HP Inc.
1070 NE Circle Blvd
Corvallis, Oregon 97330-4239

hp.com

February 17, 2022

To: Joint Committee on Information Management and Technology
          Sen Rachel Armitage and Rep Nancy Nathanson, Co-Chairs

From: Boris Balacheff, Chief Technologist for System Security Research and Innovation,
          Paul Benning, Chief Technologist, Strategy & Incubation
          HP Inc.

Re: Testimony in support of HB4155

Greetings,

Members of the Joint Committee on Information Management and Technology, thank you
for the opportunity to submit written testimony in support of HB 4155 on behalf of HP
Inc. HP is a multinational information technology company headquartered in Palo Alto
that develops personal systems printers and printing solutions, as well as 3D printing
solutions. We have had a substantial presence in Corvallis Oregon since 1977, with a
major research, development, and manufacturing site; and we actively sponsor
cybersecurity education in the state, through initiatives like the new Oregon Research and
Teaching Security Operations Center (ORTSOC) at OSU.

AN EVOLVING THREAT LANDSCAPE AND SHORTAGE OF SKILLED WORKERS
With the advancement of digital technologies there has been a proportional development
in their misuse. Daily, organizations face phishing, ransomware, malware, and other
forms of cyberattacks. Oregon has to face these challenges. To take but a few examples
from the last few months, a ransomware attack on a medical group[1] resulted in a breach
of data on 750,000 patients and 522 current and former employees. An Oregon business

---

[1] https://www.zdnet.com/article/oregon-medical-group-notifies-patients-of-cybersecurity-
breach-says-fbi-seized-hellokitty-accounts/

which operates tens of hotels, movie theaters, bars and restaurants in the Northwest was targeted by a ransomware attack which took down its online reservation system[2].
In this context, due to the pandemic, hundreds of millions of employees around the world were forced to work from home. Working from home became the only way organizations could continue to function and IT and security teams needed to adapt to manage and secure fleets of computers spread out over geographies without the visibility of devices, how they are being used, and by whom. These vulnerabilities were exploited by attackers resulting in a 238% increase in global cyberattack[3] volume during the early days if the pandemic. Many organizations will need to adapt to a new hybrid world of IT, where distributed teams are more common, and agility to support remote work is necessary. In this new environment the increased rate of cyber-attacks coupled with the behaviors resulting from remote working compound the cyber risks that governments, companies, and individuals are exposed to. Cyber-attacks will continue unabated, and our best path forward is to build for cyber resilience.

Beyond technology itself, a key component to achieve cyber resilience will be access to a large enough pool of skilled cybersecurity professionals. However, the number of cybersecurity related jobs already outpaces the number of people with the skillset to fill them, and the demand for a skilled cybersecurity workforce continues to grow. According to the ISC², a non-profit specializing in training and certifications for cybersecurity professionals, in 2021 the cybersecurity workforce gap was 2.72 million worldwide, and 377 thousand in the United States alone[4]. This means that the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets. Cybersecurity threats will not be effectively managed if there is not significant investment in growing a skilled workforce.

CYBER EDUCATION THROUGH ORTSOC
HB 4155 would help to address the cybersecurity workforce gap. Programs supported by this Bill, such as the Oregon Cybersecurity Center of Excellence would help oversee, coordinate, and fund cybersecurity education, awareness, and training for public, private, and nonprofit sectors, as well as cybersecurity workforce development which will all contribute towards closing the critical cybersecurity skills gap.
HP is already invested in this mission worldwide, and in Oregon specifically, where we expanded our long-established partnership with Oregon State University (OSU) to sponsoring the new Oregon Research and Teaching Security Operations Center (ORTSOC). ORTSOC aims to address the shortage of trained cybersecurity professionals while serving the security needs of underserved entities — such as small local government agencies, K-12 schools, smaller higher education institutions, and nonprofit organizations — who

---

2 https://www.oregonlive.com/business/2021/12/mcmenamins-hit-by-ransomware-attack-chain-says-customer-data-appears-secure-but-employee-info-at-risk.html
[3] https://press.hp.com/content/dam/sites/garage-press/press/press-releases/2021/wolf-security-and-flexworker/2021_HP_Wolf_Security_Blurred_Lines_Report.pdf
4 https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

struggle to meet their cybersecurity needs. Studies have shown that to best prepare students for careers in cybersecurity, experiential learning is the key. HP believes ORTSOC is critical to be able to accelerate cyber training to create and train a workforce for business and public organizations. It can have tremendous positive impact on cybersecurity research and education at Oregon State, while addressing the security workforce and skills shortage in the region.

HP has long been invested in technology and education in Oregon. Another example in the field of cybersecurity is our sponsorship and participation in Oregon's NW Cyber Camp[5] – a K-12 camp exposing students to careers in cybersecurity. We believe that this program focused on growing Oregon's cybersecurity workforce greatly deserves the financial support necessary to continue to grow, attract, and support a larger number of students across the state.

We believe in investing in the next generation of skilled cybersecurity workers. HP's investment in Oregon's cybersecurity training efforts to date, as well as our support of the objectives of HB 4155 are testament to our commitment to bridging the cybersecurity gap. The funding objectives of HB4155 will amplify the impactful activities that are already underway in Oregon and help to maximize our chances of successfully addressing the challenge we all face to build a cyber resilient future.

Thank you for the opportunity to submit testimony.

Best,

Boris Balacheff
HP Fellow
Chief Technologist for System Security Research and Innovation, HP Inc.
Advisory Board Member, ORTSOC, OSU

Paul Benning
HP Senior Fellow
Chief Technologist Strategy & Incubation, HP Inc
Oregon Venture Fund Advisor

---

[5] https://www.nwcyber.camp/