A Call to Action to Maximize Cyber Defenses by Better Aligning Cybersecurity Regulations

Dear G7 and OECD Member States,

As a community of Chief Information Security Officers (CISOs), we write to express our support for your efforts to strengthen cybersecurity and resilience and counter cyber threat actors. We encourage you to prioritize greater alignment of cybersecurity regulations to maximize the effective use of limited resources.

We recognize that in response to growing cyber threats, there has been a proliferation of new cybersecurity laws and regulations. Some governments, like the United States, have gone beyond voluntary partnerships and started using regulatory authorities. Others, like Australia, the European Union, and Singapore are updating existing regulations and have created new ones. The UK government recently announced its plans to pass a new cybersecurity law. Other governments may take similar regulatory actions in the coming years.

At the same time, there has been a growing divergence among these domestic regulatory efforts across countries and across sectors. This growing fragmentation is adding complexity to our companies' operational cyber defense and ability to defend against growing cyber threats. It creates difficulty in implementing consistent security measures across different jurisdictions, complexity to time-sensitive incident response activities, potential negative impact on reporting due to conflicting requirements, delays in cybersecurity regulatory implementation due to the need of managing multiple regulatory landscapes and exacerbates the cybersecurity talent shortage.

We understand the need for regulation and its role to help strengthen cybersecurity and resilience. To maximize the regulations' intent and operational cyber defenses, we urge you to make greater alignment and reciprocity of cybersecurity regulations a political priority in the coming months.

Specifically, we encourage you to:

- **Issue a joint senior political commitment to focus on greater alignment of cybersecurity regulations in relevant multilateral forums, namely at the G7 and upcoming OECD meetings,** ideally (i) specifying a focus on aligning the implementation of existing regulations consistently, (ii) committing to greater collaboration for future regulations, (iii) the need to balance the timing for implementation versus new regulations, (iv) enabling faster, secure exchange of threat intelligence and (v) a commitment to engage with the private sector for consultations.
- **Agree that you will leverage the OECD's expertise and ability to serve as a key forum to implement this political commitment and to convene regulators across countries**

and sectors on a regular basis, including in a multistakeholder format with private sector participation. The OECD will ideally convene relevant stakeholders, including industry and other nongovernmental representatives, once or twice a year, developing an action plan to implement the senior political commitment across countries and sectors, with regular progress updates to senior decision-makers and regulatory authorities.

International mechanisms for governments to cooperate and coordinate on cybersecurity regulation remain nascent. This gap complicates our ability to implement cohesive cybersecurity practices and diverts important resources. The OECD can help fill this gap and serve as a key forum and provide clarity to address this growing problem.

Potential solutions for greater international cybersecurity regulatory alignment include reciprocity agreements, adopting international standards, and maximizing the cross-regulatory applicability of third-party assessments and audits. This approach would result in a cohesive and harmonized regulatory environment that would facilitate better cooperation and information sharing among nations, enhance our collective defense against cyber threats while helping drive business forward, making us more efficient.

Malicious cyber threat actors continue to target our companies, governments, and societies, often with impunity. We are keen to engage with governments to identify more effective ways to deter cyber attacks and impose appropriate consequences. In the meantime, we will invest in strengthening our cyber resilience. The interconnected nature of the cyber landscape necessitates collaboration across borders, and we look forward to continuing to do our part.

Respectfully,

- Adrian M. Mayers, CISO, Premera Blue Cross
- Alexis Wales, CISO, GitHub
- Andrea Smith Abell, Senior Vice President and CISO, Eli Lilly
- Arno van der Walt, CISO, Marriott International
- Brad Arkin, Chief Trust Officer, Salesforce
- Bret Arsenault, Corporate Vice President, Global Chief Security Advisory, Microsoft
- Chris Betz, CISO, Amazon Web Services
- Chris Ulliott, CISO, Natwest Group
- Christopher Chew, Member, ISC2 & OWASP
- Dr. Carl Windsor, CISO, Fortinet
- Espen Jul Larsen, Director Group Security, CSO, Gjensidige
- Frank Fischer, Group CISO, DHL Group
- Fook Hwa Tan, Chief Quality Officer, Northwave
- Gene Yoo, CEO / CISO, Resecurity, Inc.

- Hans Lindberg, CEO, Swedish Bankers' Association
- James Bouchard, CISO, Enbridge
- John Dickson, CISO, Colonial Pipeline Company
- JR Williamson, Senior Vice President and CISO, Leidos
- Lance McGrath, Chief Security Officer, Danske Bank
- Lea Kissner, CISO, LinkedIn
- Madinah Ali, President/CEO, SafePC Solutions
- Malin Hammenhög, CISO, Sparbanken Syd
- Marcel Zumbühl, Group CISO, Swiss Post
- Marco Wyrsch, Chief Security Officer, Swisscom
- Mario Ferket, CISO, Dow Inc
- Matej Zachar, CIO & CISO, Kontent.ai
- Matthew Chase Carpenter, Chief Security Officer, Honeywell
- Max Eugen Boedder, Senior Director, Cybersecurity and Technical Services, The Mosaic Company
- Michael Lashlee, Chief Security Officer, Mastercard
- Natalia Oropeza Gutierrez, Global CISO and Chief Diversity Officer, Siemens and Chairwoman for the Charter of Trust
- Peter Gripner, CISO, Resurs Bank AB
- Robert Huber, Chief Security Officer, Tenable
- Sebastian Lange, Chief Security Officer, SAP SE
- Scott Brown, CISO, Rio Tinto
- Stephane Lenco, Vice President, CISO, Thales Group
- Sumit Chanda, CISO, Eviden
- Sydney Klein, SVP, CISO & Head of IT CORE Services, Bristol Myers Squibb
- Vaughn Hazen, CISO, Canadian National Railroad
- Vikram Rao, Chief Trust Officer, Atlassian
- Volker Wagner, CISO, BASF SE
- Christoph Peylo, Chief Cyber Security Officer, Robert Bosch GmbH
- Sandro Bucchianeri, Group Chief Security Officer, National Australia Bank
- Sara Hall, CISO, Teladoc Health