

Hello Larry,

The following are items, screenshots, or information needed from your IT section, for us to continue our audit of the Bristol County Sheriff's office. As we already talked about, these requests are a routine auditing procedure and are not meant to imply any issues at the BCSO.

If you can please provide for us the following information at your earliest convenience, it would be much appreciated. If there are any questions on what I am referring to, please feel free to ask. Some terminology I use may not be the exact terminology utilized by your IT staff. I can always provide an example of what is needed via email if there are any clarification issues.

I broke down each request by item number and description below to help keep everything organized.

You can send me each request individually as they are obtained, just as long as each one is clarified to which question it is in reply. The I can cross it off the list one by one.

Thanks so much

Lou

Louis E. Bertolino

Senior Auditor II

Office of the State Auditor

1 Winter St. 9th Floor

Boston, MA 02108

857-294-8708

{ [HYPERLINK "mailto:Louis.Bertolino@massmail.state.ma.us"](mailto:Louis.Bertolino@massmail.state.ma.us) }

IT requests: (emails and scans will work fine)

1- A copy of the IS (IT) Security plan

2a- A list of all employees (contractors, and vendors) with any access to a computer on the BCSO network.

2b- To be determined once I obtain the list from 2a

2c- to be determined once I obtain the list from 2a

2d- a list of all terminated users in the last 30 days

2c- a list from HR of all users who were transferred or promoted in the last 30 days. I will need to determine if those users had their access rights updated to reflect their new roles.

3- A screen shot of the “account lockout” settings for users on the network. Example- a user is locked out after x amount of incorrect password entries.

4- A screen shot showing if a user’s session is terminated after a specified period of inactivity

5- I’ll need some sort of evidence if possible showing that user access is reviewed annually. If a policy exists in your IT security plan, please provide the location (in case I can’t find it myself) . Most places have a form upon hire, of one’s user access privileges, and annually that form is either signed or reviewed showing that particular employee access rights have been reviewed in some way.

6- a copy of the “security awareness policy” (if it’s part of your IT security plan, just provide the location page)

7- a list of your last 10 hires (or new users) , and provide a scan or screen shot of their signed copies in of their participation in security awareness training upon hire.

7b- a scan or copy of those same peoples annual refresher training. (if they haven’t been hired longer than 1 year, that’s ok.)

8- A copy of your “IT audit policy” (if its part of your IT security plan, please point out to its location.)

9- A screen shot of your “audit logs” that will show various “auditable events” example- failed logon attempts, privileged user activity etc

10a- A screen shot of the maximum size of the “audit log”

10b- A screen shot of the setting showing what happens when the audit log is full. Example- is it overwritten, moved to another location, or stop logging)

11a- A listing of all audit logs for the last 30 days.

11b- Provide evidence that those logs were reviewed. (Signatures on a log, or a memo to someone stating logs were reviewed, etc)

11c- if there were any negative events on the last 30 logs, please provide what corrective activity took place regarding such activity.

12- A copy of the “configuration Management policy” (this policy should address items regarding updates to your software, patches, configuration changes etc.)

13- If there were any major software changes in the last 6 months, please provide any documentation that testing has been performed on that new software, prior to its implementation.

14- A screen shot of your “identification and authentication” policy. This policy normally addresses minimum password lengths, password expirations, requirement of special passwords etc.

15- A screen shot of the password complexity settings

16- a copy (if it is not already provided in any of the above copies) a “personnel security policy”. Which details any pre-employment screening, requirements on special skills or knowledge, applicant verifications, requirements of cori checks etc. (this may come from HR)

17- To be determined once I have the results of question 2a