



วันที่ 12 ตุลาคม 2561

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
120 หมู่ที่ 3 ชั้น 6-9 ศูนย์ราชการเฉลิมพระเกียรติ
ถนนแจ้งวัฒนะ พุ่งสองห้อง
หลักสี่ กรุงเทพมหานคร 10210

เรื่อง ความเห็นเกี่ยวกับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ....

เรียนท่านปลัดกระทรวง

ความนำและคำชี้แจงเรื่องส่วนได้เสียในร่างพระราชบัญญัติ

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (“บีเอสเอ”)¹ ขอขอบคุณกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
สำหรับโอกาสให้มีการเสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.... (“ร่าง พ.ร.บ.”) ที่ได้ลงประกาศในเว็บไซต์ www.lawamendment.go.th เมื่อวันที่ 27
กันยายน 2018

¹ บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอเป็นบริษัทต่างๆ ที่สร้างสรรค์นวัตกรรมที่ทันสมัยที่สุดของโลก ซึ่งนำเสนอโซลูชันซอฟต์แวร์ที่ผลักดันให้เศรษฐกิจเติบโตและปรับปรุงคุณภาพชีวิตในยุคปัจจุบัน บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดี.ซี. และมีการดำเนินการในกว่า 60 ประเทศทั่วโลก โดยเป็นผู้ริเริ่มโครงการส่งเสริมการปฏิบัติตามกฎหมายเพื่อรองรับการใช้ซอฟต์แวร์ที่ถูกกฎหมาย และสนับสนุนนโยบายสาธารณะที่ส่งเสริมให้มีการสร้างสรรค์นวัตกรรมเทคโนโลยีและขับเคลื่อนให้เศรษฐกิจดิจิทัลเติบโต

สมาชิกของบีเอสเอรวมถึงบริษัท BSA's members include: Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, and Workday.

บีเอสเอเป็นผู้กระทำการแทนบริษัทซอฟต์แวร์ชั้นนำระดับโลก โดยมีสมาชิกเป็นบริษัทแนวหน้าด้านนวัตกรรมที่ขับเคลื่อนด้วยข้อมูล และด้านการพัฒนาความก้าวหน้าในเชิงนวัตกรรม ให้แก่เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence (AI)) เครื่องจักรสมองกล (Machine Learning) เทคโนโลยีคลาวด์เพื่อใช้ในการวิเคราะห์ และ Internet of Things (IoT) ซึ่งเป็นสิ่งที่ขับเคลื่อนเศรษฐกิจข้อมูลข่าวสารในทั่วโลกและทำให้มนุษย์มีความเป็นอยู่ในชีวิตประจำวันที่ดีขึ้น สมาชิกของเราได้รับความไว้วางใจจากลูกค้าในการจัดให้มีเทคโนโลยีรักษาความปลอดภัยที่สำคัญเพื่อปกป้องพวกเขาจากภัยคุกคามทางไซเบอร์ ภัยคุกคามเหล่านี้อาจเกิดขึ้นจากผู้ประสงค์ร้ายที่มีวัตถุประสงค์แตกต่างกันไป ซึ่งรวมถึงผู้ที่ต้องการขโมยอัตลักษณ์ของเรา ทำร้ายบุคคลที่เรารัก เอาไปซึ่งความลับที่มีค่าในทางการค้า หรือเป็นภัยต่อความมั่นคงของชาติ

จากการทำงานอย่างใกล้ชิดร่วมกับรัฐบาลทั่วโลกเพื่อพัฒนานโยบายและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ ทำให้บีเอสเอมองเห็นความเป็นไปได้ที่กฎหมายและกฎระเบียบเพื่อความมั่นคงปลอดภัยไซเบอร์จะทำหน้าที่สำคัญสองอย่างไปพร้อมกัน ได้แก่ หน้าที่ในส่วนของการป้องกันและจัดการความเสี่ยงภัยไซเบอร์ และหน้าที่ในส่วนของการคุ้มครองความเป็นส่วนตัวและสิทธิเสรีภาพของพลเมือง ดังนั้น บีเอสเอจึงได้พัฒนารอบนโยบายสากลว่าด้วยเรื่องความมั่นคงปลอดภัยไซเบอร์² (กรอบนโยบาย) รวมถึงรูปแบบของนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุม ซึ่งประเทศต่างๆ สามารถนำไปเป็นต้นแบบได้ นอกจากนี้ บีเอสเอขอแนะนำให้รัฐบาลไทยและกระทรวงฯ อ้างอิงถึงแนวทางปฏิบัติสากลที่ดีอื่น ๆ เช่น National Institute of Standards and Technology's Cybersecurity Framework³ ในขณะพิจารณาเรื่องกฎระเบียบและอื่นๆ เพื่อการบังคับใช้กฎหมาย ภายหลังจากที่ร่าง พ.ร.บ. มีผลบังคับใช้แล้ว

สมาชิกของบีเอสเอจึงเป็นผู้มีส่วนได้เสียโดยตรงในการที่รัฐบาลไทยจะเสนอร่าง พ.ร.บ. ฉบับนี้ โดยบีเอสเอ ร่วมกับสภาธุรกิจสหรัฐอเมริกาและอาเซียน (US-ASEAN Business Council) ได้เสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับก่อนหน้านี้ รายละเอียดปรากฏตามเอกสารที่แนบมาพร้อมกันนี้

- ภาคผนวก เอ: ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (17 เมษายน 2561)
- ภาคผนวก บี: ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (21 พฤษภาคม 2561)
- ภาคผนวก ซี: ความเห็นของบีเอสเอต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (6 พฤษภาคม 2558)

² กรอบนโยบายสากลว่าด้วยเรื่องความมั่นคงปลอดภัยไซเบอร์ https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf. สำหรับข้อมูลเพิ่มเติม <https://bsacybersecurity.bsa.org/>

³ The Framework for Enhancing Critical Infrastructure Cybersecurity, Version 1.1 ที่ได้ให้แนวทางเพื่อส่งเสริมความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญและเครือข่าย สำหรับข้อมูลเพิ่มเติม <https://www.nist.gov/cyberframework>.

บีเอสเอขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้สำหรับความพยายามครั้งสำคัญที่ดำเนินการเพื่อให้แน่ใจว่าประเทศไทยมีความพร้อมที่จะรองรับภัยภัยและจัดการกับภัยคุกคามไซเบอร์ เนื่องจากภัยคุกคามไซเบอร์มีความซับซ้อนและมีอันตรายขึ้นทุกวัน ความเสี่ยงที่เกิดจากนโยบายระดับประเทศที่กำหนดขึ้นอย่างไม่เพียงพอหรือไม่มีประสิทธิภาพในการรับมือกับภัยคุกคามไซเบอร์จึงอาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

ความเห็นอย่างละเอียด

ร่าง พ.ร.บ. ฉบับปัจจุบันมีการแก้ไขเพิ่มเติมร่างฉบับก่อนในประเด็นที่สำคัญ และได้รวมหลักการพื้นฐานอันจะทำให้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์บังคับใช้ได้มีประสิทธิภาพเพื่อประโยชน์ของชาวไทย โดยเฉพาะเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ทำให้เห็นได้ชัดเจนว่าเรื่องนี้เป็นวัตถุประสงค์หลักของรัฐบาลไทยอย่างไรก็ดี ร่าง พ.ร.บ. ฉบับปัจจุบันยังคงมีบทบัญญัติในหลายเรื่องที่อาจสร้างภาระเกินควรและอาจสร้างความกำกวมในแง่กฎหมายต่ออุตสาหกรรมเทคโนโลยี โดยเฉพาะการตัดบทบัญญัติที่กำหนดให้การเข้าถึงข้อมูลต้องเป็นไปตามขั้นตอนที่ชอบด้วยกฎหมาย ในหนังสือฉบับนี้ บีเอสเอขอเรียนเสนอความเห็นและแสดงข้อกังวลในเรื่องต่อไปนี้

- ความชัดเจนในขอบเขตการบังคับใช้ร่าง พ.ร.บ. ฉบับปัจจุบัน และความสัมพันธ์กับกฎหมายกฎระเบียบ และกฎเกณฑ์อื่น
- กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- อำนาจของ กปช.
- อำนาจหน้าที่ในการสอดส่องดูแล
- ความรับผิดชอบทางอาญา
- การรักษาความลับ
- การแบ่งปันข้อมูลข่าวสาร
- ประเด็นอื่นๆ

รายละเอียดมีดังนี้

เอ. ความชัดเจนในขอบเขตการบังคับใช้ร่าง พ.ร.บ. ฉบับปัจจุบัน และความสัมพันธ์กับกฎหมายกฎระเบียบ และกฎเกณฑ์อื่น

บีเอสเอสนับสนุนการจำกัดขอบเขตของการแจ้งเตือน รายงาน จัดการ และรับมือกับสถานการณ์ (มาตรา 38-58) ในร่าง พ.ร.บ. ฉบับนี้ ที่ใช้เฉพาะกับระบบข้อมูลของหน่วยงานรัฐและหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) (หรือ

หน่วยงานเอกชน) อย่างไรก็ตาม บีเอสเอเห็นว่าคำจำกัดความของ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ควรมีความชัดเจน ดังต่อไปนี้

1. แนวคิดเกี่ยวกับ “โครงสร้างพื้นฐานสำคัญ” (Critical infrastructure) ควรสอดคล้องกันกับแนวทางสากล และควรมีคำจำกัดความดังนี้

- “ทรัพย์สิน บริการ และระบบ ไม่ว่าที่จับต้องได้หรือเสมือนจริง ที่หากถูกทำลาย ถูกทำให้เสียหาย หรือไม่สามารใช้การได้เป็นระยะเวลาแล้ว จะส่งผลกระทบต่อความมั่นคงของชาติ สาธารณสุข ความปลอดภัยของประชาชน ความมั่นคงด้านเศรษฐกิจของชาติ หรือการปฏิบัติงานหลักของหน่วยงานในระดับท้องถิ่นหรือระดับชาติ”

ด้วยเหตุนี้ กปช. จึงควรกำหนดว่าโครงสร้างพื้นฐานใดเป็นโครงสร้างพื้นฐานที่สำคัญ โดยพิจารณาจากความสำคัญ และความสำคัญของผลกระทบที่จะเกิดขึ้นกับประเทศไทย ความจำเป็นต่อระบบอื่น และระดับความเสี่ยง มิใช่พิจารณาจากภารกิจหรือบริการของแต่ละหน่วยงาน ตามที่กำหนดไว้ใน **มาตรา 43** การกำหนดให้หน่วยงานที่มีภารกิจหรือบริการในเจ็ดด้านเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นมีขอบเขตที่กว้างเกินไปโดยมิได้คำนึงถึงข้อเท็จจริงว่า ภายในแต่ละหน่วยงานมีโครงสร้างพื้นฐานเพียงบางประการเท่านั้นที่เป็นโครงสร้างพื้นฐานที่สำคัญ

2. ต้องมีความชัดเจนเกี่ยวกับองค์กร ที่เป็น “หน่วยงานเอกชน” ที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) เพราะในบางสถานการณ์ อาจมีองค์กรที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) อันเดียวกันมากกว่าหนึ่งแห่ง เช่น กรณีของการมอบหมายให้ องค์กรภายนอกปฏิบัติงานบางส่วน (Outsource) บีเอสเอจึงขอแนะนำให้มีการกำหนดความชัดเจนเกี่ยวกับหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) และขอเสนอแนวคิดดังนี้

- หน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) หมายถึงองค์กรที่มีอำนาจควบคุมเหนือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือมีหน้าที่รับผิดชอบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเป็นเจ้าของสินทรัพย์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศในทางกฎหมาย
- ในสถานการณ์ที่มีองค์กรที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศมากกว่าหนึ่งองค์กร คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) ควรปรึกษากับหน่วยงานที่ทำหน้าที่กำกับดูแลของแต่ละหน่วยงาน เพื่อกำหนดความชัดเจนเกี่ยวกับองค์กรเหล่านั้น

3. ความชัดเจนเรื่องความรับผิดชอบของ “หน่วยงานเอกชน” ที่ปฏิบัติงานเกี่ยวกับโครงสร้าง

พื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ที่ต้องทำให้แน่ใจว่า
คู่ค้าของตนทำตามข้อกำหนดที่จำเป็นด้านความปลอดภัย

หน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรยังคงมีหน้าที่รับผิดชอบโดยรวมในเรื่องความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และร่าง พ.ร.บ. ฉบับปัจจุบันไม่ควรกำหนดความรับผิดชอบให้กับคู่ค้าที่เป็นองค์กรภายนอกของหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และควรกำหนดให้ชัดเจนว่าหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถสร้างข้อกำหนดที่จำเป็นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในสัญญาที่ทำกับคู่ค้าที่เป็นองค์กรภายนอกของตนได้

4. ความชัดเจนเรื่องการบังคับใช้ร่าง พ.ร.บ. ฉบับปัจจุบัน กับกฎหมายอื่นที่มีอยู่แล้วในแต่ละหน่วยงาน เช่น กฎหมาย กฎระเบียบ และกฎเกณฑ์ ของธนาคารแห่งประเทศไทย สำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เป็นต้น โดยเฉพาะไม่ชัดเจนเกี่ยวกับเรื่องการรายงานที่จะเข้าช้อนระหว่างคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) กับหน่วยงานที่ทำหน้าที่กำกับดูแลของแต่ละหน่วยงานหรือไม่ บีเอสเอขอแนะนำให้กระทรวงฯ เพิ่มบทบัญญัติในร่าง พ.ร.บ. เพื่อสร้างความชัดเจนในเรื่องนี้

บี. กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ในหนังสือเสนอความเห็นของบีเอสเอต่อร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2558 และปี 2561 บีเอสเอได้เน้นในประเด็นที่ว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) ควรประกอบด้วยกรรมการที่มาจากหลายที่มามากขึ้น โดยรวมถึงกรรมการที่จะปกป้องผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของบุคคลด้วย เช่น กรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดิน นอกจากนี้ บีเอสเอขอเรียนเสนอว่าการดำเนินการในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ควรมีหน่วยงานของรัฐบาลพลเรือนเป็นผู้มีหน้าที่รับผิดชอบเป็นหลัก เนื่องจากภัยคุกคามทางไซเบอร์อาจส่งผลกระทบต่อผลประโยชน์ทางด้านเศรษฐกิจทั้งในระดับชาติและระดับนานาชาติได้ในวงกว้าง กปช. จึงควรมีกรรมการที่จะดูแลรักษาผลประโยชน์ดังกล่าวอยู่ด้วย นอกจากนี้ บีเอสเอขอเรียนเสนอให้ กปช. มีกรรมการที่มาจากภาคอุตสาหกรรมด้วย เพื่อให้มีมุมมองที่รอบด้านขึ้น อีกทั้งเป็นการส่งเสริมความร่วมมือระหว่างภาครัฐกับภาคเอกชน อันจะนำไปสู่วิถีปฏิบัติที่เป็นไปอย่างมีประสิทธิภาพสูงสุด

ในร่าง พ.ร.บ. ฉบับปัจจุบัน กปช. ก็ยังคงไม่มีกรรมการที่จะดูแลรักษาผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชน ด้วยเหตุนี้ กรรมการยังมีแต่กรรมการที่เป็นผู้บังคับใช้กฎหมายและกรรมการที่เป็นผู้รักษาความมั่นคงของประเทศ โดยมีรัฐมนตรีว่าการกระทรวงกลาโหมเป็นรองประธานกรรมการ

อนึ่ง มาตรา 19 ของร่าง พ.ร.บ. ฉบับปัจจุบัน ได้บัญญัติเพิ่มเติมเกี่ยวกับคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (คณะกรรมการกำกับสำนักงาน) ซึ่งมีกรรมการที่มาจากฝ่ายพลเรือนเป็นส่วนใหญ่ โดยมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ บีเอสเอเห็นว่าคณะกรรมการกำกับสำนักงานควรมีกรรมการที่มาจากหลากหลายหน่วยงานเช่นกัน โดยมาจากทั้งภาคประชาชนและภาคเอกชน

ซี. การมีอำนาจอย่างกว้างขวางของ กปช.

บีเอสเอยังคงเห็นด้วยที่มาตรา 9 แห่งร่างพระราชบัญญัติฯ กำหนดให้ กปช. มีอำนาจหน้าที่เป็นศูนย์กลางในการประสานงานระหว่างหน่วยงานเพื่อรับมือกับภัยคุกคามไซเบอร์และสถานการณ์ด้านภัยคุกคามไซเบอร์ การกำหนดให้มีหน่วยงานระดับประเทศเพียงหน่วยงานเดียวทำหน้าที่เป็นหน่วยงานหลักที่มีความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะทำให้เกิดความชัดเจน มีความสอดคล้องและเป็นไปในทิศทางเดียวกันในการเตรียมความพร้อมของรัฐบาลในการรับมือกับภัยคุกคามและปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ บีเอสเอยังการเปลี่ยนแปลงในทางที่ดีของการใช้อำนาจของ กปช. ที่จำกัดให้เฉพาะในสถานการณ์ “การโจมตีทางไซเบอร์ที่ร้ายแรง” (มาตรา 56-58) อย่างไรก็ตาม บีเอสเอยังคงมีความกังวลเรื่องขอบเขตอำนาจของ กปช. อยู่

1. อำนาจของ กปช. ควรใช้เฉพาะกับหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยจำกัดเฉพาะบริษัทที่จัดตั้งขึ้นในประเทศไทยและเป็นผู้ประกอบการหรือเป็นผู้ควบคุมโครงสร้างพื้นฐานที่สำคัญในประเทศไทยเท่านั้น องค์กรระหว่างประเทศที่มีสำนักงานตั้งอยู่ในประเทศไทย อาจมีโครงสร้างพื้นฐานและระบบเทคโนโลยีสารสนเทศ โดยทั้งหมดที่ตั้งอยู่นอกประเทศไทย จึงจำเป็นที่ร่าง พ.ร.บ. ต้องสร้างความชัดเจนว่า “คอมพิวเตอร์” และ “ระบบคอมพิวเตอร์” โดยทั้งหมดที่ตั้งอยู่นอกประเทศไทย ไม่ได้เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อหลีกเลี่ยงความขัดแย้งกันระหว่างกฎหมายระหว่างประเทศที่อาจจะเกิดขึ้น
2. การให้อำนาจที่กว้างขวางตามมาตรา 56 ถึงมาตรา 58 ในกรณี “ภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง” ควรต้องให้คำจำกัดความในลักษณะที่สอดคล้องกับวิธีปฏิบัติที่ดีของสากลในประเด็นนี้ บีเอสเอขอเรียนย้ำว่าควรให้คำจำกัดความดังนี้
 - “ภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง” หมายความว่า “เหตุภัยคุกคามทางไซเบอร์ที่ทำให้ (i) มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือมีการถูกปฏิเสธไม่ให้เข้าถึงข้อมูล หรือมีการทำลาย ลบ ปรับเปลี่ยน หรือระงับข้อมูลที่จำเป็นต่อการทำงานของโครงสร้างพื้นฐานที่สำคัญ หรือ (ii) การควบคุมการปฏิบัติการหรือการควบคุมทางเทคนิคที่จำเป็นต่อความปลอดภัยหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญถูกโจมตี”

นอกจากนี้ บีเอสเอขอเรียนเสนอคำจำกัดความของ “ภัยคุกคามทางไซเบอร์” ดังนี้

- “ภัยคุกคามทางไซเบอร์” หมายความว่า “เหตุการณ์ที่โดยตั้งใจเพื่อก่อให้เกิดผลกระทบที่ร้ายแรงต่อความมั่นคงปลอดภัย การมีอยู่ การรักษาความลับ หรือความสมบูรณ์ของระบบสารสนเทศ หรือข้อมูลที่ถูกเก็บไว้ หรือที่ถูกประมวลผลโดยระบบสารสนเทศ หรือที่ถูกส่งต่อไปยังระบบสารสนเทศ”

นอกจากนี้ ร่าง พ.ร.บ. ฉบับนี้ ควรระบุเหตุการณ์ใดที่เรียกว่าร้ายแรง เพื่อความชัดเจนในเรื่องการใช้อำนาจสืบสวน

3. การกำหนดขอบเขตอำนาจของ กปช. ก่อให้เกิดหน้าที่ในส่วน of หน่วยงานเอกชน (มาตรา 38, 40, 44-45 และ 53-58) การให้อำนาจแก่ กปช. อย่างกว้างขวาง อาจส่งผลกระทบต่อ การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของภาคพลเรือน และอาจบั่นทอนความร่วมมือจากภาคเอกชน เพื่อป้องกันความเสี่ยงที่จะมีต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังนั้น ควรกำหนดและจำกัดอำนาจที่ให้แก่ กปช. ให้มีความชัดเจนยิ่งขึ้น รวมถึงให้มีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาล อีกทั้งหน่วยงานเอกชนควรมีโอกาสอย่างเต็มที่ในการโต้แย้งคำสั่งและมีสิทธิยื่นอุทธรณ์ต่อศาลหากไม่เห็นพ้องด้วยกับคำวินิจฉัย นอกจากนี้ บทบัญญัติที่จำกัดอำนาจบางประการโดยกำหนดให้ต้องได้รับคำสั่งศาลก่อนดำเนินการ (เว้นแต่ในกรณีจำเป็นเร่งด่วน) นั้นถูกตัดออกไปจากร่างพระราชบัญญัติฉบับนี้ บีเอสเอจึงขอเรียนว่าควรจำกัดอำนาจโดยกำหนดให้ต้องได้รับคำสั่งศาลก่อนดำเนินการเช่นเดิม นอกจากนี้ การใช้อำนาจของ กปช. ควรต้องมีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาลในหลายกรณีมากขึ้น เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับ “หน่วยงานเอกชน”

โดยเฉพาะบทบัญญัติในมาตรา 46 มีลักษณะที่กว้างมาก และดูเหมือนจะสวนทางกับร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงฯ และแนวทางปฏิบัติสากล ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการแก้ไขเมื่อเร็วๆ นี้ เพื่อให้สอดคล้องกับหลักการของกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป แต่ระดับของการคุ้มครองเจ้าของข้อมูลภายใต้ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กลับไม่สอดคล้องกันกับหลักการของ GDPR ยิ่งไปกว่านั้น ในย่อหน้าที่ 2 ของมาตรา 46 กลับสร้างความเป็นโมฆะให้แก่กฎหมายทั้งหมดที่อาจใช้ได้กับหน่วยงานเอกชน รวมถึงความเป็นโมฆะของสัญญาที่ถูกใช้เป็นเครื่องมือที่สมควรในเรื่องการเปิดเผยข้อมูลและคุ้มครองเจ้าของข้อมูลและสิทธิในเชิงพาณิชย์ นับเป็นเรื่องที่สวนทางกับแนวทางปฏิบัติสากลที่ดีในการคุ้มครองข้อมูลส่วนบุคคล และเกือบจะเป็นไปไม่ได้ในการบังคับใช้ โดยเฉพาะหากหน่วยงานเอกชนมีหน้าที่ต้องปฏิบัติตามกฎหมายของประเทศอื่น

บีเอสเอขอแนะนำให้แก้ไขปัญหาดังกล่าว โดยกำหนดลักษณะของข้อมูลที่บัญญัติไว้ในมาตรา 46 (1)-(3) ให้แคบลง และเพิ่มขึ้นต่อนตามกระบวนการยุติธรรมที่หน่วยงานเอกชนสามารถใช้สิทธิโต้แย้งที่มีอยู่ได้ นอกจากนี้ ขอแนะนำให้ลบทั้งย่อหน้าที่ 2 ของมาตรา 46 ที่ระบุว่า “หน่วยงานที่ได้รับหนังสือตามวรรคหนึ่ง ไม่อาจยกเอาหน้าที่ตามกฎหมายอื่น หรือตามสัญญามาเป็น

ข้ออ้างเพื่อไม่เปิดเผยข้อมูล” ในกรณีนี้ การดำเนินการที่เป็นการปฏิบัติตามมาตรานี้ที่ทำโดยเจตนาสุจริต ไม่ควรถูกพิจารณาว่าเป็นการฝ่าฝืนกฎหมายหรือสัญญา

ตัวอย่างเช่น กปช. ควรมีอำนาจที่ยึดเครื่องคอมพิวเตอร์โดยไม่ต้องมีคำสั่งศาลได้เฉพาะในกรณีมีภัยหรือเกิดเหตุการณ์คุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ซึ่งเป็นสถานการณ์ที่มีความจำเป็นเร่งด่วน และไม่มีความเสี่ยงที่สมควรเพื่อให้บรรลุวัตถุประสงค์ของการสืบสวนได้ และควรทำการยึดเครื่องคอมพิวเตอร์ภายหลังจากที่มีการปรึกษาหารือกับองค์กรเอกชนและได้พิจารณาถึงความสำคัญของเครื่องคอมพิวเตอร์ที่มีต่อธุรกิจและความจำเป็นในการปฏิบัติงานขององค์กรเอกชนนั้นแล้ว กล่าวคือการยึดเครื่องคอมพิวเตอร์ควรต้องมีความจำเป็นมากกว่าผลเสียหายร้ายแรงที่จะมีต่อองค์กรเอกชนนั้น

- 4. การกำหนดหน้าที่แก่หน่วยงานเอกชนตลอดร่างพระราชบัญญัติฯ ควรจำกัดเฉพาะหน้าที่ตามสมควรและทำได้จริงในทางปฏิบัติ** บีเอสเอยังคงมีความกังวลเนื่องจากร่างพระราชบัญญัติฯ นี้ กำหนดหน้าที่แก่หน่วยงานเอกชน (เช่น มาตรา 56 และมาตรา 58) อันทำให้หน่วยงานเอกชนต้องดำเนินการบางประการเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ซึ่งอาจไม่ได้อยู่ภายใต้การควบคุมของตน หรืออาจเป็นหน้าที่เกินสมควร ไม่สามารถปฏิบัติได้จริง หรือไม่ได้สัดส่วน

การปฏิบัติตามกฎหมายใดๆ ที่หน่วยงานเอกชนต้องดำเนินการ (รวมถึง การดำเนินการ การจัดใช้เข้าถึงข้อมูล การให้ข้อมูล และ/หรือ การให้เอกสาร รายงาน เป็นต้น) ต้องเป็นให้เป็นไปตามคำสั่งศาลหรือหมายศาลที่มีสภาพบังคับและเป็นไปตามกระบวนการยุติธรรม นอกจากนี้ ร่าง พ.ร.บ. ฉบับปัจจุบันควรต้องระบุรายละเอียดและขอบเขตของการร้องขอให้เฉพาะเจาะจงและชัดเจน และเป็นการร้องขอเฉพาะกับข้อมูลหรือเอกสารที่หน่วยงานเอกชนมีอำนาจควบคุมในลักษณะที่สมเหตุสมผลในเชิงพาณิชย์และเหมาะสมในสถานการณ์นั้นๆ คำแนะนำเหล่านี้เกิดจากสภาพความเป็นจริงในเชิงพาณิชย์ที่หน่วยงานเอกชนไม่ได้อยู่ในสถานะเดียวกับหน่วยงานภาครัฐ และร่าง พ.ร.บ. ฉบับนี้ ไม่ควรสร้างข้อบังคับไม่สมควรให้แก่หน่วยงานเอกชน

ยกตัวอย่างเช่น การกระทำหลายอย่างที่กำหนดไว้ในมาตรา 57 และ 58 มีลักษณะที่ไม่สมเหตุสมผลหรือเป็นไปได้ในทางปฏิบัติสำหรับหน่วยงานเอกชน เพราะอาจทำให้เกิดการเปลี่ยนแปลงในพื้นฐานที่สำคัญของรูปแบบการดำเนินธุรกิจ เพียงเพื่อให้สามารถตอบสนองตามที่ร่าง พ.ร.บ. ฉบับปัจจุบันต้องการ และหากต้องทำเช่นนั้น อาจส่งผลกระทบต่อความสามารถในการดำเนินธุรกิจให้บริการแก่ลูกค้า ในขณะที่เดียวกัน มาตรา 58 (4) ที่ให้อำนาจเลขาธิการทำการทำการ “ยึดคอมพิวเตอร์หรืออุปกรณ์ใดๆ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์” ควรจำกัดหน้าที่ของหน่วยงานเอกชนเพียงเท่าที่จะกระทำได้ที่ภายใต้อำนาจควบคุมของตน และความสมเหตุสมผลในเชิงพาณิชย์ในสถานการณ์นั้น

นอกจากนี้ การคาดหวังให้หน่วยงานเอกชนรายงานภัยคุกคามทางไซเบอร์ที่คาดการณ์ได้ เป็นเรื่องที่ไม่

สมเหตุสมผลหรือเป็นไปได้ จึงควรลดมาตรา 51 ออกไปจากร่าง พ.ร.บ. ฉบับปัจจุบัน เนื่องจาก ภัยคุกคามไซเบอร์ที่คาดการณ์ได้ว่าจะเกิด และต้นตอของภัยคุกคามดังกล่าวมีการเปลี่ยนแปลงอยู่ตลอดเวลา ในปัจจุบัน มีบริการบางอย่างที่ต้องเผชิญกับภัยคุกคามไซเบอร์มากมายอยู่ทุกวัน ส่วนใหญ่ของภัยคุกคามได้รับการป้องกันไปแล้ว ในขณะที่องค์กรสามารถมีมาตรการที่ถูกออกแบบมาเพื่อป้องกันภัยคุกคามไซเบอร์ได้ตามแนวทางปฏิบัติที่เกิดขึ้น การระบุว่า จะเกิดภัยคุกคามไซเบอร์อะไรบ้างทั้งหมด หรือการแจ้งภัยคุกคามไซเบอร์ทั้งหมด ที่มี “โอกาสจะเกิดขึ้น” ให้หน่วยงานที่มีอำนาจทราบ จึงเป็นไปได้ การแจ้งภัยคุกคามไซเบอร์ โดยปราศจากความเสี่ยงที่แท้จริง อาจทำให้เกิดจำนวนของการแจ้งที่มากเกินไปจนเกิดความจำเป็น นำไปสู่ภาระที่เกินกว่าเหตุสำหรับหน่วยงานเอกชน และอาจทำให้หน่วยงานเอกชนเกิดข้อผิดพลาดในการแจ้งภัยคุกคามไซเบอร์ที่เป็นความเสี่ยงที่แท้จริง เมื่อถึงเวลาจริงๆ

ดังนั้น จึงจำเป็นที่ร่าง พ.ร.บ. ฉบับนี้ต้องเพิ่มบทบัญญัติที่รองรับความคล่องตัวของการทำงานของหน่วยงานเอกชนที่ต้องสมดุลย์ให้ได้สัดส่วนกับการใช้อำนาจ บีเอสเอขอแนะนำ กปช. ควรกำหนดมาตรการที่เหมาะสมสำหรับการสืบสวน สำหรับสถานการณ์ของภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง โดยปรึกษากับหน่วยงานที่ทำหน้าที่กำกับดูแลและหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

5. มาตรา 56 ถึงมาตรา 58 อันเป็นเรื่องภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ควรจำกัดเฉพาะหน่วยงานที่ได้รับผลกระทบโดยตรงจากภัยคุกคามนั้น เพื่อที่จะได้หลีกเลี่ยงไม่ให้ตีความได้ว่าหน่วยงานเอกชนที่ไม่ได้รับผลกระทบจะต้องมีหน้าที่ตามมาตรานี้

ดี. อำนาจในการสอดส่องดูแล

บีเอสเอมีความกังวลเป็นอย่างยิ่งในเรื่องที่ร่าง พ.ร.บ. ฉบับปัจจุบัน ไม่มีบทบัญญัติที่กำหนดให้ต้องได้รับคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสารของหน่วยงานเอกชน จึงขอแนะนำดังต่อไปนี้

1. บีเอสเอแนะนำว่าเป็นเรื่องจำเป็นอย่างยิ่งที่ร่าง พ.ร.บ. ฉบับปัจจุบัน ต้องมีคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสารของหน่วยงานเอกชน การใช้อำนาจให้ได้มาซึ่งข้อมูล (รวมถึงการยึดสินทรัพย์) ควรดำเนินอยู่ภายใต้เครื่องมือทางกฎหมาย มิเช่นนั้น จะไม่มีการบันทึกเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ขอบเขต วัตถุประสงค์ บริบท หรือระยะเวลา มุมมองของบีเอสเอคือควรต้องมีเอกสาร เช่น หมายศาล หรือ “เอกสารชั่วคราวในกรณีฉุกเฉิน” ที่กำหนดกระบวนการของการให้ได้มาซึ่งข้อมูล

การที่กฎหมายไม่มีบทบัญญัติที่กำหนดให้ดำเนินการตามขั้นตอนที่ชอบด้วยกฎหมายทำให้เกิดการละเมิดความเป็นส่วนตัวของลูกค้าของหน่วยงานเอกชนนั้น และจะลดความเชื่อมั่นของผู้บริโภค เนื่องจากผู้ประกอบการไม่อาจรับรองได้ว่า จะไม่มีผู้ใดเข้าถึงข้อมูลส่วนบุคคลหรือความลับทางการค้าของผู้บริโภคโดยไม่ได้รับอนุญาต นอกจากนี้ การที่กฎหมายไม่มีบทบัญญัติที่กำหนดให้ดำเนินการ

ตามขั้นตอนที่ขอด้วยกฎหมายอาจทำให้เกิดการขัดกันแห่งกฎหมายระหว่างประเทศ และสร้างปัญหาให้แก่องค์กรระหว่างประเทศในเรื่องการปฏิบัติตามกฎหมาย

2. การยกเว้นไม่ต้องขอคำสั่งศาลจำเป็นต้องกำหนดเป็นหลายลักษณะอักษรที่ชัดเจน บีเอสเอขอแนะนำว่าต้องกำหนด “กรณีเร่งด่วน” ที่ได้รับการยกเว้นให้ชัดเจนว่าเป็นกรณีที่น่าจะเป็นสาเหตุของภัยต่อความมั่นคงของประเทศ
3. องค์กรอิสระควรเข้ามากำกับดูแลการใช้อำนาจของ กปช. เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามที่กำหนดในพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรมีอำนาจในการตรวจสอบการใช้อำนาจของ กปช. ในการเข้าถึงข้อมูลของหน่วยงานเอกชน เพื่อให้มั่นใจว่ามีการถ่วงดุลระหว่างการคุ้มครองสิทธิส่วนบุคคลกับความจำเป็นในการสอดส่องดูแล
4. นอกจากนี้ บีเอสเอขอแนะนำให้เพิ่มเติมบทบัญญัติเกี่ยวกับขั้นตอนสำหรับการเข้าถึงและให้ได้มาซึ่งข้อมูล ขั้นตอนเหล่านั้นได้แก่
 - คำสั่ง คำบัญชาการ หรือคำขอทั้งหมด เพื่อให้ได้มาซึ่งข้อมูล หรือความช่วยเหลือ ควร มีข้อจำกัด กล่าวคือ ใช้เฉพาะกับสถานการณ์ที่เป็นความเสี่ยงที่จะทำให้เกิดความเสียหายในระดับร้ายแรง บีเอสเอแนะนำว่าควรต้องพิจารณาผลกระทบต่อชุมชน ภาคธุรกิจ และควรต้องมีข้อพิจารณาในทางปฏิบัติอื่นๆ เพื่อถ่วงดุลความเสียหายดังกล่าวที่อาจเกิดขึ้น หากไม่มีข้อจำกัดและการดูแล จะทำให้องค์กรที่ตกเป็นเหยื่อของการจู่โจม หรือถูกละเมิดข้อมูล เข้าใจว่าเป็นหน้าที่ที่ต้องให้ข้อมูลตามคำสั่ง มากกว่าเข้าใจว่าหน่วยงานรัฐกำลังส่งเสริมให้เกิดความร่วมมือ
 - การขอข้อมูลจากหน่วยงานเอกชนควรมีกรณียกเว้นและควรต้องแจ้งให้บุคคลภายนอกที่ได้รับผลกระทบทราบ บีเอสเอขอเรียนเสนอว่า บุคคลภายนอกที่เป็นเจ้าของข้อมูลที่ถูกเปิดเผยควรมีสสิทธิต่รับแจ้งก่อนที่จะมีการเปิดเผยข้อมูลนั้นเพื่อให้บุคคลภายนอกดังกล่าวได้มีโอกาสคัดค้านการเปิดเผยข้อมูล
 - ควรกำหนดให้คำสั่งศาลมีผลเพียงช่วงระยะเวลาหนึ่ง บีเอสเอขอเรียนเสนอว่า คำสั่งศาลไม่ควรมีผลบังคับโดยไม่จำกัดระยะเวลา เนื่องจากอาจก่อให้เกิดความไม่ชัดเจนมากขึ้นต่อหน่วยงานเอกชน
5. กฎหมายลำดับรอง กฎเกณฑ์อื่น หรือข้อบังคับ ควรต้องทำผ่านกระบวนการรับฟังความคิดเห็นก่อนเสมอ และควรประกาศใช้พร้อมกันกับร่าง พ.ร.บ. ฉบับนี้

อี. ความรับผิดชอบทางอาญา

บีเอสเอเห็นว่า มาตรา 62 และมาตรา 63 แห่งร่างพระราชบัญญัติฯ ได้กำหนดโทษทางอาญาสำหรับการกระทำที่ฝ่าฝืนร่างพระราชบัญญัติฯ ในเรื่องนี้ บีเอสเอเห็นว่า การดำเนินคดีอาญาควรจำกัดเฉพาะในกรณี ที่ผู้กระทำผิดก่อความเสียหาย หรือก่อให้เกิดปัญหาต่อโลกไซเบอร์ด้วยเจตนาทุจริตเท่านั้น

บีเอสเอเห็นว่า การกำหนดโทษทางอาญาต่อหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำขอของ กปช. ตาม มาตรา 57 และมาตรา 58 นั้นเป็นบทลงโทษที่รุนแรงเกินควร และไม่ควรมีโทษทางอาญาสำหรับการกระทำ ความผิดโดยไม่ตั้งใจ หรือเนื่องจากเหตุผลทางเทคนิค อันอาจทำให้บริษัทต่างชาติระงับแผนที่จะเข้ามาประกอบธุรกิจในประเทศไทยหากมีความเสี่ยงว่าบุคลากรของตนจะต้องมีความรับผิดชอบทางอาญา สำหรับการกระทำ ความผิดโดยไม่ตั้งใจหรือการกระทำ ความผิดเพียงเล็กน้อย

เอฟ. การรักษาความลับ

บีเอสเอเห็นว่าบทบัญญัติที่เกี่ยวกับการรักษาความลับถูกลบทิ้งไปจากร่าง พ.ร.บ. ฉบับนี้ จึงขอเรียนเสนอ เช่นเดิมว่า ร่างพระราชบัญญัติฯ ควรมีบทบัญญัติเพิ่มเติมที่ชัดเจนในเรื่องการรักษาความลับของข้อมูล ที่อ่อนไหวและข้อมูลส่วนบุคคล ซึ่งรวมถึงการกำหนดหน้าที่ที่ชัดเจนของพนักงานเจ้าหน้าที่ในการปกป้อง และรักษาความลับของข้อมูลดังกล่าว รวมถึงการกำหนดหน้าที่และขั้นตอนในการขอความยินยอม และวิธีใช้ เปิดเผย เก็บ และกำจัดข้อมูลดังกล่าวเมื่อไม่จำเป็นแล้วตามวัตถุประสงค์ทางกฎหมายของผู้ออก คำสั่ง

นอกจากนี้ ควรกำหนดประเภทของข้อมูลที่ได้รับการยกเว้นไม่ต้องเปิดเผย เช่นข้อมูลที่ได้รับสิทธิ พิเศษ หรือข้อมูลที่จะก่อให้เกิดการละเมิดสิทธิอื่น เช่นข้อมูลส่วนบุคคล หรือละเมิดสิทธิในทรัพย์สินทาง ปัญญาหรือความลับทางการค้า

ควรกำหนดให้เจ้าพนักงานของ กปช. มีความรับผิดชอบทางอาญาด้วยหากมีการนำข้อมูลดังกล่าวไป ใช้ในทางที่มีขอบด้วยเช่นกัน

จี. การแบ่งปันข้อมูลข่าวสาร

บีเอสเอเห็นว่า การแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ ช่องโหว่ และเหตุทางไซเบอร์ ต่อ ผู้ที่ได้รับผลกระทบ ตลอดจนหน่วยงานอื่นๆ เพื่อป้องกันการโจมตี เป็นเรื่องที่สำคัญต่อการส่งเสริมการ รักษาความมั่นคงปลอดภัยทางไซเบอร์

บีเอสเอขอเรียนย้ำว่า ร่างพระราชบัญญัติฯ ควรสนับสนุนให้มีการจัดทำนโยบายที่มีประสิทธิภาพในเรื่อง การแบ่งปันข้อมูลข่าวสารระหว่างภาครัฐและเอกชน ระหว่างหน่วยงานเอกชนด้วยกัน และระหว่าง หน่วยงานของรัฐด้วยกัน นอกจากนี้ นโยบายเรื่องการแบ่งปันข้อมูลข่าวสารควรมีข้อจำกัดเกี่ยวกับความ รับผิดชอบของหน่วยงานที่เป็นผู้แบ่งปันข้อมูลข่าวสาร โดยที่ยังคงสามารถปกป้องความเป็นส่วนตัวของผู้ที่ ได้รับผลกระทบจากการแบ่งปันข้อมูลข่าวสาร อำนวยความสะดวกในการแบ่งปันข้อมูลข่าวสารหลายทาง ส่งเสริมให้ดำเนินการอย่างทันท่วงที และทำให้แน่ใจว่าข้อมูลข่าวสารที่ได้รับไปนั้นจะใช้เพื่อส่งเสริมการ รักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น

เอช. ระยะเวลาของการบังคับใช้กฎหมาย

รัฐบาลควรกำหนดระยะเวลาอันสมควรระหว่างการประกาศใช้และการบังคับใช้กฎหมาย ซึ่งจะทำให้เกิดประโยชน์มากกว่ากับบุคคล องค์กรธุรกิจ และรัฐบาลเอง นอกจากนี้ รัฐบาลยังออกแนวทางในการปฏิบัติ ตามกฎหมายใหม่นี้ ในช่วงระยะเวลาระหว่างการประกาศใช้และการบังคับใช้กฎหมาย รวมถึงองค์กรธุรกิจ สามารถเตรียมตัวเพื่อประเมินความพร้อมในการปฏิบัติตามกฎหมายใหม่ที่กำลังจะมีการบังคับใช้ โดยทั่วไป ในประเทศอื่น ระยะเวลาการประกาศใช้และการบังคับใช้กฎหมายว่าด้วยเรื่องการป้องกันภัยไซเบอร์จะอยู่ที่ 2 ปี บีเอสเอขอแนะนำให้กระทรวงฯ ให้ระยะเวลาไม่น้อยกว่า 2 ปี ก่อนที่จะมีการ บังคับใช้กฎหมาย

ไอ. แง่มุมอื่น ๆ ของนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

นอกจากนี้ บีเอสเอขอเรียนย้ำว่า นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยควร ครอบคลุมประเด็นที่สำคัญอื่นๆ ด้วย เช่น การปฏิบัติตามแนวทางในการจัดซื้อเทคโนโลยีและซอฟต์แวร์ ของภาครัฐ การให้การสนับสนุนจากรัฐบาลอย่างเต็มที่ในด้านการวิจัยและพัฒนาเทคโนโลยีสำหรับการ รักษาความมั่นคงปลอดภัยไซเบอร์ โครงการให้ความรู้เพื่อเพิ่มความตระหนักรู้ การฝึกอบรม และการ จัดทำนโยบายต่างประเทศให้ครอบคลุมถึงเรื่องการประสานความร่วมมือในการรักษาความมั่นคงปลอดภัย ไซเบอร์ บีเอสเอขอสนับสนุนให้รัฐบาลไทยพิจารณาเพิ่มเติมประเด็นที่สำคัญเหล่านี้ไว้ในระเบียบข้อบังคับ ที่ออกโดยอาศัยร่างพระราชบัญญัตินี้

บทสรุปและการดำเนินการขั้นต่อไป

บีเอสเอขอแสดงความชื่นชมรัฐบาลไทยอีกครั้งสำหรับความพยายามในการปกป้องโครงสร้างพื้นฐานจาก ภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ตาม บีเอสเอใคร่ขอความอนุเคราะห์ให้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาประเด็นที่ได้เรียนเสนอไว้ข้างต้น เพื่อที่กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมจะสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มี ประสิทธิภาพ ซึ่งคำนึงถึงเรื่องความเสี่ยงเป็นหลักและสอดคล้องกับแนวปฏิบัติในระดับสากล อันจะช่วย เสริมสร้างความเชื่อมั่นระหว่างภาครัฐและเอกชน และยกระดับความมั่นคงปลอดภัยของข้อมูลและ โครงสร้างพื้นฐาน

นอกจากนี้ รัฐบาลควรเน้นย้ำเรื่องการป้องกันและการลดความเสี่ยงภัยไซเบอร์ โดยส่งเสริมให้องค์กร ปฏิบัติตามวิธีปฏิบัติที่ดีที่มีอยู่แล้ว หรือมีแนวทางป้องกันภัยไซเบอร์ที่ดี เช่น การใช้ซอฟต์แวร์ที่มีสัญญา อนุญาตให้ใช้สิทธิและได้รับบริการความช่วยเหลือจากบริษัทซอฟต์แวร์ รวมถึงการใช้ฮาร์ดแวร์ด้วย ที่ต้อง ได้รับบริการอัปเดตด้านความปลอดภัยอย่างสม่ำเสมอ ตลอดจนไปถึงการป้องกันเครือข่ายที่มี ประสิทธิภาพ ขั้นตอนการรับมือกับสถานการณ์ที่เกิดขึ้น การจัดการลดความเสี่ยง

บีเอสเอยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อนางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่

varuneer@bsa.org หรือที่หมายเลข +668-1840-0591 บีเอสเอขอขอบพระคุณที่ท่านสละเวลาพิจารณา
ในเรื่องนี้

ขอแสดงความนับถือ

เจเร็ด แร็กแลนด์

ผู้อำนวยการอาวุโส ฝ่ายนโยบาย ภูมิภาคเอเชียแปซิฟิก

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง

ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ภาคผนวก เอ

ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคง
ปลอดภัยไซเบอร์
(17 เมษายน 2561)

(กระดาษหัวจดหมายของบีเอสเอ)

(สมาชิกรัฐสภาสหรัฐอเมริกา-อาเซียน)

วันที่ 17 เมษายน 2561

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวง
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
120 หมู่ที่ 3 ชั้น 6-9
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ
ทุ่งสองห้อง หลักสี่ กรุงเทพมหานคร 10210

เรื่อง ความเห็นของภาคอุตสาหกรรมในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านปลัดกระทรวง

1. ความนำและคำชี้แจงเรื่องส่วนได้เสียในร่างพระราชบัญญัติ

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (“บีเอสเอ”)¹ และสมาชิกรัฐสภาสหรัฐอเมริกา-อาเซียน (สมาชิกรัฐฯ)² เป็นผู้กระทำการแทนบริษัทอเมริกันชั้นนำด้านเทคโนโลยีที่ประกอบธุรกิจในประเทศไทย โดยมีสมาชิกเป็นบริษัทแนวหน้าด้านนวัตกรรมที่ขับเคลื่อนด้วยข้อมูล ผู้พัฒนาและนำเสนอผลิตภัณฑ์ซอฟต์แวร์ที่มีความสำคัญและจำเป็น เครื่องมือรักษาความปลอดภัย อุปกรณ์สื่อสาร เซิร์ฟเวอร์ และคอมพิวเตอร์ ซึ่งเป็น

¹ บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอรวมถึง Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatca, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation และ Workday

² ตลอดกว่า 30 ปีที่ผ่านมา สมาชิกรัฐสภาสหรัฐอเมริกา-อาเซียนเป็นองค์กรชั้นนำที่ทำหน้าที่เป็นผู้แทนของบริษัทสหรัฐที่ดำเนินกิจการอยู่ในกลุ่มประเทศอาเซียนซึ่งเป็นประชาคมที่เติบโตขึ้นอย่างต่อเนื่อง สมาชิกของสมาชิกรัฐฯ กว่า 150 ราย มีรายได้โดยรวมถึงกว่า 6 ล้านล้านดอลลาร์สหรัฐ และมีพนักงานกว่า 13 ล้านคนในทั่วโลก สมาชิกของสมาชิกรัฐฯ ล้วนเป็นบริษัทสหรัฐขนาดใหญ่ที่สุดที่ดำเนินกิจการอยู่ในกลุ่มประเทศอาเซียน ซึ่งมีตั้งแต่บริษัทที่เพิ่งเข้ามายังภูมิภาคนี้ไปจนถึงบริษัทที่ดำเนินกิจการอยู่ในเอเชียตะวันออกเฉียงใต้เป็นเวลากว่า 100 ปีมาแล้ว สมาชิกรัฐฯ มีสำนักงานอยู่ที่กรุงวอชิงตัน ดี.ซี., เมื่อนิวยอร์ก รัฐนิวยอร์ก, กรุงเทพมหานคร ประเทศไทย, กรุงฮานอย เวียดนาม, กรุงจาการ์ตา อินโดนีเซีย, กรุงกัวลาลัมเปอร์ มาเลเซีย, กรุงมะนิลา ฟิลิปปินส์ และสิงคโปร์

สิ่งที่ขับเคลื่อนเศรษฐกิจข้อมูลข่าวสารในทั่วโลกและทำให้มนุษย์มีความเป็นอยู่ในชีวิตประจำวันที่ดีขึ้น สมาชิกของเราได้รับความไว้วางใจจากลูกค้าในการจัดให้เทคโนโลยีรักษาความปลอดภัยที่สำคัญเพื่อปกป้องจากภัยคุกคามทางไซเบอร์ ภัยคุกคามเหล่านี้อาจเกิดขึ้นจากผู้ประสงค์ร้ายที่มีวัตถุประสงค์แตกต่างกันไป ซึ่งรวมถึงผู้ที่ต้องการขโมยอัตลักษณ์ของเรา ทำร้ายบุคคลที่เรารัก เอาไปซึ่งความลับที่มีค่าในทางการค้า หรือเป็นภัยต่อความมั่นคงของชาติ

ด้วยเหตุที่เรียนมานี้ สมาชิกของเราจึงเป็นผู้มีส่วนได้เสียโดยตรงในการที่รัฐบาลไทยมีแผนจะเสนอร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (“ร่าง พ.ร.บ. ปี 2561”)

บีเอสเอและสภาธุรกิจฯ ได้ทำงานอย่างใกล้ชิดกับรัฐบาลในทั่วโลกในเรื่องเกี่ยวกับการพัฒนานโยบายและกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศต่างๆ อันทำให้เราได้ประจักษ์ถึงศักยภาพของนโยบายและกฎหมายดังกล่าวที่จะระงับยับยั้งและจัดการกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และสามารถปกป้องความเป็นส่วนตัวและเสรีภาพของประชาชนได้ในขณะเดียวกัน บีเอสเอได้นำประสบการณ์ดังกล่าวมาใช้ในการพัฒนากรอบนโยบายสากลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (“กรอบนโยบายสากล”) เพื่อเป็นแนวทางสำหรับจัดทำนโยบายระดับประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมเนื้อหาอย่างครบถ้วน ซึ่งสภาธุรกิจฯ ก็ได้ให้การสนับสนุนกรอบนโยบายสากลดังกล่าวอย่างเต็มที่ รายละเอียดของกรอบนโยบายสากลดังกล่าวปรากฏตามสำเนาที่แนบมาพร้อมนี้

กล่าวโดยสรุป กรอบนโยบายสากลดังกล่าวนำเสนอหลักการ 6 ข้อ เพื่อใช้เป็นแนวทางในการจัดทำนโยบายระดับประเทศในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ กล่าวคือ นโยบายในเรื่องดังกล่าวควรมีลักษณะดังนี้

1. สอดคล้องกับมาตรฐานซึ่งเป็นที่ยอมรับในระดับสากล
2. คำนี้ถึงเรื่องความเสี่ยงเป็นหลัก มุ่งเน้นที่ผล และเป็นกลางทางเทคโนโลยี
3. อาศัยกลไกที่ขับเคลื่อนด้วยการตลาดหากสามารถกระทำได้
4. มีความยืดหยุ่นและสนับสนุนให้มีการพัฒนาวัตกรรม
5. ส่งเสริมให้มีการประสานความร่วมมือระหว่างภาครัฐและเอกชน และ
6. มุ่งปกป้องความเป็นส่วนตัว

2. ความเห็นของภาคอุตสาหกรรม

บีเอสเอได้เรียนเสนอความเห็นต่อร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับปี พ.ศ. 2558 ที่ออกโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งประเทศไทย (“ร่าง พ.ร.บ. ปี 2558”) รายละเอียดปรากฏตามสำเนาหนังสือแสดงความเห็นของบีเอสเอในภาคผนวกของหนังสือฉบับนี้

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้สำหรับความพยายามครั้งสำคัญที่ดำเนินการเพื่อให้แน่ใจว่าประเทศไทยมีความพร้อมที่จะระงับยับยั้งและจัดการกับภัยคุกคามไซเบอร์ เนื่องจากภัยคุกคามไซเบอร์มีความซับซ้อนและมีอันตรายขึ้นทุกวัน ความเสี่ยงที่เกิดจากนโยบายระดับประเทศที่กำหนดขึ้นอย่างไม่เพียงพอหรือไม่มีประสิทธิภาพในการรับมือกับภัยคุกคามไซเบอร์จึงอาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

ภัยคุกคามไซเบอร์โดยลักษณะแล้วเป็นเรื่องระดับโลก ดังนั้น การรับมือกับภัยคุกคามทางไซเบอร์จึงจำเป็นต้องดำเนินการในระดับโลกเช่นกัน บีเอสเอและสภาธุรกิจ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและรัฐบาลไทยที่เปิดรับฟังความคิดเห็นจากภาคเอกชนและผู้มีส่วนได้เสียอื่น ๆ ในการจัดทำกฎหมายนี้ และขอสนับสนุนให้ยังคงมีการเปิดโอกาสให้มีการสื่อสารและหารือกับภาคเอกชนต่อไป ซึ่งรวมถึงบริษัทระดับโลก ด้วยเหตุนี้ ทางบีเอสเอและสภาธุรกิจ จึงขอเรียนเสนอให้กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ระบุให้ชัดเจนว่า บทบัญญัติที่กล่าวถึงการประสานความร่วมมือระหว่างภาครัฐและเอกชนนั้น (เช่น ตามมาตรา 5(4) และ มาตรา 7(5) เป็นต้น) เป็นการอนุญาตและส่งเสริมให้มีการประสานความร่วมมือกับเอกชนที่เป็นบริษัทที่ประกอบธุรกิจในหลายประเทศด้วย

บีเอสเอและสภาธุรกิจ ทราบดีและซาบซึ้งในความพยายามที่จะแก้ไขปัญหาของร่าง พ.ร.บ. ปี 2558 ตามที่ได้มีการเสนอความเห็นไว้ อย่างไรก็ตาม ปัญหาส่วนใหญ่ของร่าง พ.ร.บ. ปี 2558 ก็ยังคงปรากฏอยู่ในร่าง พ.ร.บ. ปี 2561 นี้ บีเอสเอจึงขอเรียนเสนอความเห็นต่อไปนี้ด้วยเจตนาที่จะมีส่วนช่วยให้ร่างกฎหมายดังกล่าวบรรลุตามเจตนารมณ์อันดีที่จะกำหนดให้มี “การดำเนินการที่ทันท่วงทีและเป็นไปในทิศทางเดียวกัน” ต่อภัยคุกคามทางไซเบอร์ โดยไม่ก่อให้เกิดผลอันไม่พึงประสงค์

เอ. กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ในหนังสือเสนอความเห็นของบีเอสเอต่อร่าง พ.ร.บ. ปี 2558 บีเอสเอได้เน้นในประเด็นที่ว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) ควรประกอบด้วยกรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดินด้วย เพื่อให้มีมุมมองที่รอบด้านขึ้นจากมุมมองของกรรมการของ กปช. ที่มาจากหน่วยงานด้านการรักษาความมั่นคงปลอดภัยและความมั่นคง ทั้งนี้ เพื่อให้แน่ใจว่า ในการจัดทำกลยุทธ์หรือแผนรับมือด้านความมั่นคงปลอดภัยไซเบอร์ กปช. จะพิจารณาประเด็นเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชนในทุกมิติ

บีเอสเอและสภาธุรกิจ ทราบดีว่ามาตรา 6 แห่งร่าง พ.ร.บ. ปี 2561 ได้กำหนดให้กรรมการใน กปช. มาจากหลากหลายหน่วยงานมากขึ้น โดยมีผู้แทนจากหลายกระทรวง รวมถึงกระทรวงคมนาคม กระทรวงศึกษาธิการ และกระทรวงสาธารณสุข ซึ่งย่อมทำให้ได้มุมมองที่หลากหลายและสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผ่านการพิจารณาอย่างรอบด้านเพื่อเสนอต่อคณะรัฐมนตรีได้ อย่างไรก็ตาม เนื่องจาก กปช. ไม่มีกรรมการที่จะดูแลรักษาผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชน มุมมองของ กปช. จึงยังคงเน้นไปที่ประเด็นเรื่องการบังคับใช้กฎหมายและความมั่นคง โดยมีรัฐมนตรีว่าการกระทรวงกลาโหมเป็นรองประธาน กปช.

บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า คณะทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่ควรนำโดยรัฐมนตรีว่าการกระทรวงกลาโหมแต่เพียงผู้เดียว แต่ควรให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีส่วนร่วมในการนำคณะทำงานดังกล่าวด้วย เนื่องจากภัยคุกคามทางไซเบอร์อาจส่งผลกระทบต่อผลประโยชน์ทางด้านเศรษฐกิจทั้งในระดับชาติและระดับนานาชาติได้ในวงกว้าง กปช. จึงควรมีกรรมการที่จะดูแลรักษาผลประโยชน์ของประชาชนอยู่ด้วย

บี. การมีอำนาจอย่างกว้างขวางของ กปช.

ตามมาตรา 14 แห่งร่าง พ.ร.บ. ปี 2561 กปช. มีอำนาจหน้าที่เป็นศูนย์กลางในการประสานงานระหว่างหน่วยงานเพื่อรับมือกับภัยคุกคามไซเบอร์และสถานการณ์ด้านภัยคุกคามไซเบอร์ บีเอสเอและสภาธุรกิจ ยังคงเห็นด้วยในเรื่องนี้ การกำหนดให้มีหน่วยงานระดับประเทศเพียงหน่วยงานเดียวทำหน้าที่เป็นหน่วยงานหลักที่มีความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะทำให้เกิดความชัดเจน มีความสอดคล้อง และเป็นไปในทิศทางเดียวกันในการเตรียมความพร้อมของรัฐบาลในการรับมือกับภัยคุกคามและปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ในฐานะที่ กปช. เป็นศูนย์กลางในการประสานงานดังกล่าว กปช. จึงมีอำนาจอย่างกว้างขวางในการจัดการกับภัยคุกคามไซเบอร์ที่กฎหมายนี้กำหนดให้ต้องมีการดำเนินการอย่างหนึ่งอย่างใด ตัวอย่างเช่น ตามมาตรา 36 และมาตรา 37 แห่งร่าง พ.ร.บ. ปี 2561 กปช. มีอำนาจสั่งการให้หน่วยงานเอกชน³ดำเนินการอย่างหนึ่งอย่างใดเมื่อมีเหตุฉุกเฉินหรือภัยอันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ บีเอสเอและสภาธุรกิจ ตระหนักว่าได้มีความพยายามที่จะระบุให้ชัดเจนขึ้นว่า อำนาจเหล่านี้จะมีขึ้นเฉพาะในกรณีที่ “การให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ” ได้รับผลกระทบเท่านั้น ซึ่งสอดคล้องกับความเห็นที่บีเอสเอได้ให้ไว้สำหรับร่าง พ.ร.บ. ปี 2558 อย่างไรก็ดี หลักเกณฑ์และกรณีที่ กปช. อาจใช้อำนาจตามมาตราเหล่านี้ได้ก็ยังไม่ได้มีการบัญญัติไว้อย่างชัดเจน

- **อำนาจของ กปช. ควรจำกัดให้มีเฉพาะในกรณีที่ “โครงสร้างพื้นฐานที่สำคัญ” ได้รับผลกระทบ** หลายประเทศได้นำเรื่อง “โครงสร้างพื้นฐานที่สำคัญ” มาใช้ในกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นกรณีที่ยอมรับได้ว่าหน่วยงานผู้บังคับใช้กฎหมายจะมีอำนาจอย่างกว้างขวางดังเช่นที่ปรากฏในร่าง พ.ร.บ. ปี 2561 ดังนั้น เพื่อให้สอดคล้องกับกฎหมายที่ใช้ในทั่วโลก บีเอสเอและสภาธุรกิจ ขอเรียนเสนอคำจำกัดความดังนี้
 - **โครงสร้างพื้นฐานที่สำคัญ** หมายความว่า “ทรัพย์สิน บริการ และระบบ ไม่ว่าจะจับต้องได้หรือเสมือนจริง ที่หากถูกทำลาย ถูกทำให้เสียหาย หรือไม่สามารใช้การได้เป็นระยะเวลาหนึ่งแล้ว จะส่งผลกระทบในวงกว้างต่อความมั่นคงของชาติ สาธารณสุข ความปลอดภัยของประชาชน ความมั่นคงด้านเศรษฐกิจของชาติ หรือการปฏิบัติงานหลักของหน่วยงานในระดับท้องถิ่นหรือระดับชาติ”

ในการกำหนดว่าโครงสร้างใดเป็นโครงสร้างพื้นฐานที่สำคัญ บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า กปช. ควรพิจารณาจากความสำคัญ ความจำเป็น และความเสี่ยงที่เกี่ยวข้อง

³ “หน่วยงานเอกชน” เป็นคำที่เพิ่มคำจำกัดความเข้ามาใหม่ในมาตรา 3 ซึ่งหมายความว่า “หน่วยงานที่จัดตั้งขึ้นจากการรวมตัวของบุคคล หรือคณะบุคคลเข้าด้วยกัน ไม่ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือไม่แสวงหากำไร ทั้งนี้ ไม่ว่าจะจดทะเบียนเป็นนิติบุคคลหรือไม่ก็ตาม”

- การให้อำนาจที่กว้างขวางตามมาตรา 36 และมาตรา 37 ควรจำกัดเฉพาะในกรณี “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” ในเรื่องนี้ควรต้องให้คำจำกัดความทั้งคำว่า “เหตุภัยคุกคามทางไซเบอร์” และ “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” ดังนั้น เพื่อให้สอดคล้องกับกรอบนโยบายสากล บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอคำจำกัดความดังนี้
 - “เหตุภัยคุกคามทางไซเบอร์” หมายความว่า “เหตุการณ์ที่ระบุได้ ไม่ว่าจะเกิดขึ้นเพียงครั้งเดียวหรือหลายครั้ง ต่อระบบ บริการ หรือเครือข่าย ซึ่งแสดงให้เห็นได้ว่าอาจมีการกระทำอันเป็นการฝ่าฝืนนโยบายด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ หรือมีความบกพร่องในการรักษาความมั่นคงปลอดภัย หรือสถานการณ์ที่อาจมีความเกี่ยวข้องกับความปลอดภัยของระบบ บริการ หรือเครือข่าย ที่เกิดขึ้นมาก่อนหน้านี้แต่ไม่ทราบมาก่อน”
 - “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” หมายความว่า “เหตุภัยคุกคามทางไซเบอร์ที่ทำให้ (1) มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือมีการถูกปฏิเสธไม่ให้เข้าถึงข้อมูล หรือมีการทำลาย ลบ ปรับเปลี่ยน หรือระงับข้อมูลที่จำเป็นต่อการทำงานของโครงสร้างพื้นฐานที่สำคัญ หรือ (2) การควบคุมการปฏิบัติการหรือการควบคุมทางเทคนิคที่จำเป็นต่อความปลอดภัยหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญถูกโจมตี

ซี. การรายงานเหตุภัยคุกคามทางไซเบอร์

บีเอสเอและสภาธุรกิจฯ มีความกังวลว่า บทบัญญัติที่กำหนดให้หน่วยงานเอกชนรายงานไปยังเลขาธิการกรณีเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ตามมาตรา 35 นั้นอาจจะกว้างเกินไป การกำหนดเงื่อนไขของการรายงานที่กว้างเกินไปนั้นอาจกลับทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์กระทำได้ยากขึ้น เนื่องจากจะทำให้บริษัทต่างๆ รายงานเหตุที่เกิดขึ้นกับระบบของตนบ่อยครั้งเกินไป อันทำให้ความใส่ใจต่อการรายงานลดหายไป อีกทั้งทำให้มีค่าใช้จ่ายสูงขึ้น การปฏิบัติงานถูกรบกวน และยากที่จะระบุว่าเหตุภัยคุกคามใดที่มีความสำคัญที่สุดและควรดำเนินการอย่างไร ดังนั้น บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอให้การรายงานต้องกระทำเฉพาะในกรณีของ “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” ที่ส่งผลกระทบต่อ “โครงสร้างพื้นฐานที่สำคัญ” เท่านั้น ตามที่เรียนไว้ข้างต้น

ดี. อำนาจในการสอดส่องดูแล

บีเอสเอและสภาธุรกิจฯ ทราบว่า ร่าง พ.ร.บ. ปี 2561 นั้นได้มีการแก้ไขปรับเปลี่ยนตามที่บีเอสเอได้เรียนเสนอไว้ในครั้งก่อนเกี่ยวกับอำนาจหน้าที่ของเลขาธิการในการสอดส่องดูแลตามร่าง พ.ร.บ. ปี 2558 แล้ว กล่าวคือ มาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 กำหนดว่า เลขาธิการอาจเข้าถึงข้อมูลการติดต่อสื่อสารของหน่วยงานเอกชนได้ต่อเมื่อมีคำสั่งศาลอนุญาตให้ปฏิบัติการดังกล่าว เว้นแต่ “ในกรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง” ซึ่งกฎหมายได้อนุญาตให้เลขาธิการเข้าถึงข้อมูลการติดต่อสื่อสารไปก่อน แล้วจึงรายงานให้ศาลทราบโดยเร็ว บีเอสเอและสภาธุรกิจฯ ขอเรียนว่า ข้อยกเว้นที่บัญญัติไว้อย่างกว้างดังกล่าวนี้อาจก่อให้เกิดความไม่ชัดเจนในทางปฏิบัติ ซึ่งอาจทำให้ความเชื่อมั่นของผู้บริโภคที่ว่าโดยทั่วไปแล้วบริษัทต่างๆ จะสามารถรับรองได้ว่าข้อมูลส่วนบุคคลหรือข้อมูลลับของ

ผู้ใช้บริการจะได้รับการป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาตนั้นต้องถูกลดทอนลงไป ในเรื่องนี้ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอแนวทางแก้ปัญหาดังนี้

- **ควรกำหนดให้คำสั่งศาลมีผลเพียงช่วงระยะเวลาหนึ่ง** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่าคำสั่งศาลไม่ควรจะมีผลบังคับโดยไม่จำกัดระยะเวลา เนื่องจากอาจก่อให้เกิดความไม่ชัดเจนต่อหน่วยงานเอกชน
- **ข้อยกเว้นของการขอคำสั่งศาลควรใช้ถ้อยคำที่ชัดเจน** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่ากรณี “จำเป็นเร่งด่วน” ที่เป็นข้อยกเว้นดังกล่าวนั้นควรระบุให้ชัดเจนว่าต้องเป็นกรณีที่เกิดจากความเสียหายต่อความมั่นคงของชาติเท่านั้น
- **ควรกำหนดให้มีหน่วยงานอิสระควบคุมดูแลการใช้อำนาจของ กปช. ตามมาตรา 47** บีเอสเอและสภาธุรกิจฯ ขอเรียนย้ำว่า หน่วยงานอิสระ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เสนอให้มีการแต่งตั้งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ควรมีอำนาจในการตรวจสอบดูแลการใช้อำนาจของ กปช. ตามมาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 เพื่อให้แน่ใจว่ามีการถ่วงดุลระหว่างผลประโยชน์ของเอกชนกับความจำเป็นในการใช้อำนาจสอดส่องดูแล

อี. ความรับผิดชอบทางอาญา

มาตรา 53 ถึงมาตรา 56 แห่งร่าง พ.ร.บ. ปี 2561 ได้กำหนดโทษทางอาญาสำหรับการกระทำที่ฝ่าฝืนร่าง พ.ร.บ. ปี 2561 ในเรื่องนี้ บีเอสเอและสภาธุรกิจฯ เห็นว่า การดำเนินคดีอาญาควรจำกัดเฉพาะในกรณีที่ผู้กระทำความผิดก่อความเสียหาย หรือก่อให้เกิดปัญหาต่อโลกไซเบอร์ด้วยเจตนาทุจริตเท่านั้น

บีเอสเอและสภาธุรกิจฯ เห็นว่า การกำหนดโทษทางอาญาต่อหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำขอของ กปช. ตามมาตรา 47 นั้นเป็นบทลงโทษที่รุนแรงเกินควร อันอาจทำให้บริษัทต่างชาติระงับแผนที่จะเข้ามาประกอบธุรกิจในประเทศไทยหากมีความเสี่ยงว่าบุคลากรของตนจะต้องมีความรับผิดชอบทางอาญาสำหรับการกระทำความผิดโดยไม่ตั้งใจหรือการกระทำความผิดเพียงเล็กน้อย

เอฟ. แง่มุมอื่น ๆ ของนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

นอกจากนี้ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยควรครอบคลุมประเด็นที่สำคัญอื่นๆ ด้วย เช่น การปฏิบัติตามแนวทางในการจัดซื้อเทคโนโลยีและซอฟต์แวร์ของภาครัฐ การให้การสนับสนุนจากรัฐบาลอย่างเต็มที่ในด้านการวิจัยและพัฒนาเทคโนโลยีสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ โครงการให้ความรู้เพื่อเพิ่มความตระหนักรู้ การฝึกอบรม และการจัดทำนโยบายต่างประเทศให้ครอบคลุมถึงเรื่องการประสานความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์ บีเอสเอและสภาธุรกิจฯ ขอสนับสนุนให้รัฐบาลไทยพิจารณาเพิ่มเติมประเด็นที่สำคัญเหล่านี้ไว้ในร่าง พ.ร.บ. ปี 2561 และขอเรียนเสนอกรอบนโยบายสากลและแบ่งปันประสบการณ์ในการดำเนินการในระดับสากลของเราในด้านนี้เพื่อเป็นแนวทางในการจัดทำนโยบายที่เกี่ยวข้องต่อไป

3. บทสรุปและการดำเนินการขั้นต่อไป

บีเอสเอและสมาชิกรักใจ ขอแสดงความชื่นชมรัฐบาลไทยอีกครั้งสำหรับความพยายามในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ตาม บีเอสเอและสมาชิกรักใจ ใคร่ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาประเด็นที่ได้เรียนเสนอไว้ข้างต้น เพื่อที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจะสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งคำนึงถึงเรื่องความเสี่ยงเป็นหลักและสอดคล้องกับแนวปฏิบัติในระดับสากล อันจะช่วยเสริมสร้างความเชื่อมั่นระหว่างภาครัฐและเอกชน และยกระดับความมั่นคงปลอดภัยของข้อมูลและโครงสร้างพื้นฐาน

บีเอสเอและสมาชิกรักใจ ยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อโดยตรงไปที่ afeldman@usasean.org หรือที่หมายเลข 202-375-4393 หรือที่ jaredr@bsa.org หรือที่หมายเลข +65 6292 9609 หรือติดต่อนางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่ varuneer@bsa.org หรือที่หมายเลข +668-1840-0591 หรือนางสาวเอลล่า ดวงแก้ว ผู้จัดการประจำประเทศไทยแห่งสมาชิกรักใจสหรัฐอเมริกา-เอเชีย ณ eduangkaew@usasean.org หรือที่หมายเลข 202-440-3642 บีเอสเอและสมาชิกรักใจ ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

อเล็กซานเดอร์ ซี. เฟลด์แมน
ประธานและประธานเจ้าหน้าที่บริหาร
สมาชิกรักใจสหรัฐอเมริกา-เอเชีย

(ลายมือชื่อ)

เจเร็ด แร็กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย ภูมิภาคเอเชีย
แปซิฟิก
บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง

1. ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ภาคผนวก บี

ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคง
ปลอดภัยไซเบอร์
(21 พฤษภาคม 2561)

(กระตาดหัวจดหมายของบีเอสเอ)

(สภาธุรกิจสหรัฐอเมริกา-อาเซียน)

วันที่ 21 พฤษภาคม 2561

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

ปลัดกระทรวง

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

120 หมู่ที่ 3 ชั้น 6-9

ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550

ถนนแจ้งวัฒนะ

ทุ่งสองห้อง หลักสี่ กรุงเทพมหานคร 10210

เรื่อง ความเห็นเพิ่มเติมของภาคอุตสาหกรรมในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านปลัดกระทรวง

ตามที่ บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (“บีเอสเอ”) และสภาธุรกิจสหรัฐอเมริกา-อาเซียน (“สภาธุรกิจ”) ได้เรียนเสนอความเห็นในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามหนังสือลงวันที่ 17 เมษายน 2561 ที่ผ่านมา (สำเนาหนังสือปรากฏอยู่ในภาคผนวก บี ของหนังสือฉบับนี้) นั้น

จากการศึกษาร่าง พ.ร.บ. ปี 2561 และการหารือกับกลุ่มสมาชิกเพิ่มเติม บีเอสเอและสภาธุรกิจ ขอเรียนเสนอความเห็นเพิ่มเติมจากความเห็นที่อ้างถึงข้างต้นมาตามภาคผนวก เอ ของหนังสือฉบับนี้ ซึ่งมีเนื้อหาโดยสรุปดังปรากฏด้านล่างนี้ บีเอสเอและสภาธุรกิจ ใ้ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาความเห็นเพิ่มเติมดังกล่าวประกอบกับความเห็นที่ได้เรียนเสนอไว้เมื่อครั้งก่อนด้วยจักเป็นพระคุณยิ่ง

เนื้อหาของความเห็นเพิ่มเติมจากความเห็นตามหนังสือฉบับลงวันที่ 17 เมษายน 2561 สามารถกล่าวโดยสรุปได้ดังนี้

- การกำหนดให้มีกรรมการที่เป็นผู้แทนจากภาคอุตสาหกรรมจะเป็นประโยชน์ต่อคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”)
- ร่าง พ.ร.บ. ปี 2561 ควรใช้บังคับกับ “หน่วยงานเอกชน” ที่จัดตั้งขึ้นในประเทศไทยและเป็นผู้ประกอบกิจการหรือเป็นผู้ควบคุมโครงสร้างพื้นฐานที่สำคัญ (ตามคำจำกัดความที่ได้เรียน

เสนอไว้ในหนังสือฉบับวันที่ 17 เมษายน 2561) เท่านั้น และควรกำหนดหน้าที่ให้กับหน่วยงาน เอกชนดังกล่าวไว้อย่างชัดเจน โดยจำกัดเฉพาะแต่เพียงหน้าที่ที่มีความเหมาะสมและสามารถปฏิบัติ ได้จริง

- หน้าที่ในการรายงานควรจำกัดเฉพาะกรณีเหตุภัยคุกคามทางไซเบอร์ที่สำคัญซึ่งได้เกิดขึ้นแล้ว เท่านั้น โดยไม่รวมถึงเหตุภัยคุกคามทางไซเบอร์ที่ไม่มีความสำคัญ หรือเหตุภัยคุกคามทางไซเบอร์ที่ “คาด”ว่าจะเกิดขึ้น
- การใช้อำนาจในการเข้าถึงข้อมูลและเครื่องมือควรเป็นไปอย่างได้สัดส่วนและมีมาตรการตรวจสอบ และถ่วงดุลที่เหมาะสม ซึ่งรวมถึงการตรวจสอบความชอบด้วยกฎหมายโดยศาลและสิทธิใน การโต้แย้งหรืออุทธรณ์คำสั่ง
- ควรมีหน่วยงานกำกับดูแลเพียงหน่วยงานเดียวที่มีอำนาจหน้าที่ในการตรวจสอบดูแลและบังคับใช้ กฎหมายตามร่าง พ.ร.บ. ปี 2561
- ร่าง พ.ร.บ. ปี 2561 ควรบัญญัติในเรื่องการรักษาความลับและการคุ้มครองความเป็นส่วนตัว อย่างเป็นชัดเจนด้วย
- ร่าง พ.ร.บ. ปี 2561 ควรส่งเสริมให้มีการแบ่งปันข้อมูลข่าวสาร ซึ่งรวมถึงโดยการจำกัดความรับผิดชอบ ที่เกิดขึ้นจากการแบ่งปันข้อมูลข่าวสารไว้อย่างเหมาะสม

บีเอสเอและสภาธุรกิจ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาใน โอกาสนี้ที่ได้เปิดรับฟังความคิดเห็นจากภาคเอกชนและผู้มีส่วนได้เสียอื่นๆ ในการจัดทำกฎหมายนี้ และ ขอสนับสนุนให้ยังคงมีการเปิดโอกาสให้มีการสื่อสารและหารือกับภาคเอกชนต่อไป โดยเฉพาะอย่างยิ่ง ใน การจัดทำระเบียบและประกาศต่างๆ หรือข้อกำหนดเพิ่มเติมใดๆ ที่ออกตามร่าง พ.ร.บ. ปี 2561 นี้ ควรมี ขั้นตอนการหารือกับภาคเอกชนเช่นกัน เพื่อให้เกิดความชัดเจนและความสอดคล้องกัน

บีเอสเอและสภาธุรกิจ ยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อเช่นเคย หากท่านมีข้อสงสัยหรือ ความเห็นประการใด กรุณาติดต่อโดยตรงไปที่ afeldman@usasean.org หรือที่หมายเลข 202-375-4393 หรือที่ jaredr@bsa.org หรือที่หมายเลข +65-6292-9609 หรือติดต่อนางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่ varuneer@bsa.org หรือที่หมายเลข +668-1840-0591 หรือนางสาวเอลล่า ดวงแก้ว ผู้จัดการประจำประเทศไทยแห่งสภาธุรกิจสหรัฐอเมริกา-อาเซียน ที่ eduangkaew@usasean.org หรือที่หมายเลข 202-440-3642

บีเอสเอและสภาธุรกิจ ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

อเล็กซานเดอร์ ซี. เฟลด์แมน
ประธานและประธานเจ้าหน้าที่บริหาร
ภูมิภาคเอเชีย
สภาธุรกิจสหรัฐอเมริกา-อาเซียน

(ลายมือชื่อ)

จาเร็ด แร็กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย
ภูมิภาคเอเชีย แปซิฟิก
บีเอสเอ | พันธมิตรธุรกิจซอฟต์แวร์

สำเนาถึง

1. ดร.พิเชฐ ตูรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ภาคผนวก เอ – ความเห็นเพิ่มเติมเกี่ยวกับร่าง พ.ร.บ. ปี 2561

บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอความเห็นเพิ่มเติมเกี่ยวกับร่าง พ.ร.บ. ปี 2561 ตามที่ปรากฏในตารางด้านล่างนี้ เพื่อประกอบความเห็นที่ได้เรียนเสนอไว้ก่อนหน้านี้ ตามหนังสือลงวันที่ 17 เมษายน 2561 (ภาคผนวก บี)

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจฯ |
|---|---|---|---|
| เอ. กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | | | |
| 1. | กรรมการใน กปช. (มาตรา 6) | แม้ร่าง พ.ร.บ. ปี 2561 จะได้มีการกำหนดให้แต่งตั้ง กรรมการจากหน่วยงานที่หลากหลายมากขึ้นแล้ว แต่ ยังไม่มีกรรมการรายใดที่เป็นผู้แทนจาก ภาคอุตสาหกรรม | จากความเห็นที่ได้เรียนเสนอไว้ในครั้งก่อนว่า กปช. ควรประกอบด้วย กรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงาน ผู้ตรวจการแผ่นดินด้วยนั้น บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอเพิ่มเติมว่า กปช. ควรประกอบด้วยกรรมการที่มาจากภาคอุตสาหกรรมด้วย ซึ่งไม่ เพียงแต่จะช่วยให้คณะกรรมการมีมุมมองที่รอบด้านมากขึ้นเท่านั้น แต่ ยังช่วยเสริมสร้างการประสานความร่วมมือระหว่างภาครัฐและเอกชน อันจะ นำไปสู่การปฏิบัติที่ก่อให้เกิดประสิทธิภาพสูงสุดด้วย |
| บี. อำนาจของ กปช. | | | |
| 2. | คำจำกัดความ ของ “หน่วยงาน เอกชน” และ ความจำเป็นใน การกำหนด หลักเกณฑ์ที่ เหมาะสม | ร่าง พ.ร.บ. ปี 2561 ประสงค์จะกำกับดูแล “หน่วยงานเอกชน” ซึ่งได้แก่หน่วยงานที่จัดตั้งขึ้น ไม่ ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือไม่แสวงหากำไร ทั้งนี้ ไม่ว่าจะจดทะเบียนเป็นนิติบุคคล หรือไม่ก็ตาม คำจำกัดความของ “หน่วยงานเอกชน” ดังกล่าวนี้อาจกว้างเกินไปสำหรับเรื่องการรักษา ความมั่นคงปลอดภัยทางไซเบอร์ และควรกำหนดให้ แคบลงกว่านี้ | บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ในกฎหมายนี้ คำจำกัดความของ “หน่วยงานเอกชน” ควรจำกัดอยู่ที่บริษัทที่จัดตั้งขึ้นในประเทศไทยซึ่งเป็นผู้ ประกอบกิจการหรือเป็นผู้ควบคุม “โครงสร้างพื้นฐานที่สำคัญ” (ตามคำจำกัด ความที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) ในประเทศไทยเท่านั้น |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|-----|--|--|---|
| | (มาตรา 3, 36 และ 37) | | |
| 3. | <p>หน้าที่ในการบังคับบัญชาและสั่งการให้หน่วยงานต่าง ๆ ปฏิบัติงาน (มาตรา 33, 34, 36 และ 37)</p> | <ul style="list-style-type: none"> อำนาจของ กปช. ในการบังคับบัญชาและสั่งการหน่วยงานเอกชนตามมาตรา 33 และในการสั่งการให้หน่วยงานเอกชน “กระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง” ตามมาตรา 37 มีข้อจำกัดอยู่เพียงเล็กน้อย ตามมาตรา 34 กปช. มีดุลพินิจอย่างกว้างขวางในการมีมติว่าหน่วยงานเอกชนไม่ปฏิบัติตามพระราชบัญญัตินี้ หรือปฏิบัติการโดยขัดหรือแย้งกับแนวทางที่กำหนด หรือในการแจ้งให้แก้ไขยกเลิก หรือยุติการดำเนินการดังกล่าว ซึ่งหากไม่ดำเนินการภายในเวลาที่กำหนด คณะรัฐมนตรีจะเป็นผู้พิจารณาสั่งการต่อไปตามดุลพินิจที่มีอย่างกว้างขวาง บทบัญญัติในมาตรา 36 และมาตรา 37 ใช้ถ้อยคำที่กว้างเกินไปโดยบังคับใช้กับหน่วยงานเอกชนทั้งหมด แม้กระทั่งหน่วยงานที่ไม่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ | <ul style="list-style-type: none"> ควรกำหนดและจำกัดอำนาจที่ให้แก่ กปช. และหน่วยงานที่ได้รับแต่งตั้งให้มีความชัดเจนยิ่งขึ้น รวมถึงให้มีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาล อีกทั้งหน่วยงานเอกชนและบุคคลภายนอกควรมีโอกาสอย่างเต็มที่ในการโต้แย้งคำสั่งและยื่นอุทธรณ์ต่อศาลหากไม่เห็นพ้องด้วยกับคำวินิจฉัย บีเอสเอและสภาธุรกิจ ทราบว่าตาม ร่าง พ.ร.บ. ปี 2561 นั้น จำเป็นต้องขอคำสั่งศาลก่อนใช้อำนาจบางประการ (เว้นแต่กรณีจำเป็นเร่งด่วน) อย่างไรก็ดี บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า การใช้อำนาจของ กปช. ควรต้องมีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาลในหลายกรณีมากขึ้น เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับ “หน่วยงานเอกชน” มาตรา 34 ควรแก้ไขให้มีการระบุให้ชัดเจนว่า กปช. มีอำนาจบังคับบัญชาหรือสั่งการหน่วยงานเอกชนให้ดำเนินการอย่างไรได้บ้าง ทั้งนี้ เพื่อให้ได้มีหลักเกณฑ์ที่ชัดเจน เพื่อให้ทุกฝ่ายมีความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง อันจะนำไปสู่ความชัดเจนในเรื่องการรักษาความมั่นคงไซเบอร์ในประเทศไทย บีเอสเอและสภาธุรกิจ มีความกังวลว่า ตามร่าง พ.ร.บ. ปี 2561 (รวมถึงหน้าที่ตามมาตรา 36 และมาตรา 37 เป็นต้น) หน่วยงานเอกชนมีหน้าที่ต้องดำเนินการบางประการในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ที่อาจ |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|--|--------------------------------------|---|--|
| | | | <p>ไม่ได้อยู่ภายใต้การควบคุมของหน่วยงานเอกชนนั้นแต่อย่างใด หรืออาจมีความไม่สมเหตุสมผล ไม่สามารถปฏิบัติได้จริง หรือไม่ได้สัดส่วนแก่กรณีด้วยเหตุนี้ บีเอสเอและสภาธุรกิจ จึงขอเรียนเสนอว่า ในร่าง พ.ร.บ. ปี 2561 ทั้งฉบับ (ไม่เพียงแต่เฉพาะบางมาตรา) การกำหนดหน้าที่แก่หน่วยงานเอกชนควรต้องจำกัดเฉพาะแต่เพียงหน้าที่ที่มีความเหมาะสม และสามารถนำไปปฏิบัติได้จริงเท่านั้น</p> <ul style="list-style-type: none"> • สำหรับมาตรา 36 และมาตรา 37 นอกเหนือจากความเห็นที่ได้เรียนเสนอไว้ก่อนหน้าที่ว่าควรใช้หลักเกณฑ์ในเรื่องเหตุภัยคุกคามทางไซเบอร์ที่สำคัญแล้ว บีเอสเอและสภาธุรกิจ มีความเห็นว่า ทั้งสองมาตรานี้ควรใช้บังคับเฉพาะกับหน่วยงานที่ได้รับผลกระทบโดยตรงจาก "เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ" (ตามคำจำกัดความที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) เท่านั้น เพื่อที่จะได้หลีกเลี่ยงไม่ให้ความได้ว่าหน่วยงานเอกชนที่ไม่ได้รับผลกระทบจะต้องมีหน้าที่ตามมาตรานี้ |
| ซี. หน้าที่ในการรายงานเหตุภัยคุกคามทางไซเบอร์ | | | |
| 4. | หน้าที่ในการรายงาน (มาตรา 35 และ 40) | มาตรา 35 กำหนดหน้าที่ในการรายงานทั้งในกรณีที่เกิดและคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ | <ul style="list-style-type: none"> • กฎหมายไม่ควรกำหนดให้มีหน้าที่ต้องรายงานทุกกรณีที่เกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ เนื่องจากประเภทของเหตุภัยคุกคามทางไซเบอร์และที่มาของเหตุดังกล่าวมีการเปลี่ยนแปลงอยู่ตลอดเวลา ด้วยเหตุนี้ บริการบางอย่างจึงอาจตกเป็นเป้าหมายของการโจมตีได้วันละหลายพันครั้ง (หรือกว่านั้น) ซึ่งส่วนใหญ่แล้วสามารถป้องกันได้สำเร็จ แม้ว่าจะองค์กรต่างๆ อาจจะมีมาตรการที่กำหนดขึ้นเพื่อป้องกันเหตุภัยคุกคามทางไซเบอร์โดยใช้วิธีการที่องค์กรต่างๆ ใช้กันอยู่ล่าสุด แต่การที่จะสามารถ |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|-----|--------|------------|--|
| | | | <p>ระบุเหตุภัยคุกคามได้ทุกครั้งหรือรายงานให้พนักงานเจ้าหน้าที่ทราบทุกครั้งที่คาดว่าจะเกิดเหตุภัยคุกคามก็เป็นเรื่องที่ย่อมเป็นไปได้ นอกจากนี้หน้าที่ดังกล่าวจะสร้างภาระอย่างยิ่ง ในขณะที่พนักงานเจ้าหน้าที่ไม่สามารถนำข้อมูลไปใช้ประโยชน์ได้เท่าใดนัก เนื่องจากต้องประมวลผลรายงานกรณีทีคาดว่าจะเกิดเหตุภัยคุกคามซึ่งมีจำนวนมหาศาล ซึ่งส่วนใหญ่แล้วไม่ได้เกิดขึ้นจริง (หรืออาจป้องกันได้สำเร็จหรือไม่มีความเสี่ยงว่าจะมีความเสียหายเกิดขึ้นจริง)</p> <ul style="list-style-type: none"> • บีเอสเอและสภาธุรกิจ ขอเรียนเสนอให้ใช้ถ้อยคำที่สอดคล้องกันตลอดทั้งฉบับ และกำหนดคำจำกัดความของ “เหตุภัยคุกคามทางไซเบอร์” และ “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” ให้ชัดเจน (ตามที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) • นอกจากนี้ บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า ควรกำหนดหน้าที่ในการรายงานเฉพาะในกรณีที่เข้า “หลักเกณฑ์ที่พิจารณาจากความสำคัญ” เช่น กรณีของเหตุภัยคุกคามทางไซเบอร์ที่สำคัญและมีความเสี่ยงอย่างแท้จริงว่าจะเกิดความเสียหายอย่างร้ายแรง • บีเอสเอและสภาธุรกิจ เชื่อว่า กฎหมายในเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ควรมีขึ้นเพื่อสร้างสภาพแวดล้อมที่เอื้อต่อการแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ มิใช่เพื่อบังคับให้รายงานทุกกรณีที่คาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ ความเห็นเรื่องนี้ในรายละเอียดปรากฏอยู่ในข้อ 8 ด้านล่าง |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|---|---|---|--|
| ดี. อำนาจหน้าที่ในการสอดส่องดูแล | | | |
| 5. | การเข้าถึงข้อมูลและเครื่องมือ (มาตรา 34, 36, 37, 43, 46 และ 47) | <ul style="list-style-type: none"> มาตรา 43 ใต้ให้อำนาจแก่เจ้าหน้าที่ของรัฐที่เกี่ยวข้องและสำนักงาน กปช. ในการขอให้มีการให้ข้อมูล สนับสนุนบุคลากร หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ของหน่วยงานเอกชน โดย กปช. ต้องขอให้ศาลมีคำสั่งหากหน่วยงานเอกชนไม่ยินยอมให้ข้อมูล ให้การสนับสนุนบุคลากร หรือจัดให้ใช้เครื่องมือทางอิเล็กทรอนิกส์ มาตรา 47 ให้อำนาจแก่เลขาธิการในการเรียกบุคคลมาให้ถ้อยคำ ส่งเอกสารหรือหลักฐาน หรือดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช. หรือเข้าถึงข้อมูลการติดต่อสื่อสาร (รวมถึงการติดต่อสื่อสารทางไปรษณีย์ โทรศัพท์ คอมพิวเตอร์ อุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศ) ตามที่เรียนไว้ในหนังสือฉบับก่อนหน้านี้ แม้จะกำหนดให้เลขาธิการต้องขอคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสาร แต่ “กรณีจำเป็นเร่งด่วน หากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง” ที่เป็นข้อยกเว้นนั้นก็มิขบเขตที่กว้าง นอกจากนี้ มาตรา 47 ใต้ให้อำนาจแก่ กปช. | <p>สำหรับมาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 บีเอสเอและสภาธุรกิจ ขอเรียนเสนอเพิ่มเติมดังนี้</p> <ul style="list-style-type: none"> การสั่งการ กำกับ หรือขอให้มีการให้ข้อมูลหรือการสนับสนุนใด ๆ ควรจำกัดเฉพาะในกรณีที่มีความเสี่ยงสูงที่จะเกิดความเสียหายอย่างร้ายแรง บีเอสเอและสภาธุรกิจ ขอเรียนว่า ความเสียหายดังกล่าวควรต้องพิจารณาร่วมกับหลักเกณฑ์อื่นด้วย เช่น ผลกระทบต่อชุมชน การพิจารณาในเชิงเศรษฐกิจ และการพิจารณาเรื่องความเป็นไปได้ในทางปฏิบัติ หน้าที่ตามมาตรา 34 ในการปฏิบัติตามคำสั่งของ กปช. ควรมีการกำหนดเวลาตามสมควรสำหรับการปฏิบัติดังกล่าว ในทุกกรณี กำหนดเวลาดังกล่าวควรมีความเหมาะสมเมื่อพิจารณาจากปัจจัยทั้งหมดที่เกี่ยวข้อง เช่น ผลกระทบที่จะได้รับ ความสามารถของบริษัทในการดำเนินการตามคำสั่งได้จริง ค่าใช้จ่ายในการดำเนินการดังกล่าว และประโยชน์ที่จะได้รับจากการดำเนินการดังกล่าว ปัจจุบัน มาตรา 34 ให้อำนาจแก่ กปช. ในการกำหนดเวลาได้ตามดุลพินิจของ กปช. ซึ่งอาจไม่มีความเหมาะสม และการไม่ปฏิบัติตามคำสั่งนั้นอาจทำให้บริษัทที่เกี่ยวข้องได้รับโทษที่รุนแรงได้ การขอข้อมูลจากหน่วยงานเอกชนตามมาตรา 43 และ 47 ควรมีกรณียกเว้นและควรต้องแจ้งให้บุคคลภายนอกที่ได้รับผลกระทบ บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า บุคคลภายนอกที่เป็น |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|-----|--------|--|--|
| | | <p>ในการเสนอให้หน่วยงานรัฐที่มีหน้าที่กำกับดูแลพิจารณาลงโทษหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำสั่งของ กปช. “โดยใช้อำนาจตามกฎหมายประกาศ ข้อบังคับอื่นใดที่มีอยู่”</p> <ul style="list-style-type: none"> นอกจากนี้ มาตรา 34, 36, 37 และ 46 ได้ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการสั่งการ ขอ และกำกับให้หน่วยงานเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง ปฏิบัติการตามร่าง พ.ร.บ. ปี 2561 นี้ หรือแนวทางที่เกี่ยวข้อง และให้ความช่วยเหลือในสถานการณ์อย่างใดอย่างหนึ่ง โดยที่ไม่ต้องมีคำสั่งศาล โดยมีข้อยกเว้นเพียงกรณีเดียวตามมาตรา 44 ที่ กปช. ต้องได้รับอนุญาตจากศาลหาก กปช. ต้องใช้เครื่องมือสื่อสาร เครื่องมือทางอิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใดเพื่อติดตามการก่อให้เกิดภัยคุกคามทางไซเบอร์ อันมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลอื่น หน่วยงานที่อยู่ภายใต้บังคับของกฎหมายนี้ไม่มีสิทธิโต้แย้งคำสั่ง อีกทั้งการไม่ปฏิบัติตามคำสั่งอาจทำให้ได้รับโทษที่รุนแรงได้ | <p>เจ้าของข้อมูลที่ถูกเปิดเผยตามมาตรา นี้ควรมีสิทธิได้รับแจ้งก่อนที่จะมีการเปิดเผยข้อมูลนั้นเพื่อให้บุคคลภายนอกดังกล่าวได้มีโอกาสคัดค้านการเปิดเผยข้อมูล</p> <ul style="list-style-type: none"> อำนาจในการเข้าถึงข้อมูลควรต้องมีการตรวจสอบและการถ่วงดุลตามควรเสมอ เช่น การตรวจสอบความชอบด้วยกฎหมายโดยศาล (ได้แก่ การขอคำสั่งศาล) และสิทธิในการโต้แย้งคำสั่ง การพิจารณาโทษตามมาตรา 47 มีความไม่ชัดเจน บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า มาตรา 47 ควรกำหนดโทษที่หน่วยงานเอกชนอาจได้รับให้ชัดเจน มิใช่เพียงแค่อ้างถึงกฎหมาย ประกาศ หรือข้อบังคับอื่นใด |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|--------------|---|--|--|
| เรื่องอื่น ๆ | | | |
| 6. | กฎหมายและเจ้าหน้าที่มีอำนาจซ้ำซ้อนกัน (มาตรา 7, 14, 17 และ มาตรา 30 ถึง 52) | ร่าง พ.ร.บ. ปี 2561 ให้อำนาจแก่เจ้าหน้าที่หลายราย (รวมถึงกรรมการที่แต่งตั้งจากหลากหลายองค์กร รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และคณะรัฐมนตรี) ในการขอความร่วมมือและสั่งการให้หน่วยงานเอกชนกระทำการหรืองดเว้นกระทำการใดๆ ในสถานการณ์หนึ่งๆ | ตามร่าง พ.ร.บ. ปี 2561 อำนาจที่ให้แก่เจ้าหน้าที่หลายรายอาจทำให้มีการสั่งการที่ขัดแย้งกัน ซึ่งทำให้หน่วยงานเอกชนอาจต้องถ่วงถ่วงว่าจะดำเนินการอย่างไรกับคำสั่งต่างๆ ที่ได้รับจากเจ้าหน้าที่หลายราย โดยเฉพาะในกรณีเหตุภัยคุกคามทางไซเบอร์ที่จำเป็นต้องดำเนินการในทันที เนื่องจากการติดต่อเจ้าหน้าที่หลายรายย่อมทำให้เกิดความล่าช้าในการดำเนินการ ด้วยเหตุนี้ บีเอสเอและสภาธุรกิจ จึงขอเรียนเสนอให้มีหน่วยงานกำกับดูแลเพียงหน่วยงานเดียวที่มีอำนาจหน้าที่ในการตรวจสอบดูแลและบังคับใช้กฎหมายตามร่าง พ.ร.บ. ปี 2561 แทนการกำหนดให้หลายหน่วยงานมีอำนาจหน้าที่ดังกล่าว นอกจากนี้ อำนาจของหน่วยงานดังกล่าวต้องมีการควบคุมโดยมีกฎระเบียบที่โปร่งใสและมีกฎหมายที่กำหนดอำนาจของหน่วยงานนั้นไว้อย่างชัดเจน อีกทั้งมีการตรวจสอบโดยรัฐมนตรีและศาล |
| 7. | การรักษาความลับ (มาตรา 48) | <ul style="list-style-type: none"> นอกจากมาตรา 48 แล้ว ไม่มีบทบัญญัติอื่นใดในร่าง พ.ร.บ. ปี 2561 ที่กล่าวถึงเรื่องการรักษาความลับหรือการปกป้องความเป็นส่วนตัว แม้มาตรา 48 จะกำหนดโทษสำหรับพนักงานเจ้าหน้าที่ที่เปิดเผยข้อมูลที่ได้มาโดยการใช้อำนาจของตน แต่การคุ้มครองดังกล่าวจำกัดแต่เพียงการเปิดเผยแก่บุคคลอื่น แต่ไม่ได้ห้ามการใช้ข้อมูลดังกล่าวโดยพนักงานเจ้าหน้าที่รายนั้นเองเพื่อประโยชน์ของตน | บีเอสเอและสภาธุรกิจ ขอเรียนว่า ร่าง พ.ร.บ. ปี 2561 ควรมีบทบัญญัติเพิ่มเติมที่ชัดเจนในเรื่องการรักษาความลับและการปกป้องข้อมูลส่วนบุคคล ซึ่งรวมถึงการกำหนดหน้าที่ที่ชัดเจนของพนักงานเจ้าหน้าที่ในการปกป้องและรักษาความลับของข้อมูลดังกล่าว รวมถึงการกำหนดหน้าที่และขั้นตอนในการขอความยินยอม และวิธีใช้ เปิดเผย เก็บ และกำจัดข้อมูลดังกล่าวเมื่อไม่จำเป็นแล้ว |

| ข้อ | เรื่อง | รายละเอียด | ความเห็นของบีเอสเอและสภาธุรกิจ |
|-----|----------------------------------|--|---|
| 8. | การแบ่งปันข้อมูลข่าวสาร (ทั่วไป) | ร่าง พ.ร.บ. ปี 2561 ไม่มีการกล่าวถึงเรื่องการแบ่งปันข้อมูลไว้อย่างชัดเจน | <ul style="list-style-type: none"> • บีเอสเอและสภาธุรกิจ เห็นว่า การแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ ช่องโหว่ และเหตุทางไซเบอร์ ต่อผู้ที่ได้รับผลกระทบ ตลอดจนหน่วยงานอื่นๆ เพื่อป้องกันการโจมตี เป็นเรื่องที่สำคัญต่อการส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเป็นวิธีที่น่าจะมีประสิทธิภาพมากกว่าการรายงานเหตุภัยคุกคามทางไซเบอร์ • เนื่องจากเป้าหมายของการโจมตีอาจเป็นได้ทั้งภาคเอกชนและหน่วยงานของรัฐทั่วประเทศ บีเอสเอและสภาธุรกิจ จึงขอเรียนเสนอว่า ร่าง พ.ร.บ. ปี 2561 ควรสนับสนุนให้มีการจัดทำนโยบายที่มีประสิทธิภาพในเรื่องการแบ่งปันข้อมูลข่าวสารระหว่างภาครัฐและเอกชน ระหว่างหน่วยงานเอกชนด้วยกัน และระหว่างหน่วยงานของรัฐด้วยกัน • บีเอสเอและสภาธุรกิจ ขอเรียนเสนอว่า ร่าง พ.ร.บ. ปี 2561 และนโยบายเรื่องการแบ่งปันข้อมูลข่าวสารควรมีข้อจำกัดเกี่ยวกับความรับผิดชอบที่หน่วยงานที่เป็นผู้แบ่งปันข้อมูลข่าวสารอาจมี โดยที่ยังคงสามารถปกป้องความเป็นส่วนตัวของผู้ที่ได้รับผลกระทบจากการแบ่งปันข้อมูลข่าวสาร อำนวยความสะดวกในการแบ่งปันข้อมูลข่าวสารหลายทาง ส่งเสริมให้ดำเนินการอย่างทันท่วงที และทำให้แน่ใจว่าข้อมูลข่าวสารที่ได้รับไปนั้นจะใช้เพื่อส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น |

ภาคผนวก ซี

ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคง
ปลอดภัยไซเบอร์
(6 พฤษภาคม 2558)

(กระดาษหัวจดหมายของบีเอสเอ)

วันที่ 6 พฤษภาคม 2558

เป็นความลับและห้ามเผยแพร่

เลขาธิการคณะกรรมการกฤษฎีกา
สำนักงานคณะกรรมการกฤษฎีกา
ถนนพระอาทิตย์ เขตพระนคร
กรุงเทพมหานคร 10200

เรื่อง ความเห็นของบีเอสเอเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านเลขาธิการคณะกรรมการกฤษฎีกา

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (บีเอสเอ)¹ ไคร์ขอขอบพระคุณที่ท่านได้เปิดโอกาสให้มีการเสนอความเห็นต่อคณะกรรมการกฤษฎีกาเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (“ร่าง พ.ร.บ.”) และขอแสดงความชื่นชมในความพยายามครั้งสำคัญที่แสดงถึงความมีวิสัยทัศน์ของรัฐบาลไทยในครั้งนี้อย่างเต็มที่ในการให้แน่ใจว่าประเทศจะมีความพร้อมในการระงับยับยั้งและจัดการกับภัยคุกคามทางไซเบอร์ หนึ่งในกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพต้องจัดทำขึ้นบนพื้นฐานกฎหมายที่ชัดเจน เพื่อเอื้อให้มีการประสานความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมาย ภาครัฐ และภาคเอกชน ซึ่งการประสานความร่วมมือดังกล่าวย่อมต้องอาศัยความไว้วางใจซึ่งกันและกัน ซึ่งจะเกิดขึ้นได้ก็ต่อเมื่อมีมาตรการป้องกันอย่างเพียงพอและภาคเอกชนจะได้รับประโยชน์อย่างเหมาะสม ตัวอย่างเช่น ข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยต้องมีความสมดุลอย่างเหมาะสมระหว่างความจำเป็นในการคุ้มครองความเป็นส่วนตัวกับเสรีภาพของประชาชน เมื่อคำนึงถึงหลักการเหล่านี้เป็นสิ่งสำคัญ บีเอสเอมีความกังวลว่า บทบัญญัติของร่าง พ.ร.บ. นี้ที่ให้อำนาจในการสอดส่องดูแล

¹ บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอเป็นบริษัทต่างๆ ที่สร้างสรรค์นวัตกรรมที่ทันสมัยที่สุดของโลก ซึ่งนำเสนอโซลูชันซอฟต์แวร์ที่ผลักดันให้เศรษฐกิจเติบโตและปรับปรุงคุณภาพชีวิตในยุคปัจจุบัน บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดี.ซี. และมีการดำเนินการในกว่า 60 ประเทศทั่วโลก โดยเป็นผู้ริเริ่มโครงการส่งเสริมการปฏิบัติตามกฎหมายเพื่อรณรงค์การใช้ซอฟต์แวร์ที่ถูกกฎหมาย และสนับสนุนนโยบายสาธารณะที่ส่งเสริมให้มีการสร้างสรรค์นวัตกรรมเทคโนโลยีและขับเคลื่อนให้เศรษฐกิจดิจิทัลเติบโต สมาชิกของบีเอสเอรวมถึงบริษัท Adobe, Altium, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks และ Trend Micro

(ตามมาตรา 35) อาจก่อให้เกิดผลอันไม่พึงประสงค์ได้ ซึ่งรวมถึงการที่ความเชื่อมั่นของผู้บริโภคต่อระบบเทคโนโลยีสารสนเทศของประเทศไทยอาจลดทอนลง ด้วยเหตุนี้ บีเอสเอจึงขอเรียนเสนอความเห็นต่อไปนี้ด้วยเจตนาที่จะมีส่วนช่วยให้ร่างกฎหมายดังกล่าวบรรลุตามเจตนารมณ์อันดีในการกำหนดให้มี “การดำเนินการที่ทันทางที่และเป็นไปในทิศทางเดียวกัน” ต่อภัยคุกคามทางไซเบอร์

มาตรา 6 กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรรมการส่วนใหญ่ในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) มาจากหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความปลอดภัยและความมั่นคง เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงกลาโหม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ บีเอสเอขอเรียนเสนอว่า เพื่อให้ กปช. มีทัศนคติที่เป็นกลางและเพื่อให้แน่ใจว่าจะมีการพิจารณาในเรื่องความเป็นส่วนตัวของบุคคลและเสรีภาพของประชาชน กปช. ควรประกอบด้วยกรรมการที่แต่งตั้งจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดินด้วย เนื่องจากการที่คณะกรรมการประกอบด้วยกรรมการที่มีความรู้และประสบการณ์ที่หลากหลายนั้นจะช่วยป้องกันไม่ให้สิทธิของบุคคลถูกกระทบเกินควรได้

มาตรา 7 ถึงมาตรา 34 ของร่าง พ.ร.บ. ให้อำนาจแก่ กปช. อย่างกว้างขวาง

บีเอสเอเห็นด้วยกับการที่ร่างกฎหมายนี้กำหนดให้ กปช. ทำหน้าที่เป็นศูนย์กลางที่อำนวยความสะดวกในการประสานความร่วมมือระหว่างหน่วยงานของรัฐทั้งหมดที่เกี่ยวข้องในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ ทั้งนี้ ตามมาตรา 7 กปช. มีอำนาจหน้าที่ต่างๆ ซึ่งรวมถึงการ “จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” และมาตรา 27 และมาตรา 28 ได้กำหนดให้สำนักงาน กปช. จัดทำแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องและเป็นตามนโยบายและแผนดังกล่าว ดังนั้น ร่าง พ.ร.บ. นี้จึงควรต้องกำหนดไว้อย่างชัดเจนว่า เหตุการณ์ลักษณะใดที่ถือเป็นภัยคุกคามทางไซเบอร์ที่กฎหมายนี้กำหนดให้ต้องมีการดำเนินการอย่างหนึ่งอย่างใด เช่น เมื่อเกิดภัยคุกคามทางไซเบอร์ มาตรา 33 ได้ให้อำนาจแก่ กปช. ในการสั่งการให้หน่วยงานของรัฐทั้งหมดที่เกี่ยวข้องดำเนินการใดก็ตามอันจะมีผลเป็นการควบคุมหรือบรรเทาความเสียหายที่เกิดขึ้น และมาตรา 34 ได้ขยายอำนาจของ กปช. ให้สามารถสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นการกระทำอย่างใดอย่างหนึ่ง และให้รายงานผลการปฏิบัติการต่อ กปช. หากเป็นกรณีภัยคุกคามทางไซเบอร์อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ

จะเห็นได้ว่า บทบัญญัติในมาตราข้างต้นได้ให้อำนาจแก่ กปช. ไว้อย่างกว้างขวาง แต่กฎหมายฉบับนี้กลับไม่ได้กำหนดคำจำกัดความของ “ภัยคุกคามทางไซเบอร์” ไว้อย่างชัดเจน อีกทั้งไม่ได้กำหนดหลักเกณฑ์ในการพิจารณาว่าความเสียหายที่เกิดขึ้นนั้นถึงขนาดที่ กปช. พึงต้องดำเนินการอย่างหนึ่งอย่างใดหรือไม่ นอกจากนี้ ร่าง พ.ร.บ. ดังกล่าวไม่ได้กำหนดแนวทางในการพิจารณาว่าเหตุการณ์ใดที่อาจกระทบต่อ “ความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ” ซึ่งมีความรุนแรงถึงขนาดที่ กปช. มีอำนาจสั่งการต่อหน่วยงานภาคเอกชนได้ ร่าง พ.ร.บ. ดังกล่าวจึงควรกำหนดคำจำกัดความของคำที่มี

ความหมายกว้างเหล่านี้ให้ชัดเจน เพื่อที่บุคคลทุกคนที่ได้รับผลกระทบจะได้เข้าใจสถานะของตน และเพื่อที่จะได้ไม่มีความกำกวมต่อไป

มาตรา 35 (1) และ (2) รัฐบาลเรียกขอข้อมูลหรือให้ดำเนินการอย่างใดอย่างหนึ่ง

มาตรา 35 (1) แห่งร่าง พ.ร.บ. นี้ให้อำนาจแก่พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการสำนักงาน กปช. ในการมีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติตามพระราชบัญญัตินี้

มาตรา 35 (2) ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการมีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.

บีเอสเอขอเรียนเสนอว่า เพื่อให้แน่ใจว่าจะไม่มีการใช้อำนาจที่กว้างขวางเหล่านี้ในทางมิชอบ กฎหมายฉบับนี้ควรต้องมีหลักเกณฑ์ที่ชัดเจนที่กำหนดประเภทและขอบเขตของข้อมูลที่พนักงานเจ้าหน้าที่สามารถเรียกได้ และระบุกรณีที่สำนักงาน กปช. สามารถเรียกให้หน่วยงานเอกชนดำเนินการอย่างใดอย่างหนึ่งได้อีกทั้งควรกำหนดว่าบุคคลใดในสำนักงาน กปช. ที่อาจเรียกขอข้อมูลได้ และกำหนดหลักเกณฑ์ในการจัดการข้อมูลดังกล่าวเพื่อให้แน่ใจว่าข้อมูลที่ กปช. ได้รับไปนั้นจะได้รับความคุ้มครองอย่างเหมาะสม นอกจากนี้ การใช้อำนาจเหล่านี้ควรจำกัดอยู่เฉพาะในกรณีที่เชื่อได้ว่าจะมีภัยคุกคามทางไซเบอร์อย่างใดอย่างหนึ่งเกิดขึ้นเท่านั้น

มาตรา 35 (3) อำนาจในการสอดส่องดูแล

มาตรา 35 (3) ให้อำนาจแก่ กปช. ในการเข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากอำนาจหน้าที่อย่างกว้างขวางของ กปช. ในการสอดส่องดูแลดังกล่าวนี้ทำให้ กปช. สามารถเข้าถึงเครือข่ายสื่อสารได้อย่างไม่จำกัด บีเอสเอจึงมีความกังวลเป็นอย่างยิ่งในเรื่องความเป็นส่วนตัว บีเอสเอเห็นว่ามาตรา 35 (3) ดังกล่าวไม่มีการถ่วงดุลที่จำเป็นต้องมีระหว่างความมั่นคงของประเทศกับความเป็นส่วนตัวของข้อมูล เนื่องจากกฎหมายดังกล่าวกำหนดให้รัฐบาลมีดุลพินิจในการใช้อำนาจได้โดยไม่ต้องมีการตรวจสอบความชอบด้วยกฎหมายโดยศาล เช่น ไม่มีบทบัญญัติใดที่กำหนดให้ต้องขออนุญาตศาลก่อนเข้าถึงการติดต่อสื่อสารส่วนบุคคล กฎหมายนี้เพียงแต่กำหนดว่า พนักงานเจ้าหน้าที่อาจมีอำนาจเข้าถึงข้อมูลได้หากได้รับมอบหมายเป็นหนังสือจากเลขาธิการสำนักงาน กปช.

หากพิจารณาในแง่พาณิชย์ มาตรา 35 (3) ของร่าง พ.ร.บ. นี้อาจขัดขวางการลงทุนด้านเทคโนโลยีสารสนเทศในประเทศไทยได้ เนื่องจากธุรกิจใดก็ตามที่มีระบบเทคโนโลยีสารสนเทศ ตั้งแต่ธนาคารและสถาบันการเงินไปจนถึงธุรกิจค้าปลีก อาจต้องอยู่ภายใต้บังคับของมาตรา 35 (3) ดังกล่าว โดยที่ผู้ให้บริการไม่อาจรับรองแก่ลูกค้าของตนได้ว่าข้อมูลส่วนบุคคล ความลับทางการค้า หรือประวัติการซื้อหุ้นของลูกค้าจะถูกเก็บไว้เป็นความลับ ซึ่งอาจทำให้ธุรกิจด้านเทคโนโลยีสารสนเทศระงับการใช้หรือการ

ลงทุนด้านระบบเทคโนโลยีสารสนเทศในประเทศไทย อันเป็นทิศทางที่ตรงกันข้ามกับความพยายามในการผลักดันให้ประเทศไทยเป็นศูนย์กลางด้านเทคโนโลยีสารสนเทศของกลุ่มประเทศอาเซียน

การที่มาตรา 35 (3) ไม่มีมาตรการตรวจสอบและถ่วงดุลอำนาจดังกล่าวนี้ขัดกับมาตรการรักษาความเป็นส่วนตัวของข้อมูลตามกฎหมายที่ใช้บังคับอยู่ในประเทศไทยและตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ เช่น ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 (“พ.ร.บ. การสอบสวนคดีพิเศษ”) มีการให้อำนาจในการเข้าถึงข้อมูลส่วนบุคคลในทำนองเดียวกันหากมีเหตุอันควรเชื่อได้ว่ามีสื่อใดที่ถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ ประการสำคัญ มาตรา 25 แห่ง พ.ร.บ. การสอบสวนคดีพิเศษดังกล่าวกำหนดให้พนักงานสอบสวนคดีพิเศษต้องยื่นคำขอ ฝ่ายเดียวต่อศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้ นอกจากนี้ ศาลอาจสั่งอนุญาตดังกล่าวได้คราวละไม่เกิน 90 วันเท่านั้น ในทำนองเดียวกัน ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็ได้กำหนดให้พนักงานเจ้าหน้าที่ผู้บังคับใช้กฎหมายต้องได้รับคำสั่งศาลก่อนจึงจะเรียกให้ผู้ให้บริการเปิดเผยเนื้อหาของการติดต่อสื่อสารของผู้ใช้บริการได้

จากบทบัญญัติข้างต้น มาตรา 35 (3) ของร่าง พ.ร.บ. นี้จึงควรกำหนดให้พนักงานเจ้าหน้าที่ต้องได้รับคำสั่งศาลก่อนจึงจะสามารถเข้าถึงข้อมูลส่วนบุคคลได้เช่นกัน อีกทั้งควรกำหนดให้คำสั่งอนุญาตดังกล่าวมีผล บังคับเพียงช่วงระยะเวลาหนึ่งๆ เท่านั้น นอกจากนี้ ควรกำหนดให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจตาม มาตรา 35 (3) ได้เฉพาะในกรณีที่เกิดความเสียหายต่อความมั่นคงของชาติเท่านั้น สุดท้ายนี้ บีเอสเอขอ เคารพเสนอให้มีหน่วยงานอิสระ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เสนอให้มีการแต่งตั้งตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีอำนาจตรวจสอบการใช้อำนาจของ กปช. ตามมาตรา 35 (3) เพื่อให้แน่ใจว่าการถ่วงดุลอย่างเพียงพอระหว่างความเป็นส่วนตัวกับความจำเป็นของการใช้อำนาจในการ สอดส่องดูแล

บทสรุป

บีเอสเอเห็นถึงความพยายามของรัฐบาลไทยในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์ และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดี พนักงานเจ้าหน้าที่ตามกฎหมายนี้ควรกระทำการอย่าง โปร่งใสและไม่ล่วงละเมิดความเป็นส่วนตัวของผู้ใช้ ไม่เช่นนั้นอาจก่อให้เกิดผลเสียต่อแผนด้านดิจิทัลเพื่อ เศรษฐกิจได้ นอกจากนี้ ควรเน้นย้ำในเรื่องการให้ความร่วมมือของเอกชนในการรายงานรัฐบาลเมื่อมีการ กระทำที่เป็นภัยต่อความปลอดภัยของระบบเพื่อป้องกันภัยคุกคามทางไซเบอร์เพื่อรักษาความมั่นคง ปลอดภัยไซเบอร์ของชาติ การที่กฎหมายนี้ให้อำนาจแก่ กปช. และ/หรือพนักงานเจ้าหน้าที่ตามกฎหมาย นี้อย่างกว้างขวางอาจนำไปสู่การกระทำที่เป็นการหลอกลวง ความไม่ไว้วางใจ และทำให้เอกชนให้ ความร่วมมือน้อยลงในการรายงานเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ ในขณะที่มาตรา 5(4) มาตรา 7(8) มาตรา 17(2) มาตรา 17(3) และ มาตรา 18(3) พยายามส่งเสริมให้มีการประสานความร่วมมือระหว่าง ภาครัฐและเอกชนในการป้องกันภัยคุกคามทางไซเบอร์ แต่ในความเป็นจริงแล้วภาคเอกชนอาจเกิดความ ลังเลที่จะให้ข้อมูลกับรัฐบาลด้วยเกรงว่ารัฐบาลจะเรียกขอข้อมูลที่ไม่เกี่ยวข้องหรือเข้ายุ่งเกี่ยวกับการ

(คำแปล)

ติดต่อสื่อสารส่วนบุคคลทางสื่อเทคโนโลยีสารสนเทศ ด้วยเหตุนี้ บีเอสเอจึงใคร่ขอความกรุณาให้ คณะกรรมการกฤษฎีกาพิจารณาความเห็นข้างต้นอย่างถี่ถ้วนเพื่อให้เกิดความโปร่งใสและเพื่อสร้างความไว้วางใจระหว่างภาครัฐและเอกชน โดยที่ยังสามารถรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ในขณะเดียวกัน

บีเอสเอมีความยินดีที่จะหารือในเรื่องนี้กับท่านได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นใดๆ กรุณาติดต่อนางสาววารุณี รัชตพัฒนากุล ผู้แทนในประเทศไทยของบีเอสเอ ที่ varuneer@bas.org หรือที่หมายเลข +668-1840-0591

ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

บุน โฟ มก

ผู้อำนวยการฝ่ายนโยบาย ภูมิภาคเอเชีย-แปซิฟิก

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง

1. ชพณฯ รองนายกรัฐมนตรี ดร. วิษณุ เครืองาม
2. นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)