VII. STATE LIBRARIAN'S REPORT

A.2 Operations - Cybersecurity Executive Order – Information Item

The Governor signed Executive Order 2017-02 (below) on January 16 to start implementation of the recommendations of his Cybersecurity Task Force.

The process to appoint the Director of Information Security is still underway. In the meantime, agency directors were directed to take 3 actions by April 16, 2017:

- Sign a memo acknowledging that the agency has adopted the NIST (National Institute of Standards and Technology) Cybersecurity Framework and will ensure implementation by June 30, 2017 (#2 in the Executive Order). A draft Version 1.1 of the Framework, updated to refine, clarify, and enhance Version 1.0, is currently open for public comment. It is a voluntary set of industry standards and best practices to help organizations manage cybersecurity risks.
- Decide to implement the Framework with our in-house IT staff or through the Office of the Chief Information Officer. Considering our IT staff consists of 1.0 FTP, with backup and guidance from the Administrative Services Manager, we chose to implement the Framework by having OCIO house and configure the necessary hardware and software, with our IT Systems Technician maintaining access to and control of the servers remotely. We do not yet have a cost estimate for the hardware, software, or OCIO fees and no funds were appropriated to cover implementation costs.
- Submit the outline of an agency cybersecurity awareness training plan (#5 – 7). We again had the choice of using in-house curriculum or a curriculum recommended by the Division of Human Resources with identified objectives and minimum requirements (yet to be developed). We chose DHR's curriculum. The plan included our timeline for current and future employees completing the training, and identified the employees who have elevated access to our IT systems and will need advanced training.

Item #3 in the Executive Order requires agencies to implement the first 5 Center for Internet Security Critical Security Controls (a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyberattacks) for evaluation of existing state systems by June 30, 2018.

THE OFFICE OF TH E GOVERNOR

EXECUTIVE DEPARTMENT

STATE OF IDAHO
BOISE

EXECUTIVE ORDER NO. 2017-02

FINDINGS OF THE IDAHO CYBERSECURITY
CABINET TASK FORCE

WHEREAS, Executive Order 2015-07 established the Idaho Cybersecurity Task Force (Task Force) to detect and identify threats and vulnerabilities in state government networks; and

WHEREAS. Executive Order 2015-07 directed the Task Force to make recommendations on best practices to manage and reduce cyber risks; and

WHEREAS, the members of the Task Force have met with national experts, business and industry experts and counterparts in other states to understand best practices in cybersecurity; and

WHEREAS, the Task Force has finalized a list of initial recommendations;

NOW. THEREFORE, I, Cl. "BUTCH" OTTER, Governor of the State of Idaho, by virtue of the authority vested in me under the Constitution and the laws of this state, do hereby order:

1. *The appointment of a Director of Information Security reporting directly to the Governor to oversee implementation of statewide cybersecurity policies, ensure compliance with this executive order, and develop a potential audit process.*

2. ***All state agencies to immediately adopt and to implement by June 30, 2017, the National Institute of Standards and Technology (NIST) Cybersecurity Framework in order to better foster risk and cybersecurity management communications and decision making with both internal and external organizational stakeholders.***

3. ***All executive branch agencies to implement the first five (5) Center for Internet Security Critical Security Controls (CIS Controls) for evaluation of existing state systems by June 30, 2018. Updates on adoption of the NIST Cybersecurity Framework and implementation of CIS Controls will be included in each agency's strategic plan submission to the Division of Financial Management (DFM).***

4. *The State Department of Administration to facilitate annual penetration tests and annual vulnerability scans on state technology systems in order to identify steps to mitigate identified risks. All reports generated from these activities should be made available to the Director of information Security.*

5. ***The State Division of Human Resources, in conjunction with all executive branch agencies to compile and review cybersecurity curriculum for mandatory education and training of state employees, and to determine appropriate levels of training for various classifications of state employees.***

6. ***All executive branch agencies to develop employee education and training plans and submit such plans within 90 days of the issuance of this executive order to the Director of Information Security. The plans shall describe how existing and new state employees will receive the statewide mandatory education and training module on cybersecurity before being granted access to state systems.***

7. ***All executive branch agencies to require that all state employees complete the state's annual cybersecurity training commensurate with their highest level of information access and core work responsibilities.***

8. *The State Department of Administration, in collaboration with the Director of Information Security and the Idaho Office of Emergency Management, to create, coordinate, publish, routinely update and market a statewide cybersecurity website as an information repository for intelligence sharing and cybersecurity best practices.*

9. *The Director of Information Security, in order to promote the cyber resiliency of the entire State of Idaho, to develop a public outreach program for local government, private business and Idaho citizens to share best practices and current information regarding cybersecurity.*

10. ***All public-facing state agency websites to include a link to the statewide cybersecurity website — www.cybersecurity.idaho.gov.***

IN WITNESS WHEREOF, I have hereunto set my hand and caused to be affixed the Great Seal of the State of Idaho at the Capitol in Boise on this 16th day of January, in the year of our Lord two thousand and seventeen and of the Independence of the United States of America the two hundred .forty-first and of the Statehood of Idaho the one hundred twenty-seventh.

C.L. "BUTCH" OTTER
GOVERNOR

LAWERENCE DENNEY
SECRETARY OF STATE