STATE OF WYOMING
DEPARTMENT OF AUDIT

PUBLIC FUNDS DIVISION
(307) 777-7798 Fax (307) 777-5341
pam.robinson@wyo.gov

Matthew H. Mead
Governor

Jeffrey C. Vogel
Director

Pamela Robinson
Administrator

MEMORANDUM

DATE: June 10, 2015

TO: Members of the Task Force on Digital Information Privacy

FROM: Justin Chavez, School Finance Audit Manager, Wyoming Department of Audit

SUBJECT: School Data Security

SUMMARY

What We Do
- General controls review (look at policies and procedures) over student information systems and make some observations about those systems as we are performing ADM testing
- General controls review over district-wide systems
- IT audits (high-level – look at configurations and settings) for a small number of districts

Findings
- Generally fairly weak logical and physical security
- 42 of 48 districts on the statewide ADM audit had some degree of findings related to weaknesses in security of student information systems (unencrypted connections, weak passwords, no audit trail, etc.)
- 14 of 48 districts were not using encrypted connections for Internet-based student information systems

Causes
- Personnel charged with managing the systems are unaware of security issues
- Policies/Procedures/Settings used out of convenience rather than security

Recommendations
- Create minimum security requirements (statute, WDE rule, ETS, etc.)
- Require comprehensive written IT policies and procedures
- Training (WDE/ETS?)
- Oversight (audits/reviews?)

DETAIL

As part of our normal auditing of ADM for the purposes of district funding, we perform a general controls review over the student information system. A general controls review is a high level review in which we for the most part look at policies and procedures regarding authentication and authorization (user IDs, passwords, who has access to what data, etc.). We also make observations about the system while performing our ADM testing. For example, we

note if the system is using an encrypted connection, if incorrect password attempts are logged, or if we can be logged in for extended periods of time of inactivity. We also perform this same type of review for the district networks as a whole. Additionally, we have performed more in-depth IT auditing of a few districts. For these audits, we go beyond policies and procedures and look at settings and configurations of systems.

In general, both physical and logical security tends to be on the weaker side. Physical security refers to protection of the actual equipment – in other words, are the servers, routers, switches, etc. located in a restricted area in which only authorized personnel have access? Logical security refers to passwords and who can access particular data on the network. Passwords tend to be short and are generally not required to be changed on a regular basis. Additionally, we have seen instances of accounts without lockouts after a certain number of failed login attempts or too many attempts are allowed before the lockout. We also have seen extended session timeouts – in other words, someone can log in and his/her account will stay logged in for a long period of time without any activity. Going beyond security of student information systems, other security concerns have been identified such as community administrator accounts (one account with administrative rights being used by multiple people), unnecessary services running on servers, and default accounts and passwords not being disabled.

In determining the primary cause for our findings, most of them fall into one of two categories. The first category is district personnel being unaware of security issues. It appears IT expertise might be hard to come by, especially in smaller districts. The second category is emphasis on convenience rather than good security practices. For example, when we ask why short and simple passwords are allowed or why there are extended session timeouts, the response many times is because personnel complain about having to have long passwords or having to change them regularly or having to log in multiple times during the day.

To address the concerns identified, there are a few recommendations. Most districts do not have comprehensive IT policies and procedures in place to address the concerns identified. Comprehensive policies and procedures are a first step toward reducing the risk of these issues. To help accomplish this, some training may need to be provided to districts. For example, WDE provides training to districts on a myriad of issues related to school data and this may be an area that can be addressed. It may also be beneficial for some minimum security guidelines to be established, whether through statute or rule. Finally, the Department of Audit could provide oversight through IT audits since we visit each district on a regular basis and work regularly with the data housed by these systems.