Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in summary report of common cybersecurity mistakes

User Access Management	Access to certain systems is not adequately restricted. The user access of former employees is not disabled timely.
User Authentication	Passwords are not required to be changed on a periodic basis. User accounts and passwords for accessing computers and various systems are shared by users. A password is not required to logon and authenticate access to a computer. Passwords are not required to contain a minimum number of characters.
Security Controls	Inactivity controls have not been implemented to lock a computer or system after a certain period of inactivity. Security controls have not been implemented to lock access to a computer or system after a specified number of unsuccessful logon attempts. Malware or antivirus protection software to detect and eradicate malicious code has not been installed on computer systems.
Backup and Recovery	Data in various systems is not periodically backed up. Data backups are not stored at a secure off-site location. Periodic testing of backup data is not performed. Management has not developed a formal contingency plan to ensure business operations and computer systems can be promptly restored in the event of a disaster or other disruptive incident.
Data Management and Integrity	Data management and integrity controls to guard against the improper modification or destruction of data and information have not been implemented. In addition, audit trail controls to provide evidence demonstrating how a specific transaction was initiated, processed, and recorded have not been established.

Because of the nature of this report, no rating has been provided.

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.