MONTANA UNIVERSITY SYSTEM
OFFICE OF COMMISSIONER OF HIGHER EDUCATION

560 N. Park, 4th Floor – PO Box 203201 – Helena, Montana 59620-3201
(406) 449-9124 - FAX (406) 449-9171

September 9, 2022

Angus Maciver, Legislative Auditor
Legislative Audit Division
P.O. Box 201705
Helena, MT 59620-1705

Dear Mr. Maciver:

Please find the attached progress report from the Office of the Commissioner of Higher Education (OCHE) on the information security audit of the Montana University System (MUS), which includes updates for all four audit recommendations. The recommendations from the audit have resulted in increased communication and coordination related to MUS information security and encouraged the advancement of IT governance and information security programs across the system.

Sincerely,

Clayton T. Christian
Commissioner of Higher Education

Montana University System

Progress Report: Information Security in the Montana University System

Recommendation #1

We recommend that the Board of Regents and the universities review and enforce university system security policy that includes:

A. Clear direction within policy to manage a security program and mandate a consistent security framework, going above and beyond maintaining security policies.
B. Requirements for Board of Regents security policy to be reviewed continuously.

Concur. OCHE concurs with this recommendation and recognizes one of the best ways to establish IT governance is by instituting and communicating effective governance policies including a consistent framework for how to approach security throughout the MUS.

OCHE will establish a workgroup comprised of the Commissioner's staff and university system stakeholders to identify and analyze security frameworks and their applicability to the MUS. Based on the recommendations of the workgroup, OCHE will recommend to the Board of Regents a governance approach that will ensure security controls are implemented across the MUS in a manner that will most effectively protect sensitive MUS information.

These recommendations will be incorporated into Board policy and approved by January 2023. OCHE staff will continue to convene the workgroup to ensure security policies and/or procedures are reviewed continuously.

Progress to Date: A systemwide workgroup was formed and began meeting regularly at the end of May. Several information security documents have been developed to ensure that key aspects of governance are understood throughout the MUS.

A revised BOR security policy will be presented to the Board as an information item on September 21 with Board action to follow in November. The revised policy clarifies roles and responsibilities, strengthens language around NIST standards, formalizes communication to the Board related to information security, and ensures that internal/external assessments of MUS security programs are conducted.

See attached list of meeting dates, topics discussed, and associated documents that were produced.

Progress Report: Information Security in the Montana University System

Recommendation #2 (University of Montana)

A. Update and formalize job descriptions for positions that have responsibilities for developing, maintaining, or supporting the security program.

The University concurs. Role descriptions for key positions overseeing the security program have not changed since they were revised and communicated to the incumbents in 2020. The University notes that the role descriptions reviewed during this audit were formatted differently and will ensure that the same template is used for all role descriptions. This corrective action plan will be implemented by June 30, 2022.

B. Complete a comprehensive IT risk assessment that is used to develop strategic initiatives and the required budget to mature the security program and security awareness.

The University concurs. The University will complete a comprehensive IT risk assessment and implement strategic initiatives with an eye toward maturing the security program and increasing security awareness. This corrective action plan will be implemented by June 30, 2023.

Progress to Date: The role descriptions for the Information Security office have been reviewed and updated using consistent formatting. This includes the Chief Information Security Officer, Information Security Officer, Identity Management Systems Analyst, Identity Management Systems Applications Programmer, and IT Security Analyst (currently vacant). *See attachments*.

The University engaged the Department of Homeland Security regarding CISA cybersecurity services. Following review and discussion by the flagship CIOs and the IT governance workgroup, we determined that a more robust assessment was necessary. In coordination with OCHE, UM and MSU have selected CampusGuard Services to conduct separate but similar assessments at each campus using the NIST Cybersecurity Framework, including a risk assessment specific to the Gramm Leach Bliley Act (GLBA). The UM assessment will include a risk analysis matrix that details high-risk findings specific to UM and provide recommendations for curative actions. We have initiated the procurement process to obtain this service. UM has also allocated resources to procure GRC software to support the alignment of information security governance, risk management, and compliance.

Montana University System

Progress Report: Information Security in the Montana University System

Recommendation #3 (Montana State University)

We recommend the Montana State University complete a comprehensive IT risk assessment to develop a formal approach for maturing security procedures.

Response:

Montana State University concurs with this recommendation. Our Corrective Action Plan includes the following:

- The more formal adoption of an information security related framework to further assess existing controls and procedures and further understand and address risk.
- The more formal assessment of risk specifically related to the Gramm-Leach Bliley Act.
- The documentation of how existing controls address risks identified in the Gramm-Leach Bliley Act more formal risk assessment.

Montana State University plans to complete this Corrective Action Plan by April 1, 2023.

Progress to Date: The University engaged the Department of Homeland Security regarding CISA cybersecurity services. Following review and discussion by the flagship CIOs and IT governance workgroup, we determined that a more robust assessment was necessary. In coordination with OCHE, UM and MSU have selected CampusGuard Services to conduct separate but similar assessments at each campus using the NIST Cybersecurity Framework, including a risk assessment specific to the Gramm Leach Bliley Act (GLBA). The MSU assessment will include a risk analysis matrix that details high-risk findings specific to MSU and provide recommendations for curative actions. We have initiated the procurement process to obtain this service.

Montana University System

Progress Report: Information Security in the Montana University System

Recommendation #4

We recommend that the Board of Regents establish system-wide IT governance that ensures:

A. OCHE has an active role in improving security posture of the university system,
B. Security policy addresses the requirements of data security statute and other relevant federal requirements,
C. There is clear allocation of security responsibility, authority, and accountability, and,
D. Communication and reporting mechanisms are formalized between various entities that oversee or make decisions within the university system.

Concur. As mentioned above as part of efforts related to Recommendation 1, OCHE will establish a workgroup comprised of the Commissioner's staff and university system stakeholders to further develop and inform Board policy and IT governance practices across the MUS. This process and its outcome will ensure that OCHE has an active role in improving the security posture of the MUS, and that clear lines of security responsibility and authority are established. Additionally, the collaboration with university partners will enable OCHE to better align existing MUS security practices with statutory and federal requirements, as well as with a more deliberate security framework.

Formalized communication in this risk area is already planned as part of the MUS enterprise risk management (ERM) process initiated by the Board of Regents. Information security has been identified as a system-wide risk, and as part of the ERM process, the workgroup will have a reporting line to the Board of Regents through our MUS Risk and Compliance Leadership Council.

Lastly, the process described above will help OCHE determine what resources are needed across the system and/or at OCHE to support IT governance and information security across the MUS. OCHE will identify any additional resources needed by April 2023.

Progress to Date: A systemwide workgroup was formed and began meeting regularly at the end of May. Through formalized communication between the Board, the Deputy Commissioner for Budget and Planning, and the flagship CIOs, as well as revisions to the Board information security policy and governance practices, OCHE has ensured that it has an active role in improving the security posture of the MUS.

As mentioned, the revised BOR security policy will be presented to the Board as an information item on September 21 with Board action to follow in November. The revised policy clarifies roles and responsibilities, strengthens language around NIST standards, formalizes communication to the BOR related to information security, and ensures that internal/external assessments of MUS security programs are conducted. The MUS enterprise risk management process also helps minimize the extent to which information security risks impede the MUS mission by helping to ensure the MUS allocates resources appropriately.

Additionally, cybersecurity is an MUS legislative initiative and OCHE has requested funding through the executive budgeting process to (1) develop and maintain comprehensive system-level infrastructure to support cybersecurity in the MUS and across all MUS institutions; and (2) establish a leading cybersecurity training and education center through the University of Montana, Missoula College, to prepare the next generation of cybersecurity professionals to meet the needs of Montana businesses. *See attached fact sheet.*