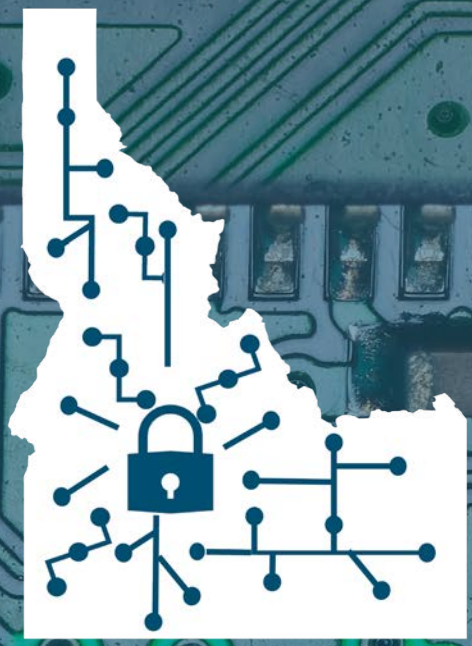
# Governor's Cybersecurity Task Force Report



March 2022

IDAHO COMMERCE

INL Idaho National Laboratory

# Table of Contents

# From the Governor

Cybersecurity attacks pose an increased and significant risk to all citizens, businesses, critical infrastructure operators, and state and local governments.

To meet the increasing threat and leverage Idaho's resources and expertise, Governor Brad Little created the Governor's Cybersecurity Task Force.

Governor Little convened the Cybersecurity Task Force to focus on promoting improved business, government, and personal cybersecurity. The task force is also focused on ensuring secure, transparent, and resilient election infrastructure and enhancing the educational pipeline for cybersecurity workforce needs.

The members of the task force, co-chaired by Idaho Department of Commerce Director Tom Kealey and Idaho National Laboratory Associate Laboratory Director Zach Tudor, represent a diverse range of expertise and experience in cybersecurity initiatives.

**Idaho Governor Brad Little**

***"Through the Idaho National Laboratory, the State of Idaho is home to unique and world-leading capabilities in countering cyberattacks and engineering solutions to the cybersecurity challenges facing our state and nation. We'll need increased resources, partnerships, and active collaboration between a broad range of organizations to successfully protect from ever-growing cybersecurity threats, and I'm confident my Cybersecurity Task Force is up to the task."***

**- Governor Brad Little**

# Welcome from the Co-Chairs

Welcome to the final report of Idaho Governor Brad Little's Cybersecurity Task Force. We hope you find the recommendations in this document useful as the state continues to make strategic investments in cybersecurity and prepares the State of Idaho for the ever-changing cybersecurity landscape.

The State of Idaho is home to unique and world-leading capabilities in countering cyberattacks and engineering solutions to the cybersecurity challenges facing our state and nation. However, the citizens, businesses, critical infrastructure operators, and state and local governments that call Idaho home, all face an increasing and significant risk of cyberattacks. It was this increasing threat that led Governor Brad Little to create the Governor's Cybersecurity Task Force in August 2021 and leverage Idaho's resources and expertise.

When we set out last fall with our private and public sector partners, we knew we would not be able to address the entire scope of cyber needs in the state. However, with the great work of the expert and dedicated task force and committee members, we made important progress in developing relationships, proposing recommendations, investments, and completing other important actions.

It was our pleasure to serve in the capacity of co-chairs for this important task force. However, there is more work to do. We view this report as a starting point for future discussions and actions needed for the State of Idaho and welcome additional conversations.

Tom Kealey
Idaho Commerce

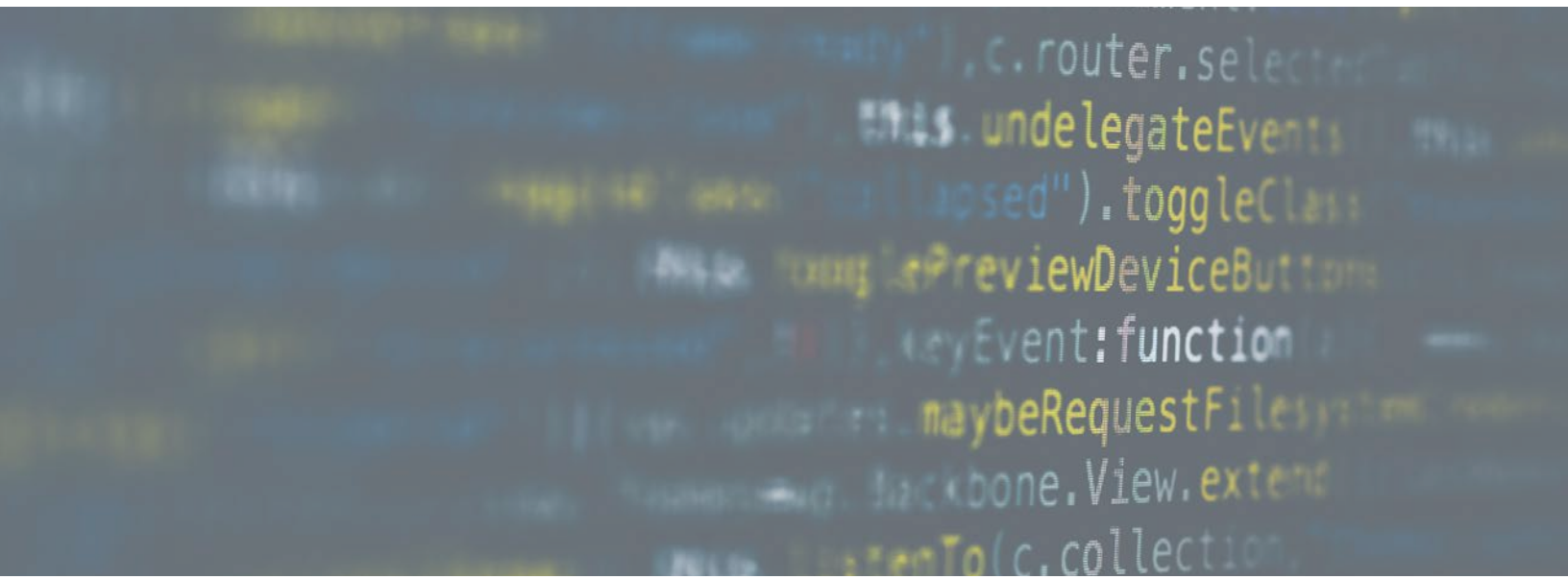
Zach Tudor
Idaho National Laboratory

# Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) was established in November 2018 when former President Donald Trump signed into law the Cybersecurity and Infrastructure Security Agency Act. Soon after, in 2019, Congress passed legislation establishing the Cyberspace Solarium Commission to develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences[1]. After two years of research, hearings, expert analysis, debates, and discussions, the commission's recommendations make one thing absolutely clear. We are a nation at great risk.

As the commission's report notes, domestic and foreign actors including China, Russia, Iran, and North Korea have used cyberspace for two decades to subvert American power and security. Be it the theft of intellectual property, the probing of our critical services, or election interference, malicious cyber actors have operated with impunity. And even though our digital connectivity has brought economic growth, technological dominance, and an improved quality of life to nearly every American, it has also created a strategic dilemma. The more digital connections people make and data they exchange, the more opportunities adversaries have to destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions. When the commission's work ended in late 2021, the U.S. was coming off one of the worst years for high-profile cyberattack events. The year began with a massive supply-chain assault on SolarWinds Corporation and ended with breaches on critical infrastructures in Florida, Georgia, and Colorado.[2,3,4,5]

Although the report and recent events strike a stark tone about the state of cybersecurity in the United States, the news is not entirely bad. In fact, the very purpose of the commission was to get the country's cyber house in order before a crippling multi-sector, multi-day cyber incident. Among the 82 recommendations the commission made, several focused on support the federal government should provide to local, state, tribal, and territorial governments including access to more funding, response resources, and training. It is under the pretext of preparation before a major cyber event occurs in Idaho, that the Governor's Cybersecurity Task Force was chartered and commissioned.



## A Word About Current Affairs

As this report was being written, Russian military forces were engaged in an unprovoked attack on the neighboring country of Ukraine. For weeks leading up to this conflict, U.S. officials had warned the public of a potential cyber spillover, a situation in which cyber conflicts seep into traditional arenas of militarized and foreign policy conflict[6], or impacts computer networks beyond the original target. Given Russia's propensity for hacking, national security officials believe Kremlin state agencies or other organizations sympathetic to their hostilities could deploy cyberattacks to advance Russian objectives. This may include attacks within or against the United States. To be clear, a sustained cyber offensive campaign has yet to emerge from the current Russia-Ukraine conflict. However, the White House has repeatedly warned that Russia's invasion, coupled with international sanctions, could lead the Kremlin to use cyberattacks against private sector organizations, including critical infrastructure owners and operators.[7] Like all states, Idaho would not be immune to the consequences of such an event.

Russia has a long history using cyberattacks against other countries. In 2015 and 2016, Russian hackers took down Ukraine's power grid for several hours leaving upwards of 250,000 residents in the dark.[8] In 2020, Russian hackers used a SolarWinds software update to maliciously infect thousands of computers operating at U.S. government agencies and Fortune 500 companies. And in 2021, a Russian ransomware group shutdown the 5,500-mile Colonial Pipeline causing delays in gasoline and other fuel deliveries to several states along the U.S. East Coast. In February 2022, reports emerged that Ukraine's embassy in Washington D.C. experienced the first U.S.-based cyberattack of the current conflict.[9] In retaliation, the hacking group Anonymous directed its 7.4 million followers to engage in cyber war against Russian President Vladamir Putin.[10] This seemingly endless series of malicious incidents brings into focus the challenging cybersecurity landscape we must confront, as it grows more dangerous and complex with each passing day.

COURTESY: INL

COURTESY: INL

## State of Idaho Preparation

Readers may wonder what all of this has to do with the State of Idaho. It is a fair point, especially because most residents have been minimally impacted by national and international cyber events to date. Despite years of dire warnings about a "cyber Pearl Harbor," electricity continues to flow to our homes and businesses, our online packages still arrive at our doorsteps, and remote work and education is not only possible, but thriving. So, is there really a concern?

The answer is yes. But the reasons are nuanced.

It is difficult to point to a single, seminal moment in which cybersecurity became a priority for the State of Idaho. But in 2015, following several disruptive cyberattacks on state agencies, then Governor CL "Butch" Otter created a task force to develop recommendations for protecting the state's computer systems. The task force was chaired by then Lt. Governor Brad Little and led Idaho to hire its first state director of information security.

Since then, the state has organized the Office of Information Technology Services around active cyber deterrence. Services have been streamlined, technology modernized, and efforts to recruit and retain a capable workforce are ongoing. Idaho has also invested in cybersecurity research through unique relationships with Idaho National Laboratory and the state's public research universities. In 2017, following legislative approval, the State Board of Education (SBOE) used its public bonding authority to construct two state-of-the-art computing and cybersecurity facilities in Idaho Falls on the campus of Idaho National Laboratory. In 2020, the legislature approved the state's request for nearly $1 million in one-time joint funding earmarked for cybersecurity curriculum development. Idaho's three public research universities all have active cybersecurity degree programs.

Even with an extensive effort to shore up cyber defenses throughout the state, rural counties, school districts, and small businesses across Idaho continue to face a barrage of cyberattacks ranging from identity theft to ransomware. With data breaches resulting in a national average loss of $4.2 million per incident[11], there is good reason to remain concerned and vigilant. In 2018, Madison County experienced a ransomware attack that locked employees out of their email and corrupted digital files. The county was able to

recover from the attack by relying on their information technology staff and backup files. A few months later, Bannock County experienced a data breach through its third-party utility payment system resulting in the loss of some resident's financial information. Several county residents later reported to police they had unauthorized funds taken from their bank accounts. And in 2021, Twin Falls County computers were infected with malware affecting department operations, phone lines, and delaying county court procedures. These incidents are but a few known examples that highlight the continuing problem of cyber intrusions on Idaho organizations.

Protecting today's information technology and operational technology networks is an immensely difficult task. Security vanguards are on watch 24/7 and must constantly act to safeguard and patch thousands of devices, ports, switches, routers, servers, and more. Some operational systems that run critical infrastructure are decades old and cannot easily be replaced or secured against advanced persistent threats. Our Idaho cybersecurity professionals must be tireless, even while the vulnerabilities are endless. And there never seems to be enough cyber talent to fill the hiring gap. At some point, the just-in-time patch and update system we rely on will break, and cyberattacks will not just be a minor inconvenience, but a full-fledged service disruption leading to undue harm and diminished faith and confidence in our Idaho institutions. In short, without preparation today, chaos could loom tomorrow.

COURTESY: UNIVERSITY OF IDAHO

## Key Themes

Over the last several months, the Governor's Cybersecurity Task Force has heard from local and national experts on cybersecurity issues around the country and in the Gem State. We have learned that in today's interconnected and interdependent internet environment, information sharing must be carefully balanced against spreading disinformation. Social identity and status updates must be balanced against concerns for identity theft. Remote access for work or play balanced against disruptions to our infrastructure. And the need to train and educate the next generation of students and workers balanced against a threat that is evolving faster than curriculum. These are the

realities of the modern cyberspace environment and a prelude to the topics confronting the state, even if we cannot see them just yet.

During the task force's work, three broad themes emerged from our discussions and interviews with local and national experts. These themes helped shape our recommendations and the path forward.

**Active Public Engagement**
In today's digital environment, cybersecurity is everyone's responsibility. That means an active and engaged public is necessary. Nearly every American consumer and business is connected to the global internet with billions of devices ranging from computers to smart phones, vehicles to vacuums. In fact, there are more internet-connected devices in the world than there are people on the planet.[12] That means the probability of attacks from bad cyber actors is enormous and growing. Since most devices are interconnected to other systems, a hack on one can compromise every other device connected to it. This is how malware spreads quickly.

This reality has led government and industry to coalesce around a new cybersecurity strategy known as zero trust. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership.[13] For the public, zero trust involves creating, maintaining, and updating complex passwords, required use of two-factor authentication, and frequent checks to verify one's identity and authorization to information. In short, it means access to online services will require additional time and effort. For zero trust to be effective, the public must be actively engaged in the security process and become knowledgeable — even at a basic level — about the benefits and responsibility of good cyber hygiene.

Zero trust is a proactive approach to securing vulnerable networks, but it is not a singular solution. Other cybersecurity philosophies advocate for secure-by-design architectures to protect both information technology and operational technology equipment. For example, cyber-informed engineering is a method that some Idaho organizations and educational institutions have a hand in developing. This method uses design decisions and engineering controls to eliminate or significantly mitigate cyberattacks throughout a product's design lifecycle.

**Adaptable Organizations**
Most cybersecurity professionals already employ a layered defense when protecting their networks from threats. This approach involves the use of multiple technologies, controls, policies, and mechanisms that overlap one another, making it difficult for cyber threats to go unnoticed.[14] But as attacks grow, evolve, and enter new domains (e.g. internet of things), the current trajectory of cyberattacks may outpace even the best defenses. Without quick action, Idaho citizens and organizations could be overwhelmed by the consequences of a major cyberattack in this continuously contested environment.

To give the state a fighting chance, all organizations and citizens — including government, industry, education, and households — should acknowledge and elevate cybersecurity to the top of their priority list. They should inventory and understand their connected critical resources and must-not-fail assets. They should capitalize on resources provided by private, state, and federal partners. Organizations should continue to converse and discuss cybersecurity topics through open lines of communication from executive

leadership to the front-line members. Workforce development and education is crucial to success. Therefore, organizations should be flexible, adaptable, and unconventional in their incentives and hiring practices.

**Communication and Coordination**

Emergency managers will tell you that communication and coordination during a crisis event is of utmost importance. Emergencies are fluid events with facts and details that change constantly. To move such an event from crisis to resolution, stakeholders must be regularly informed and consulted. Information must be vetted and shared with individuals including employees, customers, first responders, elected leaders, government officials, consultants, regulators, the press, and the public. Emergency events are almost always complex, messy, and take tremendous resources to resolve successfully. This is true whether the event is a physical disturbance like a natural disaster or a cyber event impacting access to information or services.

When Colonial Pipeline was hit with a ransomware attack in 2021, the company lost access to confidential data and some business operations. As a result, they proactively took operational systems offline, resulting in a suspension of gasoline delivery to fuel stations in several states including Florida, North Carolina, and New Jersey. After it became clear the cyber incident was a ransom-based attack from an international cyber-criminal hacking group, Colonial Pipeline worked to notify relevant stakeholders including employees, customers, law enforcement, and the federal government. They brought in an outside private contractor to support cyber recovery operations, alerted the White House, Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and National Security Agency (NSA), and they posted statements to their website. They also paid the hackers at least a $4.4 million ransom as this act was "in the best interest of the country."[15] Although this incident was resolved relatively quickly, primarily because of the ransom payment, it is a relevant case study in the need to proactively communicate and coordinate on cyber issues.

Ransomware is now a primary threat for businesses, utilities, and government organizations ranging from school districts to health departments, and individuals. Experts advise organizations large and small to be prepared by identifying and understanding the interconnections of digital assets. This includes investing in the use of cyber tools, training,

COURTESY: INL

and resources to prevent and detect breaches, and developing and practicing a response and recovery plan that ensures communication and coordination is fully understood and implemented. In today's connected environment, every organization should be prepared for a cyber breach, hack, or digital service disruption.

## About the Task Force

Idaho Governor Brad Little established the Governor's Cybersecurity Task Force in 2021. Its charter was to provide recommendations that improved business, government, and personal cybersecurity procedures, while identifying cybersecurity resources, and public-private partnerships across the state to increase awareness, education, and training. The task force also examined ways to ensure Idaho's elections remain secure, transparent, and resilient.

The task force held five official meetings and more than a dozen subcommittee meetings. Due to the COVID-19 pandemic, all but one meeting was held virtually. Co-led by the Idaho Department of Commerce and Idaho National Laboratory, the task force was composed of 19 members representing key Idaho institutions.

To take an in-depth look into cybersecurity in Idaho, additional experts served on four committees focused on critical infrastructure, workforce development and education, election security, and cyber literacy.

With the threat of a cyberattack against one of Idaho's critical infrastructures or key facilities a top concern, the critical infrastructure committee's mission was to provide recommendations on ways to ensure critical infrastructure across Idaho remains protected in the face of cyberattacks. These systems and assets, whether physical or virtual, are so vital to the United States that their incapacity or destruction could have a debilitating impact on security, economic stability, public health, and safety.

The workforce development committee's mission was to review, develop, and provide recommendations to increase workforce development and interest in cybersecurity, a growing and pervasive need within the state of Idaho. This task led to the examination of existing programs and partnerships within higher education, federal and state agencies, the public and private sectors, and Idaho's K-12 offerings.

The mission of the election security committee was to support, enhance, and highlight the existing election system in Idaho. While Idaho has proven that it currently administers elections very well, the ever-growing threat landscape demands that we continue to build on current and past successes.

The cyber literacy committee was tasked with providing recommendations to improve small business and individual cybersecurity awareness, understanding, and actions. Providing proper cyber literacy and education to businesses and the public gives individuals the toolbox of skills needed to use technology safely and effectively, reducing the likelihood of cyberattacks.

Several staff members also supported the task force. All task force members and staff served on a voluntary basis. A list of task force members, committees members, and meeting agendas can be found in the appendix of this report, or online at commerce.idaho.gov/cybersecurity/.

# Recommendations

COURTESY: INL

# Summary of Recommendations

Following extensive discussion and debate, the Governor's Cybersecurity Task Force developed 18 major recommendations. These recommendations are categorized into five strategic objectives as outlined below. Its important to note these recommendations cannot be accomplished without continued investment in cybersecurity in both public and private sectors.

## 1. Safeguard Idaho's Infrastructure and Provide Active Cyber Deterrence

Ensure safeguards are in place to protect critical infrastructure across Idaho in the face of potential cyberattacks.

## 2. Increase Investments for Cybersecurity Professionals in Workforce and Education

Increase investments in cybersecurity education to improve cybersecurity interest and workforce.

## 3. Ensure Election Integrity Through Cyber Enhancements

Support, enhance, and highlight the existing election system in Idaho and continue to build upon current and past successes.

## 4. Actively Engage the Public in Cybersecurity Awareness and Education

Improve individual and small business cybersecurity awareness, understanding, and actions by providing proper cyber literacy and education.

## 5. Continue to Address Cybersecurity in Idaho and Build Upon the Recommendations of Cybersecurity Task Force

Continue the task force's efforts to provide expert feedback and recommendations on the ever-evolving global cybersecurity landscape in Idaho.

COURTESY: INL

## Recommendations

**Recommendation 1: Safeguard Idaho's Infrastructure and Provide Active Cyber Deterrence**

*1.1 - Develop a Statewide Cybersecurity Strategy and Road Map*

The Governor's Cybersecurity Task Force recommends the Governor develop a statewide cybersecurity strategy and road map laying out a clear vision and set of actions to improve Idaho's cybersecurity posture. The strategy should address challenges and set broad, but achievable, goals for improved digital security now and into the future. The road map should build on the strategic plan and included detailed information to implement the state's vision in areas include election security, critical infrastructure protection, workforce development and education, healthcare and cyber literacy.

*1.2 - Establish an Idaho Cyber Fusion Center*

The task force recommends the Governor establish, and the state legislature fund, an Idaho Cyber Fusion Center. The center would act as a clearinghouse to communicate cyber threat information received from utilities, academic institutions, private companies, the federal government, and other appropriate sources. It would lead response efforts and provide warnings of potential cyberattacks, coordinate information sharing, assess risks to operational and information technology networks, prioritize cyber threats, and support public and private sector partners in protecting their vulnerable infrastructure.

*1.3 – Create a Cyber Response and Defense Fund*

The task force recommends the state create and invest in a Cyber Response and Defense Fund for the inevitable event that all organizations must plan for, the moment of a cyber security compromise. Funds would not be distributed until needed; however, this fund would prevent the need for deficiency warrants or supplement requests. While the Governor and its agencies are being diligent in minimizing exposure to cybersecurity threats, it is recognized that the state has many points of vulnerability. Those vulnerabilities and the increased threats across all sectors make it imperative that the state be prepared to respond.

*1.4 – Maintain and Enhance Inventory of the State's Critical Resources and Dependencies*

The task force recommends the state should continue to identify, map, and prioritize key resources, critical infrastructures, and interdependencies whose operations must function to ensure minimal disruptions to Idaho residents before, during, and after a cyberattack. This inventory should be regularly maintained and shared with appropriate individuals including emergency planners and first responders.


**Recommendation 2: Increase Investments for Cybersecurity Professionals in Workforce and Education**

*2.1 – Fund Additional Cybersecurity Faculty, Instructors, and Infrastructure at Idaho's Colleges and Universities*

The task force recommends the Idaho State Board of Education and higher education actively recruit and hire additional cybersecurity instructors and invest in infrastructure to meet the ever-growing demand of industry. As industry and academia come together to assess Idaho's cybersecurity offerings, funding must be available to hire additional faculty to instruct new courses. The ability of Idaho's colleges and universities to deliver a comprehensive cybersecurity curriculum is currently limited by a shortage of instructional faculty who specialize in cybersecurity and facilities to meet hands-on and immersive learning needs critical for student success and workforce needs.

*2.2 – Assess and Coordinate Cybersecurity Education Offerings to Ensure Consistency*

The task force recommends the Idaho State Board of Education create a comprehensive and well-defined outline of all cybersecurity offerings from Idaho's colleges and universities. Idaho should also leverage the capacity of the Idaho Regional Optical Network (IRON) to expand internet connectivity to schools across Idaho and improve the availability of cyber offerings and trainings.

This outline should identify how an individual can easily leverage courses from any Idaho college or university and how they can build upon these courses for continued education and a degree. Likewise, it should identify trainings offered through Idaho Career Technical Education, the Idaho Digital Learning Alliance, and other entities, to provide policy stakeholders with a comprehensive view of Idaho's cybersecurity training landscape. This makes it easier for individuals to select cybersecurity courses, increasing the number of cyber trained professionals. As a result of this assessment, a comprehensive cyber security workforce development plan is to be developed between academia, Idaho's Workforce Development Council, and other stakeholders. The creation of this cybersecurity training plan will better position the State of Idaho for federal or private sector grants. This thorough assessment will identify any gaps within Idaho's curricula and ensures Idaho's curricula remains cutting edge and relevant.

*2.3 – Increase Support for K-12 Computer Science and Math Literacy*
The task force recommends the State Department of Education and the State Board of Education explore and fund efforts to increase K-12 Computer Science and Mathematical literacy in Idaho. Idaho's partnerships with Code.org, Idaho's STEM Action Center, Idaho Business for Education, and the Idaho Digital Learning Alliance are pivotal to Idaho's cybersecurity workforce trajectory. These partners have resources, programming, and professional development content that helps Idaho's quest for increased literacy in math and computer science. Early exposure to computer science leads to increased interest in cybersecurity. Mathematical literacy is fundamental in cybersecurity.

Early exposure to computer science and stronger mathematical skills leads to the expansion of Idaho's cybersecurity talent pipeline.

*2.4 – Create a Forum to Discuss Cybersecurity Training and Workforce Development*
The task force recommends that the Idaho Cybersecurity Interdependencies Workshop (ICIW) annual conference include a forum for public-private discussions on cybersecurity training and workforce development needs.

The ICIW is an annual cybersecurity conference supported by the Idaho Office of Emergency Management (OEM) and the State of Idaho's Information Technology Services of Idaho (ITS). The ICIW conference provides a critical platform for developing communities of practice, sharing best practices and approaches, deepening the conversations around cybersecurity throughout the state, and providing direct or hands-on actions and artifacts that can be taken and deployed immediately. This recommendation builds upon and compliments ICIW's focus of cybersecurity. This recommendation leverages the ICIW forum, allowing both private-public feedback to Idaho's higher education on what is working in industry, what is needed, and what is evolving.

*2.5 Focused Recruitment of Veterans to Cybersecurity*
Given the state's support and commitment to Idaho's Air National Guard, the Mountain Home Air Force Base, and all military veterans, the task force recommends focused recruitment and training for Idaho veterans in cybersecurity. This recommendation allows public and private sector entities to leverage the partnerships and programs led by the Idaho Division of Veterans Services, Idaho Veterans Chamber of Commerce, nonprofit groups like Mission 43, who have demonstrated unified support in enacting the GI bill and other military funding (Department of Defense Skillbridge, Scholarship for Service, etc.). These support programs offset the cost of transitional training to Idaho veterans and prospective employers, allowing the critical "mission" to continue for many of Idaho's veterans.

*2.6 Designate a Cybersecurity Liaison Within the Presidents' Leadership Council*
The task force recommends the Presidents' Leadership Council (PLC) designate an education liaison to monitor, coordinate, and assist with Idaho's cybersecurity efforts across Idaho's post-secondary institutions. This designee would be tasked with coordinating approaches to providing cybersecurity courses across the state in a strategic manner and keeping the PLC abreast of these efforts. As more courses in cybersecurity are offered across Idaho's post-secondary institutions, a designee to the PLC will be critical to ensure a strategic approach to course offerings across the state.


**Recommendation 3: Ensure Election Integrity Through Cyber Enhancements**

*3.1 – Continued Support for Boise State University's INSURE Project*

The task force recommends the Governor continue support of the Idaho Election Cybersecurity Center (INSURE). Established in October 2020, the INSURE center, and its partners, undertake multiple research priorities essential to protecting the fair election process through the development of tools, technologies, and policies. The task force believes it is important to explore multiple avenues for additional funding including national and private sector grants.

*3.2 – Support Post-Election Audits to Maintain Election Integrity*

The task force recommends the Governor support the post-election audit efforts of the Secretary of State to validate and maintain Idaho's election integrity. Putting an audit framework into place will assist in maintaining voter confidence during primary and general elections. Because the election processes in Idaho vary minutely from county to county, a flexible audit procedure will be required, and the task force recommends supporting the post-election audit processes currently being proposed by the Secretary of State's office in consultation with leadership representatives of the Idaho Association of County Recorders and Clerks. Under this plan, the costs of the audit would be borne at the state level for these primary and general elections. It is critically important Idahoans have confidence in the election process and results, and this is a natural step to help ensure that confidence is established, and then sustained.

*3.3 – Support Early Processing of Absentee Ballots*

The task force recommends the state revisit the ability for county clerks to process absentee ballots prior to election day. During the record-setting 2020 general election, this process proved to be a safe, effective, and transparent way for clerks to process election results in a timely manner. It is no secret that timely election results engender confidence in the election process. This change is another positive step in supporting the current election system and helps ensure continued voter confidence in Idaho.

**Recommendation 4: Actively Engage the Public in Cybersecurity Awareness and Education**

*4.1 – Expand Development, Communication Strategy for State's Cybersecurity Website*

The task force recommends the Governor expands the development, content, and advertising of the state's cybersecurity information website — cybersecurity.idaho.gov. This site includes cybersecurity awareness and information for individuals, small businesses, and other vulnerable organizations like city and county municipal governments; however, site traffic and tool usage could be expanded with improved content and communication.

4.1a – The task force recommends a link to this website be placed prominently on all State of Idaho websites that individuals, organizations, and small businesses frequent for information, such as the Idaho Tax Commission, State Controller's Office, and Department of Motor Vehicles websites where Idaho citizens are required to enter sensitive information.

4.1b – The task force recommends the state produce and publish basic cybersecurity standards, guidelines, best practices, and available resources. Small businesses, school districts, and co-op utilities can use this information to inform their cybersecurity decision making process ensuring they receive a consistent and uniform level of security.

4.1c – The task force recommends that the state develop and publish a cybersecurity resource list that includes information about tools and services available to assist organizations seeking to improve their cybersecurity posture. For instance, the resource list should direct people to the federal government's ransomware response website (www.cisa.gov/stopransomware) which provides helpful information and resources for small businesses. This site could also point out programs that the state has invested in such as Idaho's own Institute for Pervasive Cybersecurity at Boise State University, and the Cyberdome Initiative. The Cyberdome is funded by a grant from the State Board of Education Higher Education Research Council (HERC) to develop regional training security operation centers across the state (at Idaho 2-year and 4-year institutions) and provide a scalable operation model that can help provide small cities and counties network security monitoring. Additional resources may also be available through federal partners including DHS, CISA, and the Idaho National Guard.

4.1d - CISA (www.cisa.gov) is the recommended site for all organizations, small businesses, and members of the public for guidance on cybersecurity matters. The Idaho Information Technology Services (www.its.idaho.gov) website is the recommended site for guidance on state cybersecurity matters.

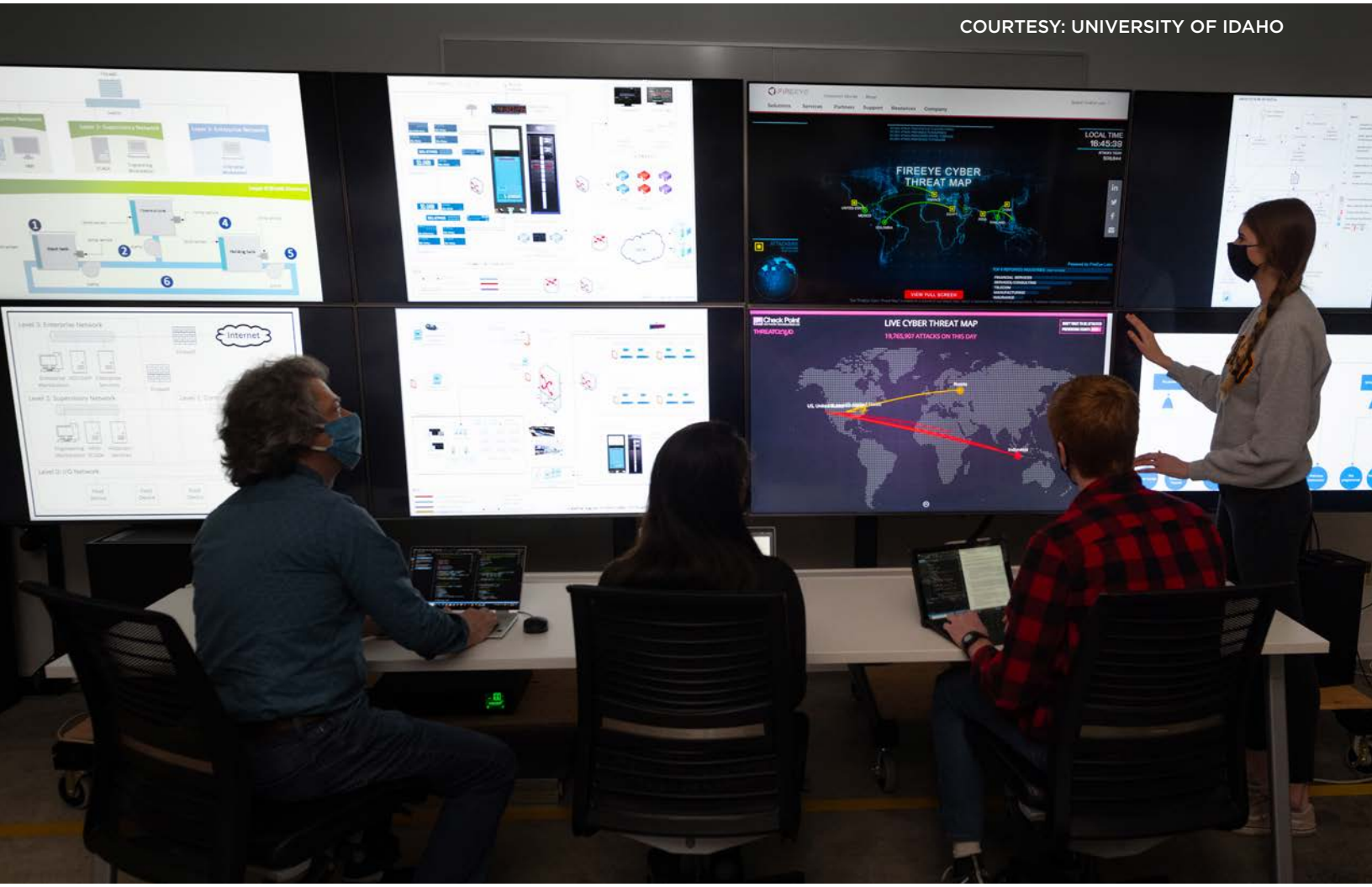
*4.2 – Launch a Series of Cyber Public Service Announcements*

The task force recommends the Governor pursue a cyber-themed public service announcement campaign to educate the public on issues including cyber prevention, detection, response, and recovery. The information in these campaigns should come from well-established and trusted organizations such as DHS, CISA, Idaho Information Technology Services, the Idaho Tax Commission, Idaho State Controller's Office, and more. Events like National Cybersecurity Awareness Month in October presents another opportunity to promote cybersecurity awareness and literacy through television or radio stations.

*4.3 – Build on the Success of and Further Develop Idaho Cybersecurity Summit*
The task force recommends the Governor continue to develop and sponsor the annual Idaho Cybersecurity Interdependencies Summit, while working to expand relevant content, topics, and speakers.

This annual cybersecurity conference is a critical platform for developing communities of practice, sharing best practices and approaches, deepening the conversations around cybersecurity throughout the state, and providing direct or hands-on actions and artifacts that can be taken and deployed immediately. It could also provide timely feedback to Idaho's higher education institutions on what is working in industry, what is needed, and what is evolving. The task force also recommends that the event organizers work with industry to underwrite and sponsor this event.

*4.4 – Continue Outreach and Information Sharing with Rural Counties*
The task force recommends the Governor continue providing cyber outreach and information sharing to rural county risk managers, emergency managers, and local elected officials. In the event of a major cybersecurity breach, service disruption, or ransomware attack of a critical business or infrastructure resource, rural counties should be aware of and understand the state and federal resources available to assist in response and recovery.



COURTESY: UNIVERSITY OF IDAHO

**Recommendation 5: Continue to Address Cybersecurity in Idaho and Build Upon the Recommendations of Cybersecurity Task Force**

*5.1 Continue to Address Future Cybersecurity Threats to Idaho*

The recommendations provided in this report are a start in the process of addressing cyber threats to the state of Idaho. However, cybersecurity is a complex and evolving global topic, and no single report or set of recommendations can cover the scale of the challenge or address all the opportunities.

Therefore, the task force recommends that the Governor's office continue this conversation and effort to address cybersecurity in Idaho through the continuation of the task force, an annual cybersecurity symposium, the creation of a new nonprofit organization, or the establishment of an advisory board. Just like the economy, information, and technology the state aims to protect, this discussion must be active, ongoing, and ever-evolving.


COURTESY: INL

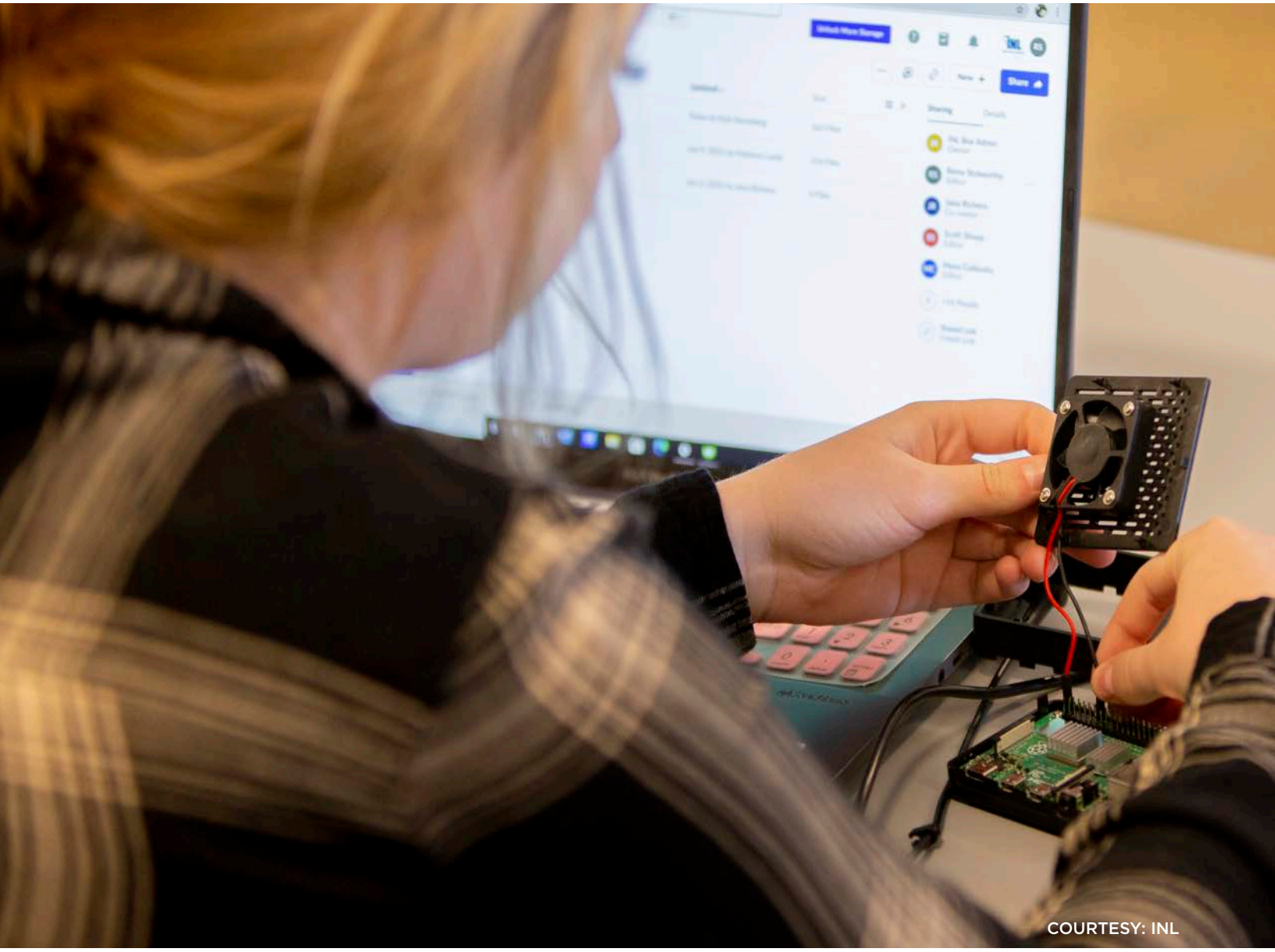
# Conclusion

The recommendations from the task force are a necessary step forward in protecting valuable Idaho resources from cyberattack while preparing the state for future threats and exigencies. Thanks to the task force members and all contributors to this process.

By focusing our efforts on active engagement, adaptability, and coordination, Idaho is stepping up to meet the global threat head-on. But it will take all of us to be successful.

From increasing resources for cybersecurity education and workforce training, to protecting our state's most vital infrastructure, partnerships will be critical. It will also be critical to continue the work of this task force and continue to make investments in cybersecurity in Idaho. Other states are already making significant investments in cybersecurity. Idaho must continue to do the same, or risk falling behind.

By working together, sharing information, communicating regularly, and remaining vigilant to the ever-evolving landscape, Idaho can help prevent, detect, respond, and recover from present and future cyber threats.



COURTESY: INL

# Appendix

# References


1. Montgomery, Mark. United States Cyberspace Solarium Commission, 12 Mar. 2020, https://www.solarium.gov/.

2. Temple-Raston, Dina. "A 'Worst Nightmare' Cyberattack: The Untold Story of the Solarwinds Hack." NPR, NPR, 16 Apr. 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

3. Greenberg, Andy. "A Hacker Tried to Poison a Florida City's Water Supply." Wired, Conde Nast, 8 Feb. 2021, https://www.wired.com/story/oldsmar-florida-water-utility-hack/.

4. Greenberg, Andy. "The Colonial Pipeline Hack Is a New Extreme for Ransomware." Wired, Conde Nast, 8 May 2021, https://www.wired.com/story/colonial-pipeline-ransomware-attack/.

5. Batista, Fabiana, et al. "All of JBS's U.S. Beef Plants Were Forced Shut by Cyberattack." Bloomberg.com, Bloomberg, 31 May 2021, https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs.

6. Maness, Ryan C, and Brandon Valeriano. "Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?" Conflict in Cyber Space Theoretical, Strategic and Legal Perspectives, edited by Karsten Friis and Jens Ringsmose, 1st Edition ed., Routledge, Taylor, Francis Group, London, NA, 2017, pp. 45–64.

7. The White House. "Statement by President Biden on Our Nation's Cybersecurity." The White House Briefing Room, The United States Government, 21 Mar. 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.

8. Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, Conde Nast, 3 Mar. 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

9 Sabin, Sam. "U.S. Cyber Officials Brace for Attacks in Wake of Ukraine Invasion." POLITICO, 28 Feb. 2022, https://www.politico.com/newsletters/weekly-cybersecurity/2022/02/28/u-s-cyber-officials-brace-for-attacks-in-wake-of-ukraine-invasion-00012203.

10. Milmo, Dan. "Anonymous: The Hacker Collective That Has Declared Cyberwar on Russia." The Guardian, Guardian News and Media, 27 Feb. 2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

11. Osborne, Charlie. "Enterprise Data Breach Cost Reached Record High during COVID-19 Pandemic." ZDNet, ZDNet, 28 July 2021, https://www.zdnet.com/article/enterprise-data-breach-cost-reached-record-high-during-covid-19-pandemic/.

# References

12. Lee, Ahyoung & Wang, Xuan & Nguyen, H. & Ra, Ilkyeun. (2018). A Hybrid Software Defined Networking Architecture for Next-Generation IoTs. KSII Transactions on Internet and Information Systems. 12. 932-945. 10.3837/tiis.2018.02.024.

13. NIST SP 800-207: Zero Trust Architecture. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

14. Pearlson, Keri, and Nelson Novaes Neto. "7 Pressing Cybersecurity Questions Boards Need to Ask." Harvard Business Review, Harvard Business Publishing, 7 Mar. 2022, https://hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask.

15. Morse, Andrew. "Colonial Pipeline CEO Tells Senate Decision to Pay Hackers Was Made Quickly." CNET, CNET, 8 June 2021, https://www.cnet.com/news/privacy/colonial-pipeline-ceo-tells-senate-decision-to-pay-hackers-was-made-quickly/.

# Cybersecurity Resources

- Cybersecurity and Infrastructure Security Agency (CISA) - https://www.cisa.gov/
- Cybersecurity Manufacturing Innovation Institute (CyManII) - https://cymanii.org/
- Federal Bureau of Investigation (FBI) - https://www.fbi.gov/
- Idaho State Board of Education (SBOE) - https://boardofed.idaho.gov/
- National Security Agency (NSA) - https://www.nsa.gov/
- State of Idaho Cybersecurity - https://cybersecurity.idaho.gov/
- State of Idaho Information Technology Services (ITS) - https://its.idaho.gov/
- State of Idaho Office of Emergency Management (OEM) - https://ioem.idaho.gov/
- United States Department of Homeland Security (DHS) - https://www.dhs.gov/

**Idaho University Cybersecurity Programs**

- Boise State University (BSU) - https://www.boisestate.edu/cybersecurity/programs/
- College of Eastern Idaho (CEI) - https://www.cei.edu/programs-of-study/technology/cybersecurity-center
- College of Southern Idaho - https://www.csi.edu/information-technology/community/cybersecurity/default.aspx
- College of Western Idaho (CWI) - https://cwi.edu/program/cybersecurity
- Idaho State University (ISU) - https://www.isu.edu/industrialcybersecurity/
- Lewis and Clark State College (LCSC) - https://www.lcsc.edu/program-finder/cybersecurity
- North Idaho College (NIC) - https://www.nic.edu/cybersecurity/
- University of Idaho Cybersecurity (U of I) - https://www.uidaho.edu/engr/programs/cybersecurity

# Task Force Members

Tom Kealey, Director, Idaho Department of Commerce

Zach Tudor, Associate Laboratory Director, Idaho National Laboratory

General Brad Richy, Director, Office of Emergency Management

Jeff Weak, Administrator, Office of Information Technology Services

Lisa Grow, President & CEO, IDACORP and Idaho Power

George Mulhern, CEO, Cradlepoint

Jeff Newgard, President & CEO, Bank of Idaho

Ryan White, Chief of Staff, Senator Jim Risch

Anand Bahl, Chief Information Officer, Micron Technology

Domini Clark, CEO, Blackmere Consulting

# Task Force Members

**Edward Vasko, Director Pervasive Cybersecurity, BSU**

**Dr. Scott Snyder, Dean, College of Science and Engineering, ISU**

**Dr. Christopher Nomura, Vice President for Research and Economic Development, U of I**

**Ben Ysursa, Former Idaho Secretary of State**

**Brad Wiskirchen, VP and General Manager, Kount-Equifax**

**Frank Harrill, VP of Security, Schweitzer Engineering Laboratories**

**Rep. Brooke Green**

**Rep. Dustin Manwaring**

**Sen. Jim Woodward**

# Committees

## Election Security

- Ben Ysursa, Chair, Former Secretary of State
- Ryan White, Office of Senator Jim Risch
- George Mulhern, Cradlepoint
- Dr. Hoda Mehrpouyan, BSU
- Dr. Amit Jain, BSU
- Sharee Sprague, Power County
- Jason Maughan, INL
- Chad Houck, Secretary of State

## Critical Infrastructure

- Frank Harrill, Chair, Schweitzer Engineering Laboratories
- General Brad Richy, Office of Emergency Management
- Lisa Grow, Idaho Power
- Representative Brooke Green
- Ed Vasko, BSU
- Will Hart, Idaho Consumer Owned Utilities Association (ICUA)
- Will Goodman, Boise School District
- Tom Schultz, Idaho Forest Group
- Kelly Wilson, INL

## Cyber Literacy

- Jeff Newgard, Chair, Bank of Idaho
- Jeff Weak, Information Technology Services
- Dr. Christopher Nomura, U of I
- Senator Jim Woodward
- Dick Fosbury, Blaine County
- Ron Pisaneschi, Idaho Public Television (IPTV)
- Britt Raybould, Raybould Farms
- John Keenan, INL

## Workforce Development

- Domini Clark, Chair, Blackmere Consulting
- Anand Bahl, Micron Technology
- Dr. Scott Snyder, ISU
- Brad Wiskirchen, Kount
- Representative Dustin Manwaring
- Dr. Rick Aman, CEI
- Eleanor Taylor, INL
- John Young, Workforce Development Council

# Staff Contributors

Idaho National Laboratory: Ethan Huffman, Elli Brown, John Revier

Idaho Commerce: Matt Borud, Carmen Achabal, Cody Allred

# Cybersecurity Task Force Meeting

Thursday, August 19, 2021
1:00 p.m. to 5:00 p.m. MT
The Riverside Hotel – Cinnabar Conference Room
2900 W. Chinden Blvd. Garden City, ID 83714

Meeting ID: 851 5003 3922
Click here to join the meeting remotely.
**Members may also be attending via conference call.*

| Time | Topic | Lead | Notes |
|---|---|---|---|
| 1:00 p.m. | Call to Order and Welcome | Tom Kealey | |
| 1:15 p.m. | Overview of Mission and Deliverables | Zach Tudor & Tom Kealey | |
| 1:30 p.m. | Introduction of Task Force Members and Support Team | Zach Tudor | |
| 2:30 p.m. | Setting the Stage – State and National Challenges | Zach Tudor & Tom Kealey | |
| 3:00 p.m. | Break | Tom Kealey | |
| 3:15 p.m. | Why Idaho – Assets and Opportunities Panel Discussion<br>• Zach Tudor, INL, Associate Lab Director<br>• Ryan White, Senator Jim Risch's Office, Chief of Staff<br>• Scott Cramer, Cybercore Integration Center, Director<br>• General Brad Richy, IOEM, Director<br>• Brad Wiskirchen, Idaho Cyber Alliance, Founder | Zach Tudor | |
| 4:15 p.m. | Next Steps – Subcommittees and Meetings | Tom Kealey | |
| 4:55 p.m. | Public Comments | Zach Tudor | |
| 5:00 p.m. | Adjournment | Tom Kealey | Action Item |

700 W State Street, Boise, Idaho 83702 — 208.334.2470 or 800.842.5858 — commerce.idaho.gov

**CYBERSECURITY TASK FORCE MEETING**
Thursday, September 30, 2021
9:00 a.m. – 2:00 p.m. MT

*The public meeting will be located at 700 W. State St. Boise, ID 83702, second floor, Clearwater conference room. Seating is limited. The public is encouraged to participate online.*

Click the link below to join this meeting remotely.
https://us02web.zoom.us/s/88217307865?pwd=YzhodWY4TTkwZnRMVVRCWklYdW5RUT09

| Time | Topic | Lead | Notes |
|---|---|---|---|
| 9:00 a.m. | Call to Order, Welcome and Updates<br>Subcommittee Introductions | Tom Kealey | Action Item |
| 9:30 a.m. | Elections in Idaho<br>Presenter: Ben Ysursa, Former Idaho Secretary of State | Zach Tudor | |
| 9:45 a.m. | Idaho Election Cybersecurity Center<br>Presenter: Dr. Hoda Mehrpouyan, Boise State University | Tom Kealey | |
| 10:15 a.m. | National Perspective on Election Security<br>Presenter: Bob Kolasky, Director National Risk Management Center | Zach Tudor | |
| 10:45 a.m. | Break | | |
| 11:00 a.m. | State and National Perspective on Election Security Panel Discussion<br>Moderator: Zach Tudor, INL, Associate Lab Director<br>Jeremy Epstein, National Science Foundation<br>Chad Houck, Idaho Secretary of State Office<br>Sharee Sprauge, Power County | Zach Tudor | |
| 12:00 p.m. | Task Force Reflections and Input | Tom Kealey | |
| 12:30 p.m. | Break | | |
| 1:00 p.m. | Subcommittee Reports<br>Election Security: Ben Ysursa<br>Workforce Development: Domini Clark | Zach Tudor | |

**CYBERSECURITY TASK FORCE MEETING**
Wednesday, November 10th
8:00 a.m. MT – 4:00 p.m. MT

*The public meeting will be located at 700 W. State St. Boise, ID 83702. Seating is extremely limited. The public is encouraged to participate online.*

Click the link below to join the meeting remotely:
https://us02web.zoom.us/j/81755325544?pwd=QlVEcXlqUW9JREk0Z1pBOHZUK3phdz09

| Time | Topic | Lead |
|---|---|---|
| 8:00 am | Call to Order, Welcome and Updates | Zach Tudor |
| 8:10 am | National Priorities and Perspectives on Cybersecurity<br>Presenter: Rob Lee; Dragos, Inc | Tom Kealey |
| 8:45 am | Critical Infrastructure Overview and Subcommittee Update<br>Presenter: Frank Harrill | Tom Kealey |
| 9:15 am | DOE Cyber Testing for Resilient Control Systems (CyTRICS)<br>presenter: Ginger Wright | Zach Tudor |
| 9:45 am | DHS Regional Resiliency Assessment Program Briefing<br>Presenter: Kelly Wilson | Zach Tudor |
| 10:15 am | State and National Perspective on Critical Infrastructure Panel Discussion<br>Moderator: Frank Harrill<br>Brad Richy, Office of Emergency Management<br>Paul Shaver, Mandiant<br>Tobias Whitney, Fortress Information Security<br>Sgt. Bret Kessinger, Idaho State Police<br>Kevin Reifsteck, Microsoft | Zach Tudor |
| 11:15 am | Task Force Reflections and Input | Tom Kealey |
| 11:45 am | Break | |
| 12:15 pm | Cyber Literacy Overview and Subcommittee Update<br>Presenter: Jeff Newgard | Tom Kealey |
| 12:30 pm | US Secret Service Cybersecurity Briefing<br>Presenter: Paul Hagedorn, Sr. Special Agent | Tom Kealey |
| 1:15 pm | Educating and Empowering Cybersecurity<br>Presenter: Lisa Plaggemier, National Cybersecurity Alliance | Tom Kealey |
| 2:00 pm | Perspectives on Cyber Literacy for Small Businesses<br>Moderator: Jeff Newgard<br>Daniel DeCloss, PlexTrac<br>James Perry, Amazon Web Services<br>Evan Francen, Security Studio | Tom Kealey |
| 2:45 pm | Task Force Reflections and Input | Tom Kealey |
| 3:15 pm | Subcommittee Updates:<br>Election Security, Ben Ysursa<br>Workforce Development, Domini Clark | Zach Tudor |
| 3:45 pm | Public Comments | Tom Kealey |
| 4:00 pm | Action Items and Adjournment<br>Future meeting dates:<br>December 15th – Location TBD<br>February 9th – Boise | Zach Tudor |

**CYBERSECURITY TASK FORCE MEETING**

Wednesday, December 15th

9:00 a.m. MT – 4:35 p.m. MT

*The public meeting will be located at 700 W. State St. Boise, ID 83702. Seating is extremely limited. The public is encouraged to participate online.*

Join the meeting remotely using the link below:

https://us02web.zoom.us/s/85656444646

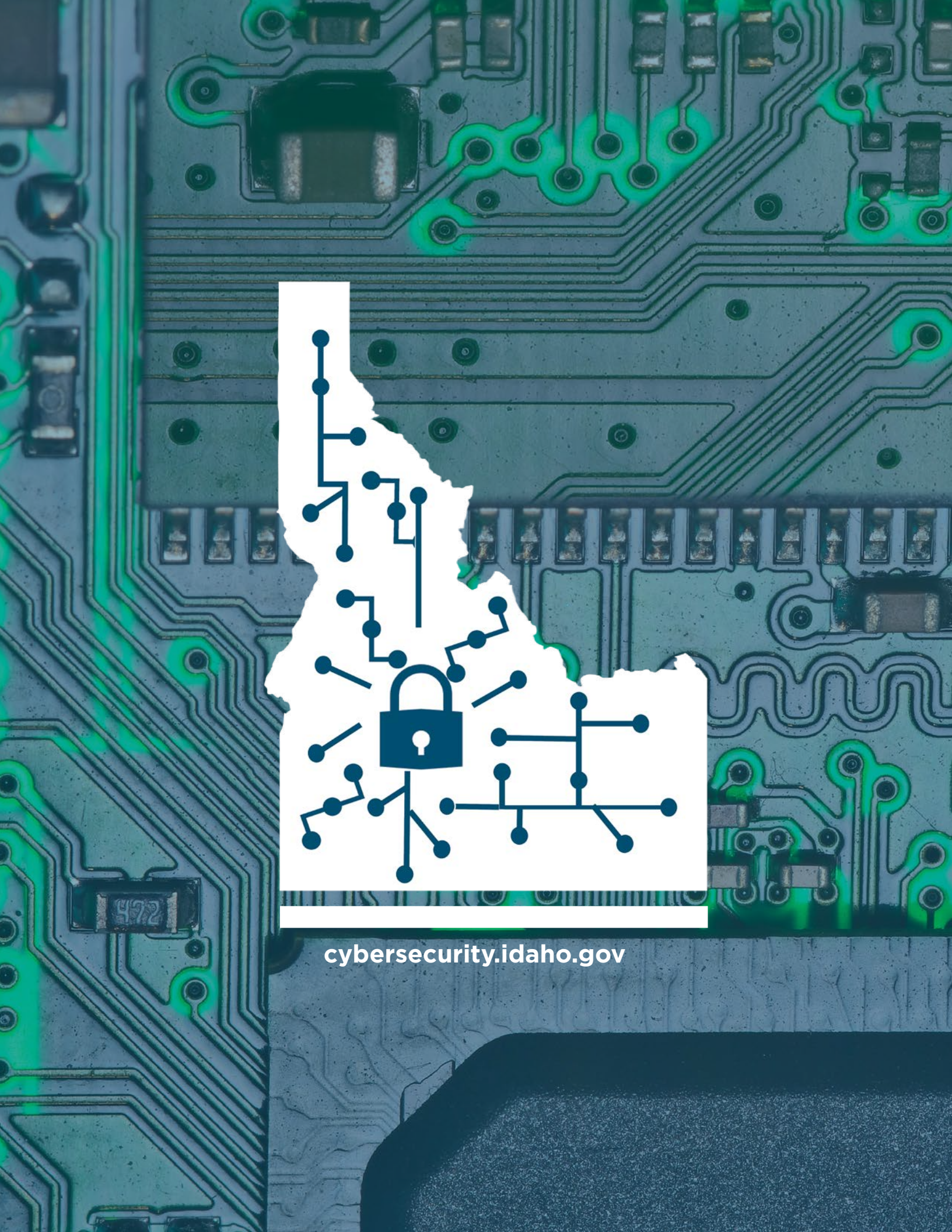
| Time | Topic | Lead |
|---|---|---|
| 9:00 a.m. | Call to Order and Welcome | Tom Kealey |
| 9:10 a.m. | National Perspectives and Initiatives on Cybersecurity Workforce Development<br>Presenter: Nitin Natarajan, Deputy Director<br>Cybersecurity & Infrastructure Security Agency (CISA) | Zach Tudor |
| 10:00 a.m. | Sparking Cyber Interest in America's Future<br>Presenter: Pat Yongpradit, Chief Academic Officer<br>CODE.org | Tom Kealey |
| 10:30 a.m. | Break | |
| 10:45 a.m. | Task Force Reflections and Input | Zach Tudor |
| 11:00 a.m. | Workforce Development Subcommittee Update | Domini Clark |
| 11:15 a.m. | Idaho K-12 Efforts in Increasing Cybersecurity Interest<br>Moderator: Wendi Secrist, Idaho Workforce Development Council<br>Kaitlin Maguire, Ph.D., Idaho STEM Action Center<br>Jennifer Jackson, Idaho National Laboratory<br>Ryan Gravette, Idaho Digital Learning Alliance<br>Roger Plothow, Idaho Business for Education | Tom Kealey |
| 12:15 p.m. | Lunch Break | |
| 1:00 p.m. | Cybersecurity and Workforce Transformation<br>Presenter: Diana Burley, Ph.D., Vice Provost for Research<br>American University | Zach Tudor |
| 1:30 p.m. | Synergizing Idaho's Higher Education Cyber Initiatives<br>Moderator: Domini Clark, Blackmere Consulting<br>Dr. Michael Haney, University of Idaho<br>Dr. Terry Soule, University of Idaho<br>Ed Vasko, Boise State University<br>Dr. Rick Aman, College of Eastern Idaho | Tom Kealey |
| 2:45 p.m. | Break | |
| 3:00 p.m. | Apprenticeships: Transitioning Veterans to Cyber Heroes<br>Moderator: Dr. Scott Snyder, Idaho State University<br>Mark Tschampl, Idaho Division of Veteran Services<br>Dr. Mindi Anderson, Idaho Veterans Chamber of Commerce<br>Alison Garrow, Mission 43<br>Ephraim Peterson, Veteran - DOD SkillBridge Program | Zach Tudor |
| 4:00 p.m. | Task Force Reflections and Input | Tom Kealey |
| 4:15 p.m. | Short-Term Recommendations<br>February 9th Meeting Expectations and Preparation | Zach Tudor and Tom Kealey |
| 4:30 p.m. | Public Comments | Zach Tudor |
| 4:35 p.m. | Action Items and Adjournment | Tom Kealey |

**CYBERSECURITY TASK FORCE MEETING**
Wednesday, February 9th
1:00 p.m. MT – 5:00 p.m. MT

*The public meeting will be located at 700 W. State St. Boise, ID 83702. Seating is extremely limited. The public is encouraged to participate online.*

Click the link below to join the meeting remotely:
https://us02web.zoom.us/s/88217307865?pwd=YzhodWY4TTkwZnRMVVRCWklYdW5RUT09

| Time | Topic | Lead | Notes |
|---|---|---|---|
| 1:00 p.m. | Call to Order, Welcome and Updates | Tom Kealey | Action Item |
| 1:15 p.m.<br><br>4:45 p.m. | Review Draft Recommendations and Report<br>Facilitator: Darcie Martinson<br><br>Public Comment Period | Zach Tudor<br><br>Tom Kealey | |
| 4:50 p.m. | Path Forward – Review Schedule | Tom Kealey | |
| 5:00 p.m. | Action Items and Adjournment | Zach Tudor | |



cybersecurity.idaho.gov