MINUTES

HOUSE ENVIRONMENT, ENERGY & TECHNOLOGY COMMITTEE

DATE:	Wednesday, February 08, 2017
TIME:	1:30 P.M.
PLACE:	Room EW41
MEMBERS:	Chairman Raybould, Vice Chairman Thompson, Representatives Hartgen, Vander Woude, Anderson, Anderst, Mendive (Mendive), Trujillo, Chaney, Nate, Cheatham, Horman, Malek, Moon, Smith, Scott, Jordan, Rubel
ABSENT/ EXCUSED:	None.
GUESTS:	Susan Buxton, DHR; Jack Lyman, Idaho Housing Alliance; Lance Wyatt, OCIO; Greg Zickau, Department of Administration.

Chairman Raybould called the meeting to order at 1:31 p.m.

MOTION: **Rep. Rubel** made a motion to approve the minutes of February 6, 2017. **Motion carried by voice vote.**

Lieutenant Governor Brad Little presented information on the formation of the Governor's Cybersecurity Task Force, saying that technology moves at a high rate of speed, doubling every 18 months, while state government regulation moves slowly. The public expects online access and an open and transparent government but state data and citizen's privacy are at risk if we don't accelerate their protection. The magnitude of urgency on dealing with cyber crime is greater than it ever has been before. Originally, hackers were young kids and malcontents, but today, they can be enemy states and organized crime. Some state agencies, like Health and Welfare and the Idaho Tax Commission already have robust systems in place. The Department of Administration headed up mandatory meetings of all state technical personnel and presented their recommendations to the Governor. **Governor's Executive Order 2017-02** created a director of information security position in the Governor's office to: 1) ensure the Department of Human Resources addresses employee education and training; 2) adopt National Institute of Standards and Technology (NIST) standards and best practices and implement Critical Security Controls (CSC); and 3) develop a public outreach program to citizens, other levels of the government and the business community, with the goal for Idaho to be the most secure place to do business. Legislators will be hearing about the costs because software and hardware programs are needed to implement the higher standard.

Lt. Governor Little responded to committee questions regarding system access and costs by informing the committee members the first thing they would do is data mapping to find out where the data is and how sensitive it is. Access levels will be determined and mandatory training will be for the highest level of security training, money won't be spent on training for lower access levels. There will be some people whose access is lowered as part of this project. Currently, this type of expense is imbedded in agencies' budgets, and is not a line item, so it is hard to determine how much is currently spent.

Lt. Governor Little introduced **General Brad Richy**, Director, Idaho Division of Emergency Management, who stated that from July 2015 to the beginning of 2016, the task force identified threats and vulnerabilities in state technology systems and cyber daily operations and developed recommendations for best practices. He explained that Lt. Governor Little took Idaho from cyber awareness into cyber knowledge. Commencing in April 2016, they looked at breaking cyber down in the general direction it should go, and divided into work groups: 1) Financial, 2) Education and Training, 3) Information and Technology Sharing, and 4) Governance. General Richy consulted with the Governance work group, who evaluated whether Idaho should have a centralized system, a federalized system or a hybrid of the two. They first decided that cyber needed to include information technology and cyber needed to be centralized. The consensus was for a federalized IT system with centralized security and that NIST are the best standards allowing for a common language and framework that every state agency needs to incorporate. Five CSC were decided upon, and by June 30, 2017, the standards and CSC need to be incorporated.

General Richy replied to committee questions about working with other states and the federal government by indicating that if the state implements NIST best practices, it would accomplish what the federal government wants accomplished as a framework. Some state agencies by the nature of their program are tied into the federal system, and our system will communicate with any federal systems. Regarding working with power companies on cyber security, he replied that he does coordinate with our power companies to monitor their cybersecurity, and that every year, the Office of Emergency Management (used to be Homeland Security) conducts an exercise with the power companies to find out what threats there are, what mitigation factors are put into place to help avoid and constantly monitor them, and to put together a good working plan. Power companies are a challenge nationwide because they are so vulnerable to bad actors who are trying to get in and evaluate to see how the system works. There is a nationwide effort being put together through FEMA called Black Sky to look at long term complications of power outages, as well as restoration processes. In response to committee questions regarding costs to Idaho, General Richy replied that he does not anticipate any federal funding to implement hardware and software standards across the states. Idaho Fish & Game did have a security breach earlier this year, which is a learning opportunity, Idaho purchased cyber insurance to mitigate long-term liability in the case of a cyber breach.

ADJOURN: There being no further business to come before the committee, the meeting adjourned at 2:14 p.m.

Representative Raybould
Chair

Lorrie Byerly
Secretary