COPY OF MEMO FROM N.J.S.P.

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC SAFETY
DIVISION OF CRIMINAL JUSTICE

MEMORANDUM

TO: AAG Ronald Susswein
Office of the Attorney General

FROM: DAG Thomas Fisken
Division of Criminal Justice

DATE: October 31, 2007

SUBJECT: Guidelines for Shared Police and Civilian Computer Systems

In 2000 the Attorney General issued guidelines regarding the police computer systems and restricting arrangements some municipalities were considering in order to merge police and civilian computer systems. The current guidelines require that police data be maintained on a separate server.

We recently received an inquiry from Assemblyman Scalera, on behalf of Nutley Township, where he also serves as a township Commissioner. Nutley is in the process of moving its email system to a private vendor who would maintain the system off site. The township would like to include the police department email system in this arrangement.

At our meeting on October 22, 2007 a working group of Department of Law and Public Safety staff reviewed the proposal to move the email system to a private vendor and discussed the security concerns raised by this proposal. The conclusion of staff participating in the meeting was that the guidelines should not be changed and the police email system should not be moved to an offsite vendor. The only manner in which the private vendor would be able to meet the standards of the existing guidelines would be if the vendor maintained the police email system on a separate server physically located in the police department.

The Attorney General's Guidelines governing Shared Municipal and Police Computer Systems were developed in 2000 in response to requests for advice on the topic from local police and the New Jersey Chiefs of Police Association. Police networks contain a great deal of confidential information which must be given the highest level of protection available. In keeping with that need the Guidelines require that police computer networks be controlled by a dedicated server, not physically or remotely accessible by non-police personnel, except for routine maintenance or repair. *Guidelines, paragraph 6.* Furthermore, Criminal Justice Information Systems (hereinafter CJIS) policy also dictates how a law enforcement agency handles its IT implementation because it is so closely intertwined with the use and management of Criminal Justice Information. CJIS Policy states that the storage and use of all CJIS related data must be housed in the control of a

Law Enforcement agency. This agency can be a Police Department, Prosecutor's Office, Sheriff's Office, Jail, or other law enforcement entity. The agency must maintain control over the resources that store and access CJIS information or risk having their access terminated. Since this restricted information can often be attached or cut and pasted into other files or email, this information is inextricably intertwined with police networks and email systems. The use of e-mail as an everyday business tool to communicate data is inherent in today's society. This means that it is used to communicate everything from case status to personal information on suspects. Separate and secure law enforcement systems help ensure compliance with FBI and CJIS mandates governing the sharing of law enforcement information.

E-mail, like other documents, must be stored on a server or workstation prior to distribution. This means that the storage device, namely a server must be housed in a law enforcement agency. The resource must be in a secured room with limited user access. IT staff concluded that the vendor's assertion that nothing will be stored or archived on the external server is a technical impossibility. It must be stored on the server or it will be lost to the system.

Accessing L&PS or NJSP e-mail through the State Portal from home is not similar to off-site storage and management by a vendor. The servers that store our e-mail systems are housed in a law enforcement building in a secured room. The State Portal is just an access method and allows for **encrypted** access to the data which then meets the CJIS mandate that requires remote access to any system be encrypted.

Other concerns raised at the meeting included the effect of broken Internet connections which would block access to the remote systems. Questions were also raised as to security measures that would be used to protect the backup media and the data on it? Anyone who has access to the backup media would also have access to the data. Finally, in the event of a breach of data security, the law enforcement agency would be forced to rely on the vendor in order to track the leak. Using an outside vendor to provide onsite support for the department's IT needs would be one possible solution. This would enable the Township to contract with one vendor while still meeting the mandate of having the systems secured in a law enforcement facility. The Township could also store the Township non-law enforcement server in the same room and still meet the same CJIS requirement. The fact that both systems would be located in the law enforcement site would allow them to reduce costs through shared location. The vendor would still have only one location to visit for support and the police department would be able to supervise access to the server, as required in the 2000 guidelines.

c: SDAG Hester Agudosi
DAG Dave Rebuck
Nick DeLuca CJIS Project manager
Maria Lapolla CIO DL&PS
Lt. Tom Coppola NJSP IT Unit
Kiran Patel OAG, IT Unit, IT Security Manager