Good afternoon Task Force members. Don't forget to register for the upcoming NCSL Executive Task Force on Cybersecurity in **Denver, Colorado on Friday, May 11th** at the J.W. Marriott, in conjunction with the NCSL Executive Committee Meeting.

The task force will host a dinner Thursday evening, May 10th and all the details as well as the proposed session topics can be found on our task force website. Click here to register for the meeting and the dinner Thursday evening.

Also in Cyber Task Force news:

Task Force Highlights

The Task Force will be taking up many important topics at our next meeting in Denver, on May 11th. We will hear from Oklahoma's Chief Information Officer Bo Reese, regarding Oklahoma's IT unification of systems and resources and how this process resulted in reduced spending and projected savings in that state. We will also hear from Debbi Blyth, the Chief Information Security Officer in Colorado who will discuss Colorado's ramped-up threat detection and prevention program. We will also hear from our own Sean McSpaden and Monique Appeaning who worked tirelessly on the Task Force's latest work product, "Budgeting For Cybersecurity."

If Task Force members have a session idea that they would like to see programming on, please let us know!

Task Force Website Gets a New Look

The Cybersecurity Task Force website now has a more colorful and streamlined look. Tabs have been added to make current information easier to find while still providing information from past meetings and different types of resources. Let us know how you like it and if you have other suggestions for the website.

Partner Highlight

NASCIO Highlights Best Practices for CISOs on Election Security

The National Association of Chief Information Officers is sharing a [Cyber tips for elected officials and candidates](#) product developed by a few of their state chief information security officer members. The document relies on the expertise of CISOs who have had personal experience helping elected officials respond to and recover from cyber threats, and developed the document to raise awareness. Follow up questions can be directed to our [NASCIO partner](#).

Security Tip of the Month: Using Virtual Private Networks

The Federal Trade Commission acknowledges that "you probably know by now that using your mobile device on the public Wi-Fi network of your local coffee shop or airport poses some risk. Public networks are not very secure – or, well, private –which makes it easy for others to intercept your data. So, what can you do to keep your mobile data private and secure while out and about? Some consumers have started using Virtual Private Network (VPN) apps to shield the information on their mobile devices from prying eyes on public networks. Before you download a VPN app, you should know that there are benefits and risks." [Read more](#).

Cyber Education–Building a Universal Language on Cybersecurity Curriculum

The Joint Task Force on Cybersecurity Education (JTF) published a comprehensive [curricular guidance in cybersecurity education](#) document developed in collaboration with major international computing societies and was co-chaired by Diana Burley, Ph.D. from the George Washington University in Washington, D.C. and Matt Bishop Ph.D. from the University of California, Davis, California.

The JTF hopes the document will be a living document that can improve with further community engagement and as a growing resource for institutions seeking to develop cybersecurity programs. They are also working with industry and government to illustrate how the curricular can be linked to workforce requirements as described in position descriptions. JTF was launched in September 2015 with the purpose of developing comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts. NCSL Cybersecurity Task Force will discuss ways to further engage on the topic of cyber education curriculum development and implementation in state schools during the May 11th task force business meeting.

The full document is available for download from their [website](#).

Articles We Are Reading

National Association of Secretaries of State on Colorado Election Security

Colorado's election security program is a finalist for the National Association of Secretaries of State (NASS) annual 2018 IDEAS innovation award. The award honors efforts cutting-edge work in states and would highlight Colorado's "Cybersecurity Protects Election Integrity" initiative. The "IDEAS" acronym reflects the award's focus on innovation, dedication, excellence and achievement in service. The winner will be announced during NASS's summer conference in Philadelphia, more information can be found [here](#).

GovTech on the Cybersecurity Workforce
One of the biggest challenges that organizations face as they try to keep up with a growing number of cyberattacks is finding workers with the right skills. Some states are addressing this problem head on. Programs in Georgia, Virginia, and Ohio offer lessons for other states on how to increase the pool of cybersecurity professionals and encourage students to pursue the profession.

GovTech's full article is found here Boosting the Cyberworkforce.

Federal Activity

U.S. Senate Introduces Bill for Funding State Elections Infrastructure

Senator Menendez (New Jersey) introduced a bill that would authorize $2.5 billion in grants to the states for Fiscal Years (FY) 2019-28 to carry out upgrades to state and local election infrastructure, including improving the process for audible paper ballots, conducting risk-limiting audits, and implementing cybersecurity standards and best practices.

Department of Energy has a new Cybersecurity Office

Department of Energy (DOE) announced the formation of a new Cybersecurity, Energy Security, and Emergency Response office. The FY 2019 White House budget request includes $96 million for the office, which would oversee 'elevating the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to natural and man-made threats."

The official notice can be found here.

State Activity

Security Breach Laws
All 50 states now have a security breach notification law. In March, South Dakota and Alabama became the 49th and 50th states to enact a security breach law.

South Dakota's S.B. 62 requires information holders to disclose any breach of system security to residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person. The law requires that the notification take place not later than 60 days from the date of discovery or notification of the breach. The law also requires information holders to notify consumer reporting agencies.

The Alabama Legislature passed S.B. 318, which requires private and public entities to establish reasonable data security measures and notify those affected when personal data has been

compromised. Notification is required if it is determined that the breach is reasonably likely to cause substantial harm, in which case notification is required no later than 45 days after discovery.

At least 30 other states in 2018 are considering measures that would amend existing security breach laws. See NCSL's 2018 Security Breach Legislation for more information.

- Registration is open for the 2018 NCSL Legislative Summit in Los Angeles. Register Here

NCSL Cybersecurity Staff: Susan Parnas Frederick (susan.frederick@ncsl.org), Danielle Dean (danielle.dean@ncsl.org), Pam Greenberg (pam.greenberg@ncsl.org, and Heather Morton (heather.morton@ncsl.org)