitive data is not required to be kept on floppy disks (which cannot be accessed by third parties) hard drives, or on a passworded file. Contrast this general lack of accountability of all departmental employees with the formidable obstacles that face the MIS employees were they to attempt a surreptitious accessing of information on the systems. First, the Department has a Code of Conduct that prohibits unauthorized access to information and any employee violating the code is subject to disciplinary action, up to and including termination. (Also see testimony of Kevin Major at TR. #2, p. 78-81) Further, the unauthorized accessing of computer data is a felony offense under R.I.G.L. 11-52 et seq. In light of the foregoing, this Board finds that the circumstances presented do not warrant an expansion of the definition of "confidential employee" as that term is presently defined by the Rhode Island Supreme Court.

Lest the parties misunderstand the Board's findings, we wish to stress that we understand completely that some of the information residing on the computer system at DOC is critical to the functioning of the Parole Board, the State Police, the Attorney General and the Courts. There has been no evidence presented however that this data would be or could be compromised by the accretion of these position to the bargaining unit. In fact, the testimony established that there was a recent technological failure that allowed an unauthorized member of the Department to call up and access all department

---

<sup>5</sup> The State attached a newspaper clipping about computer sabotage by disgruntled employees to its brief.

files on her computer. All parties who testified to this incident agreed that they did not know technologically how this happened and that the MIS unit immediately took steps to try and figure out the problem. So, if there's a fear that the system could be compromised by the employees becoming members of the Union, the facts establish that this can and does happen independent of the employees status as bargaining unit members. The answer to keeping files secure is not to exclude employees from the protections and benefits of collective bargaining, the answer is to implement as many basic security measures as possible, along with any sophisticated measures which are appropriate.

The State also argues that these positions should not be accreted to the largest rank and file unit which consists of 78% of the Department's work force. The testimony established that there are already members of the RIBCO unit within the MIS department. In the course of their duties, Mr. Pate, Ms. Charette and Mr. Kard all have extensive interaction with RIBCO members. They all work in the same complex of buildings and they are all subject to the same code of conduct and code of ethics. Member of RIBCO input data into the computers and all employees have a group responsibility to provide accurate information which is critical to the functioning of the Parole Board, the State Police, the Attorney General and the Courts. Therefore, this Board finds that these employees are appropriate for accretion into the bargaining unit previously certified in EE 2003.

### **FINDINGS OF FACT**

- 1) The Respondent is an "employer" within the meaning of the Rhode Island State Labor Relations Act.
- 2) The Union is a labor organization which exists and is constituted for the purpose, in whole or in part, of collective bargaining and of dealing with employers in grievances or other mutual aid or protection and as such is a "Labor Organization" within the meaning of the Rhode Island Labor Relations Act.
- 3) The Employer does not have any policy or standard procedure that requires employees to store sensitive data in password protected files, or on floppy disks. Further, the Employer permits its employees to post passwords in plain view on the front of their computers and to call out passwords across a room.

- 4) Ms. Charette, Mr. Kard and Mr. Pate do not have access to password protected files unless they are given the password. Further, none of the three have access to a list of passwords.
- 5) The MIS unit at the DOC includes the positions of File Clerk, Clerk Typist, Assistant Supervising Data Entry Operator, Supervisor of Data Entry and the Principal Clerk Stenographer which are all members of RIBCO. There are also five lieutenants and two captains, also RIBCO members, in the unit.
- 6) Of the Employees holding the positions which are the subject of this accretion petition, only Mr. Kard testified that he has been called into work on occasion in the middle of the night. Otherwise, their typical work week is Monday through Friday from 8:30 am to 4:00 pm. They take turns being "on call."
- 7) Neither Ms. Charette, Mr. Kard and Mr. Pate assist or act in a confidential capacity to persons who formulate, determine, and effectuate management policies in the field of labor relations. Neither Ms. Charette, Mr. Kard and Mr. Pate in the course of their duties, regularly have access to confidential information concerning anticipated changes which may result from collective bargaining negotiations.
- 8) A technological error occurred in which an unauthorized person viewed and accessed all department files, without the appropriate clearance to do so. None of the employees in the MIS unit, including Mr. Major could explain how such an error could occur.
- 9) The MIS unit has a program to track unauthorized attempts to access computer files and can identify the perpetrator with this program.
- 10) Some MIS employees have the ability to "shut down" the computer system at the DOC and the same could also happen by accident.
- 11) Mr. Kard cannot access password protected files. If files are not password protected and the file resides on the LAN, instead of a floppy disk, or the individual user's C-drive, Mr. Kard would be able to access the data inside the file, however it would take some extensive programming in order to achieve the access.
- 12) Mr. Pate, Ms. Charette and Mr. Kard all have extensive interaction with RIBCO members. They all work in the same complex of buildings and they are all subject to the same code of conduct and code of ethics. Members of RIBCO input data into the

computers and all employees have a group responsibility to provide accurate information which is critical to the functioning of the Parole Board, the State Police, the Attorney General and the Courts.

### CONCLUSIONS OF LAW

- 1) The positions of Jr. Electronic Computer Programmer, Sr. Electronic Computer Programmer, and Principal Systems Analyst are neither supervisory nor confidential and are eligible to engage in collective bargaining.
- 2) The position of Information Aide was already included within the bargaining unit prior to this petition.

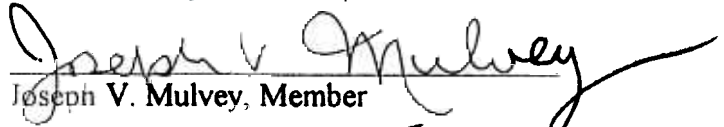
### ORDER

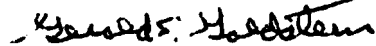
- 1) The positions of Jr. Electronic Computer Programmer, Sr. Electronic Computer Programmer, and Principal Systems Analyst are hereby accreted to the bargaining unit certified by Case No. EE-2003 on March 23, 1972.

### RHODE ISLAND STATE LABOR RELATIONS BOARD

  
Gina A. Vignetti, Chairperson, Dissent

  
Frank J. Montanaro, Member

  
Joseph V. Mulvey, Member

  
Gerald S. Goldstein, Member

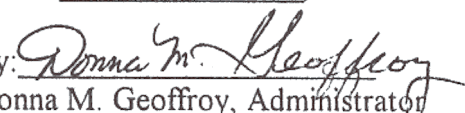
  
Ellen L. Jordan, Member, Dissent

  
Paul E. Martineau, Member

  
Joseph Virgilio, Member

Entered as an Order of the  
Rhode Island State Labor Relations Board

Dated: December 18, 1998

By:   
Donna M. Geoffroy, Administrator