(คำแปล)

(กระดาษหัวจดหมายของบีเอสเอ) *(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 (“**สภาธุรกิจฯ**”) ได้เรียนเสนอความเห็นในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ตามหนังสือลงวันที่ 17 เมษายน 2561 ที่ผ่านมา (สำเนาหนังสือปรากฏอยู่ในภาคผนวก บี ของหนังสือฉบับนี้) นั้น

จากการศึกษาร่าง พ.ร.บ. ปี 2561 และการหารือกับกลุ่มสมาชิกเพิ่มเติม บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอความเห็นเพิ่มเติมจากความเห็นที่อ้างถึงข้างต้นมาตามภาคผนวก เอ ของหนังสือฉบับนี้ ซึ่งมีเนื้อหาโดยสรุปดังปรากฏด้านล่างนี้ บีเอสเอและสภาธุรกิจฯ ใคร่ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาความเห็นเพิ่มเติมดังกล่าวประกอบกับความเห็นที่ได้เรียนเสนอไว้เมื่อครั้งก่อนด้วยจักเป็นพระคุณยิ่ง

เนื้อหาของความเห็นเพิ่มเติมจากความเห็นตามหนังสือฉบับลงวันที่ 17 เมษายน 2561 สามารถกล่าวโดยสรุปได้ดังนี้

- การกำหนดให้มีกรรมการที่เป็น**ผู้แทนจากภาคอุตสาหกรรม**จะเป็นประโยชน์ต่อคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“**กปช.**”)
- ร่าง พ.ร.บ. ปี 2561 ควรใช้บังคับกับ “**หน่วยงานเอกชน**” **ที่จัดตั้งขึ้นในประเทศไทยและเป็นผู้ประกอบกิจการหรือเป็นผู้ควบคุมโครงสร้างพื้นฐานที่สำคัญ (ตามคำจำกัดความที่ได้เรียน**

เสนอไว้ในหนังสือฉบับวันที่ 17 เมษายน 2561) เท่านั้น และควรกำหนดหน้าที่ให้กับหน่วยงานเอกชนดังกล่าวไว้อย่างชัดเจน โดยจำกัดเฉพาะแต่เพียงหน้าที่ที่**มีความเหมาะสม**และ**สามารถปฏิบัติได้จริง**

- **หน้าที่ในการรายงาน**ควรจำกัดเฉพาะกรณี**เหตุภัยคุกคามทางไซเบอร์ที่สำคัญซึ่งได้เกิดขึ้นแล้ว** เท่านั้น โดยไม่รวมถึงเหตุภัยคุกคามทางไซเบอร์ที่ไม่มีความสำคัญ หรือเหตุภัยคุกคามทางไซเบอร์ที่ “คาด” ว่าจะเกิดขึ้น
- การใช้อำนาจในการเข้าถึง**ข้อมูลและเครื่องมือ**ควรเป็นไปอย่าง**ได้สัดส่วน**และมีมาตรการ**ตรวจสอบและถ่วงดุล**ที่เหมาะสม **ซึ่งรวมถึงการตรวจสอบความชอบด้วยกฎหมายโดยศาลและสิทธิในการโต้แย้งหรืออุทธรณ์คำสั่ง**
- ควรมี**หน่วยงานกำกับดูแลเพียงหน่วยงานเดียว**ที่มีอำนาจหน้าที่ในการตรวจสอบดูแลและบังคับใช้กฎหมายตามร่าง พ.ร.บ. ปี 2561
- ร่าง พ.ร.บ. ปี 2561 ควรบัญญัติในเรื่อง**การรักษาความลับและการคุ้มครองความเป็นส่วนตัว**ไว้อย่างชัดแจ้งด้วย
- ร่าง พ.ร.บ. ปี 2561 ควรส่งเสริมให้มีการ**แบ่งปันข้อมูลข่าวสาร ซึ่งรวมถึงโดยการจำกัด**ความรับผิดที่เกิดขึ้นจากการแบ่งปันข้อมูลข่าวสารไว้อย่างเหมาะสม

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้ที่ได้เปิดรับฟังความคิดเห็นจากภาคเอกชนและผู้มีส่วนได้เสียอื่นๆ ในการจัดทำกฎหมายนี้ และขอสนับสนุนให้ยังคงมีการเปิดโอกาสให้มีการสื่อสารและหารือกับภาคเอกชนต่อไป โดยเฉพาะอย่างยิ่ง ในการจัดทำระเบียบและประกาศต่างๆ หรือข้อกำหนดเพิ่มเติมใดๆ ที่ออกตามร่าง พ.ร.บ. ปี 2561 นี้ ควรมีขั้นตอนการหารือกับภาคเอกชนเช่นกัน เพื่อให้เกิดความชัดเจนและความสอดคล้องกัน

บีเอสเอและสภาธุรกิจฯ ยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อเช่นเคย หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อโดยตรงไปที่ afeldman@usasean.org หรือที่หมายเลข 202-375-4393 หรือที่ jaredr@bsa.org หรือที่หมายเลข +65-6292-9609 หรือติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่** varuneer@bsa.org **หรือที่หมายเลข +668-1840-0591 หรือนางสาวเอลล่า ดวงแก้ว ผู้จัดการประจำประเทศไทยแห่งสภาธุรกิจสหรัฐอเมริกา-อาเซียน ที่** eduangkaew@usasean.org **หรือที่หมายเลข 202-440-3642**

บีเอสเอและสภาธุรกิจฯ ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

อเล็กซานเดอร์ ซี. เฟล์ดแมน
ประธานและประธานเจ้าหน้าที่บริหาร
ภูมิภาคเอเชีย
สภาธุรกิจสหรัฐอเมริกา-อาเซียน

(ลายมือชื่อ)

จาเร็ด แร้กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย
ภูมิภาคเอเชีย แปซิฟิก
บีเอสเอ I พันธมิตรธุรกิจซอฟต์แวร์

สำเนาถึง

1. ดร.พิเชฐ ดุรงคเวโรจน์ 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 จะได้มีการกำหนดให้แต่งตั้งกรรมการจากหน่วยงานที่หลากหลายมากขึ้นแล้ว แต่ยังไม่มีกรรมการรายใดที่เป็นผู้แทนจากภาคอุตสาหกรรม	จากความเห็นที่ได้เรียนเสนอไว้ในครั้งก่อนว่า กปช. ควรประกอบด้วยกรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดินด้วยนั้น บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอเพิ่มเติมว่า กปช. ควรประกอบด้วยกรรมการที่มาจากภาคอุตสาหกรรมด้วย ซึ่งไม่เพียงแต่จะช่วยให้คณะกรรมการมีมุมมองที่รอบด้านมากขึ้นเท่านั้น แต่ยังช่วยเสริมสร้างการประสานความร่วมมือระหว่างภาครัฐและเอกชน อันจะนำไปสู่การปฏิบัติที่ก่อให้เกิดประสิทธิภาพสูงสุดด้วย
บี. อำนาจของ กปช.			
2.	**คำจำกัดความของ “หน่วยงานเอกชน” และความจำเป็นในการกำหนดหลักเกณฑ์ที่เหมาะสม**	ร่าง พ.ร.บ. ปี 2561 ประสงค์จะกำกับดูแล “หน่วยงานเอกชน” ซึ่งได้แก่หน่วยงานที่จัดตั้งขึ้น ไม่ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือที่ไม่แสวงหากำไร ทั้งนี้ ไม่ว่าจะจดทะเบียนเป็นนิติบุคคลหรือไม่ก็ตาม คำจำกัดความของ “หน่วยงานเอกชน” ดังกล่าวนี้อาจกว้างเกินไปสำหรับเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และควรกำหนดให้แคบลงกว่านี้	บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ในกฎหมายนี้ คำจำกัดความของ “หน่วยงานเอกชน” ควรจำกัดอยู่ที่บริษัทที่จัดตั้งขึ้นในประเทศไทยซึ่งเป็นผู้ประกอบกิจการหรือเป็นผู้ควบคุม “โครงสร้างพื้นฐานที่สำคัญ” (ตามคำจำกัดความที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) ในประเทศไทยเท่านั้น

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
	(มาตรา 3, 36 และ 37)		
3.	**หน้าที่ในการบังคับบัญชาและสั่งการให้หน่วยงานต่าง ๆ ปฏิบัติงาน** (มาตรา 33, 34, 36 และ 37)	• อำนาจของ กปช. ในการบังคับบัญชาและสั่งการหน่วยงานเอกชนตามมาตรา 33 และในการสั่งการให้หน่วยงานเอกชน “กระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง” ตามมาตรา 37 มีข้อจำกัดอยู่เพียงเล็กน้อย • ตามมาตรา 34 กปช. มีดุลพินิจอย่างกว้างขวางในการมีมติว่าหน่วยงานเอกชนไม่ปฏิบัติตามพระราชบัญญัตินี้ หรือปฏิบัติการโดยขัดหรือแย้งกับแนวทางที่กำหนด หรือในการแจ้งให้แก้ไข ยกเลิก หรือยุติการดำเนินการดังกล่าว ซึ่งหากไม่ดำเนินการภายในเวลาที่กำหนด คณะรัฐมนตรีจะเป็นผู้พิจารณาสั่งการต่อไปตามดุลพินิจที่มีอย่างกว้างขวาง • บทบัญญัติในมาตรา 36 และมาตรา 37 ใช้ถ้อยคำที่กว้างเกินไปโดยบังคับใช้กับหน่วยงานเอกชน *ทั้งหมด* แม้กระทั่งหน่วยงานที่ไม่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์	• ควรกำหนดและจำกัดอำนาจที่ให้แก่ กปช. และหน่วยงานที่ได้รับแต่งตั้งให้มีความชัดเจนยิ่งขึ้น รวมถึงให้มีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาล อีกทั้งหน่วยงานเอกชนและบุคคลภายนอกควรมีโอกาสอย่างเต็มที่ในการโต้แย้งคำสั่งและยื่นอุทธรณ์ต่อศาลหากไม่เห็นพ้องด้วยกับคำวินิจฉัย บีเอสเอและสภาธุรกิจฯ ทราบว่าตาม ร่าง พ.ร.บ. ปี 2561 นั้น จำเป็นต้องขอคำสั่งศาลก่อนใช้อำนาจบางประการ (เว้นแต่กรณีจำเป็นเร่งด่วน) อย่างไรก็ดี บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า การใช้อำนาจของ กปช. ควรต้องมีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาลในหลายกรณีมากขึ้น เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับ “หน่วยงานเอกชน” • มาตรา 34 ควรแก้ไขให้มีการระบุให้ชัดเจนว่า กปช. มีอำนาจบังคับบัญชาหรือสั่งการหน่วยงานเอกชนให้ดำเนินการอย่างไรได้บ้าง ทั้งนี้ เพื่อที่จะได้มีหลักเกณฑ์ที่ชัดเจน เพื่อให้ทุกฝ่ายมีความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง อันจะนำไปสู่ความชัดเจนในเรื่องการรักษาความมั่นคงไซเบอร์ในประเทศไทย • บีเอสเอและสภาธุรกิจฯ มีความกังวลว่า ตามร่าง พ.ร.บ. ปี 2561 (รวมถึงหน้าที่ตามมาตรา 36 และมาตรา 37 เป็นต้น) หน่วยงานเอกชนมีหน้าที่ต้องดำเนินการบางประการในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ที่อาจ

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
			ไม่ได้อยู่ภายใต้การควบคุมของหน่วยงานเอกชนนั้นแต่อย่างใด หรืออาจมีความไม่สมเหตุสมผล ไม่สามารถปฏิบัติได้จริง หรือไม่ได้สัดส่วนแก่กรณีด้วยเหตุนี้ บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอว่า ในร่าง พ.ร.บ. ปี 2561 ทั้งฉบับ (ไม่เพียงแต่เฉพาะบางมาตรา) การกำหนดหน้าที่แก่หน่วยงานเอกชนควรต้องจำกัดเฉพาะแต่เพียงหน้าที่ที่*มีความเหมาะสม*และ*สามารถนำไปปฏิบัติได้จริง*เท่านั้น • สำหรับมาตรา 36 และมาตรา 37 นอกเหนือจากความเห็นที่ได้เรียนเสนอไว้ก่อนหน้านี้ว่าควรใช้หลักเกณฑ์ในเรื่องเหตุภัยคุมคามทางไซเบอร์ที่สำคัญแล้ว บีเอสเอและสภาธุรกิจฯ มีความเห็นว่า ทั้งสองมาตรานี้ควรใช้บังคับเฉพาะกับหน่วยงานที่*ได้รับผลกระทบโดยตรง*จาก “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” (ตามคำจำกัดความที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) เท่านั้น เพื่อที่จะได้หลีกเลี่ยงไม่ให้ตีความได้ว่าหน่วยงานเอกชนที่*ไม่ได้รับผลกระทบ*จะต้องมีหน้าที่ตามมาตรานี้
ซี. หน้าที่ในการรายงานเหตุภัยคุกคามทางไซเบอร์			
4.	**หน้าที่ในการรายงาน** (มาตรา 35 และ 40)	มาตรา 35 กำหนดหน้าที่ในการรายงานทั้งใน*กรณีที่เกิดและคาดว่าจะเกิด*เหตุภัยคุกคามทางไซเบอร์	• กฎหมายไม่ควรกำหนดให้มีหน้าที่ต้องรายงาน*ทุกกรณีที่เกิดหรือคาดว่าจะเกิด*เหตุภัยคุกคามทางไซเบอร์ เนื่องจากประเภทของเหตุภัยคุกคามทางไซเบอร์และที่มาของเหตุดังกล่าวมีการเปลี่ยนแปลงอยู่ตลอดเวลา ด้วยเหตุนี้ บริการบางอย่างจึงอาจตกเป็นเป้าหมายของการโจมตีได้วันละหลายพันครั้ง (หรือกว่านั้น) ซึ่งส่วนใหญ่แล้วสามารถป้องกันได้สำเร็จ แม้ว่าองค์กรต่างๆ อาจจะมีมาตรการที่กำหนดขึ้นเพื่อป้องกันเหตุภัยคุกคามทางไซเบอร์โดยใช้วิธีการที่องค์กรต่างๆ ใช้กันอยู่ล่าสุด แต่การที่จะสามารถ

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
			ระบุเหตุภัยคุกคามได้ทุกครั้งหรือรายงานให้พนักงานเจ้าหน้าที่ทราบทุกครั้งที่คาดว่าจะเกิดเหตุภัยคุกคามก็เป็นเรื่องที่ย่อมเป็นไปไม่ได้ นอกจากนี้หน้าที่ดังกล่าวจะสร้างภาระอย่างยิ่ง ในขณะที่พนักงานเจ้าหน้าที่ไม่สามารถนำข้อมูลไปใช้ประโยชน์ได้เท่าใดนัก เนื่องจากต้องประมวลผลรายงานกรณีที่คาดว่าจะเกิดเหตุภัยคุกคามซึ่งมีจำนวนมหาศาล ซึ่งส่วนใหญ่แล้วไม่ได้เกิดขึ้นจริง (หรืออาจป้องกันได้สำเร็จหรือไม่มีความเสี่ยงว่าจะมีความเสียหายเกิดขึ้นจริง) • บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอให้ใช้ถ้อยคำที่สอดคล้องกันตลอดทั้งฉบับ และกำหนดคำจำกัดความของ “เหตุภัยคุกคามทางไซเบอร์” และ “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” ให้ชัดเจน (ตามที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) • นอกจากนี้ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ควรกำหนดหน้าที่ในการรายงานเฉพาะในกรณีที่เข้า “หลักเกณฑ์ที่พิจารณาจากความสำคัญ” เช่น กรณีของเหตุภัยคุกคามทางไซเบอร์ที่สำคัญและมีความเสี่ยงอย่างแท้จริงว่าจะเกิดความเสียหายอย่างร้ายแรง • บีเอสเอและสภาธุรกิจฯ เชื่อว่า กฎหมายในเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ควรมีขึ้นเพื่อสร้างสภาพแวดล้อมที่เอื้อต่อการแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ มิใช่เพื่อบังคับให้รายงานทุกกรณีที่คาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ ความเห็นเรื่องนี้ในรายละเอียดปรากฏอยู่ในข้อ 8 ด้านล่าง

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
ดี. อำนาจหน้าที่ในการสอดส่องดูแล			
5.	**การเข้าถึงข้อมูลและเครื่องมือ** (มาตรา 34, 36, 37, 43, 46 และ 47)	• มาตรา 43 ได้ให้อำนาจแก่เจ้าหน้าที่ของรัฐที่เกี่ยวข้องและสำนักงาน กปช. ในการขอให้มีการให้ข้อมูล สนับสนุนบุคลากร หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ของหน่วยงานเอกชน โดย กปช. ต้องขอให้ศาลมีคำสั่งหากหน่วยงานเอกชนไม่ยินยอมให้ข้อมูล ให้การสนับสนุนบุคลากร หรือจัดให้ใช้เครื่องมือทางอิเล็กทรอนิกส์ • มาตรา 47 ให้อำนาจแก่เลขาธิการในการเรียกบุคคลมาให้ถ้อยคำ ส่งเอกสารหรือหลักฐาน หรือดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช. หรือเข้าถึงข้อมูลการติดต่อสื่อสาร (รวมถึงการติดต่อสื่อสารทางไปรษณีย์ โทรศัพท์ คอมพิวเตอร์ อุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด) ตามที่เรียนไว้ในหนังสือฉบับก่อนหน้านี้ แม้จะกำหนดให้เลขาธิการต้องขอคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสาร แต่ “กรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง” ที่เป็นข้อยกเว้นนั้นก็มีขอบเขตที่กว้าง นอกจากนี้ มาตรา 47 ได้ให้อำนาจแก่ กปช.	สำหรับมาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอเพิ่มเติมดังนี้ • **การสั่งการ กำกับ หรือขอให้มีการให้ข้อมูลหรือการสนับสนุนใด ๆ ควรจำกัดเฉพาะในกรณีที่มีความเสี่ยงสูงว่าจะเกิดความเสียหายอย่างร้ายแรง** บีเอสเอและสภาธุรกิจฯ ขอเรียนว่า ความเสียหายดังกล่าวควรต้องพิจารณาร่วมกับหลักเกณฑ์อื่นด้วย เช่น ผลกระทบต่อชุมชน การพิจารณาในเชิงเศรษฐกิจ และการพิจารณาเรื่องความเป็นไปได้ในทางปฏิบัติ • **หน้าที่ตามมาตรา 34 ในการปฏิบัติตามคำสั่งของ กปช. ควรมีการกำหนดเวลาตามสมควรสำหรับการปฏิบัติดังกล่าว** ในทุกกรณีกำหนดเวลาดังกล่าวควรมีความเหมาะสมเมื่อพิจารณาจากปัจจัยทั้งหมดที่เกี่ยวข้อง เช่น ผลกระทบที่จะได้รับ ความสามารถของบริษัทในการดำเนินการตามคำสั่งได้จริง ค่าใช้จ่ายในการดำเนินการดังกล่าว และประโยชน์ที่จะได้รับจากการดำเนินการดังกล่าว ปัจจุบัน มาตรา 34 ให้อำนาจแก่ กปช. ในการกำหนดเวลาได้ตามดุลพินิจของ กปช. ซึ่งอาจไม่มีความเหมาะสม และการไม่ปฏิบัติตามคำสั่งนั้นอาจทำให้บริษัทที่เกี่ยวข้องได้รับโทษที่รุนแรงได้ • **การขอข้อมูลจากหน่วยงานเอกชนตามมาตรา 43 และ 47 ควรมีกรณียกเว้นและควรต้องแจ้งให้บุคคลภายนอกที่ได้รับผลกระทบทราบ** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า บุคคลภายนอกที่เป็น

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
		ในการเสนอให้หน่วยงานรัฐที่มีหน้าที่กำกับดูแลพิจารณาลงโทษหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำสั่งของ กปช. “โดยใช้อำนาจตามกฎหมายประกาศ ข้อบังคับอื่นใดที่มีอยู่” • 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 หรือด้วยวิธีการอื่นใดเพื่อติดตามการก่อให้เกิดภัยคุกคามทางไซเบอร์อันมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลอื่น • หน่วยงานที่อยู่ภายใต้บังคับของกฎหมายนี้ไม่มีสิทธิโต้แย้งคำสั่ง อีกทั้งการไม่ปฏิบัติตามคำสั่งอาจทำให้ได้รับโทษที่รุนแรงได้	เจ้าของข้อมูลที่ถูกเปิดเผยตามมาตรานี้ควรมีสิทธิได้รับแจ้งก่อนที่จะมีการเปิดเผยข้อมูลนั้นเพื่อให้บุคคลภายนอกดังกล่าวได้มีโอกาสคัดค้านการเปิดเผยข้อมูล • **อำนาจในการเข้าถึงข้อมูลควรต้องมีการตรวจสอบและการถ่วงดุลตามควรเสมอ** เช่น การตรวจสอบความชอบด้วยกฎหมายโดยศาล (ได้แก่ การขอคำสั่งศาล) และสิทธิในการโต้แย้งคำสั่ง • **การพิจารณาลงโทษตามมาตรา 47 มีความไม่ชัดเจน** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า มาตรา 47 ควรกำหนดโทษที่หน่วยงานเอกชนอาจได้รับให้ชัดเจน มิใช่เพียงแค่อ้างถึงกฎหมาย ประกาศ หรือข้อบังคับอื่นใด

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
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 ซึ่งทำให้หน่วยงานเอกชนอาจต้องกลั่นกรองว่าจะดำเนินการอย่างไรกับคำสั่งต่างๆ ที่ได้รับจากเจ้าหน้าที่หลายราย โดยเฉพาะในกรณีเหตุภัยคุกคามทางไซเบอร์ที่จำเป็นต้องดำเนินการในทันที เนื่องจากการติดต่อเจ้าหน้าที่หลายรายย่อมทำให้เกิดความล่าช้าในการดำเนินการ ด้วยเหตุนี้ บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอให้มีหน่วยงานกำกับดูแลเพียงหน่วยงานเดียวที่มีอำนาจหน้าที่ในการตรวจสอบดูแลและบังคับใช้กฎหมายตามร่าง พ.ร.บ. ปี 2561 แทนการกำหนดให้หลายหน่วยงานมีอำนาจหน้าที่ดังกล่าว นอกจากนี้ อำนาจของหน่วยงานดังกล่าวต้องมีการควบคุมโดยมีกฎระเบียบที่โปร่งใสและมีกฎหมายที่กำหนดอำนาจของหน่วยงานนั้นไว้อย่างชัดเจน อีกทั้งมีการตรวจสอบโดยรัฐมนตรีและศาล
7.	**การรักษาความลับ** (มาตรา 48)	• นอกจากมาตรา 48 แล้ว ไม่มีบทบัญญัติอื่นใดในร่าง พ.ร.บ. ปี 2561 ที่กล่าวถึงเรื่องการรักษาความลับหรือการปกป้องความเป็นส่วนตัว • แม้มาตรา 48 จะกำหนดโทษสำหรับพนักงานเจ้าหน้าที่ที่เปิดเผยข้อมูลที่ได้มาโดยการใช้อำนาจของตน แต่การคุ้มครองดังกล่าวจำกัดแต่เพียงการเปิดเผยแก่บุคคลอื่น แต่ไม่ได้ห้ามการใช้ข้อมูลดังกล่าวโดยพนักงานเจ้าหน้าที่รายนั้นเองเพื่อประโยชน์ของตน	บีเอสเอและสภาธุรกิจฯ ขอเรียนว่า ร่าง พ.ร.บ. ปี 2561 ควรมีบทบัญญัติเพิ่มเติมที่ชัดเจนในเรื่องการรักษาความลับและการปกป้องข้อมูลส่วนบุคคล ซึ่งรวมถึงการกำหนดหน้าที่ที่ชัดเจนของพนักงานเจ้าหน้าที่ในการปกป้องและรักษาความลับของข้อมูลดังกล่าว รวมถึงการกำหนดหน้าที่และขั้นตอนในการขอความยินยอม และวิธีใช้ เปิดเผย เก็บ และกำจัดข้อมูลดังกล่าวเมื่อไม่จำเป็นแล้ว

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
8.	**การแบ่งปันข้อมูลข่าวสาร** (ทั่วไป)	ร่าง พ.ร.บ. ปี 2561 ไม่มีการกล่าวถึงเรื่องการแบ่งปันข้อมูลไว้อย่างชัดแจ้ง	• บีเอสเอและสภาธุรกิจฯ เห็นว่า การแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ ช่องโหว่ และเหตุทางไซเบอร์ ต่อผู้ที่ได้รับผลกระทบตลอดจนหน่วยงานอื่นๆ เพื่อป้องกันการโจมตี เป็นเรื่องที่สำคัญต่อการส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเป็นวิธีที่น่าจะมีประสิทธิภาพมากกว่าการรายงานเหตุภัยคุกคามทางไซเบอร์ • เนื่องจากเป้าหมายของการโจมตีอาจเป็นได้ทั้งภาคเอกชนและหน่วยงานของรัฐทั่วประเทศ บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอว่า ร่าง พ.ร.บ. ปี 2561 ควรสนับสนุนให้มีการจัดทำนโยบายที่มีประสิทธิภาพในเรื่องการแบ่งปันข้อมูลข่าวสารระหว่างภาครัฐและเอกชน ระหว่างหน่วยงานเอกชนด้วยกัน และระหว่างหน่วยงานของรัฐด้วยกัน • บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ร่าง พ.ร.บ. ปี 2561 และนโยบายเรื่องการแบ่งปันข้อมูลข่าวสารควรมีข้อจำกัดเกี่ยวกับความรับผิดที่หน่วยงานที่เป็นผู้แบ่งปันข้อมูลข่าวสารอาจมี โดยที่ยังคงสามารถปกป้องความเป็นส่วนตัวของผู้ที่ได้รับผลกระทบจากการแบ่งปันข้อมูลข่าวสาร อำนวยความสะดวกในการแบ่งปันข้อมูลข่าวสารหลายทาง ส่งเสริมให้ดำเนินการอย่างทันท่วงที และทำให้แน่ใจว่าข้อมูลข่าวสารที่ได้รับไปนั้นจะใช้เพื่อส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น

(คำแปล)

(กระดาษหัวจดหมายของบีเอสเอ) *(สภาธุรกิจสหรัฐอเมริกา-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] และสภาธุรกิจสหรัฐอเมริกา-อาเซียน (**สภาธุรกิจฯ**)[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, Informatica, 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 สภาธุรกิจสหรัฐอเมริกา-อาเซียนเป็นองค์กรชั้นนำที่ทำหน้าที่เป็นผู้แทนของบริษัทสหรัฐที่ดำเนินกิจการอยู่ในกลุ่มประเทศอาเซียนซึ่งเป็นประชาคมที่เติบโตขึ้นอย่างต่อเนื่อง สมาชิกของสภาธุรกิจฯ กว่า 150 ราย มีรายได้โดยรวมถึงกว่า 6 ล้านล้านดอลลาร์สหรัฐ และมีพนักงานกว่า 13 ล้านคนในทั่วโลก สมาชิกของสภาธุรกิจฯ ล้วนเป็นบริษัทสหรัฐขนาดใหญ่ที่สุดที่ดำเนินกิจการอยู่ในกลุ่มประเทศอาเซียน ซึ่งมีตั้งแต่บริษัทที่เพิ่งเข้ามายังภูมิภาคนี้ไปจนถึงบริษัทที่ดำเนินกิจการอยู่ในเอเชียตะวันออกเฉียงใต้เป็นเวลากว่า 100 ปีมาแล้ว สภาธุรกิจฯ มีสำนักงานอยู่ที่กรุงวอชิงตัน ดี.ซี., เมืองนิวยอร์ก 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. คำนึงถึงเรื่องความเสี่ยงเป็นหลัก มุ่งเน้นที่ผล และเป็นกลางทางเทคโนโลยี
3. อาศัยกลไกที่ขับเคลื่อนด้วยการตลาดหากสามารถกระทำได้
4. มีความยืดหยุ่นและสนับสนุนให้มีการพัฒนานวัตกรรม
5. ส่งเสริมให้มีการประสานความร่วมมือระหว่างภาครัฐและเอกชน และ
6. มุ่งปกป้องความเป็นส่วนตัว

2. <u>ความเห็นของภาคอุตสาหกรรม</u>

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

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้สำหรับความพยายามครั้งสำคัญที่ดำเนินการเพื่อให้แน่ใจว่าประเทศไทยมีความพร้อมที่จะระงับยับยั้งและจัดการกับภัยคุกคามไซเบอร์ เนื่องจากภัยคุกคามไซเบอร์มีความซับซ้อนและมีอันตรายขึ้นทุกวัน ความเสี่ยงที่เกิดจากนโยบายระดับประเทศที่กำหนดขึ้นอย่างไม่เพียงพอหรือไม่มีประสิทธิภาพในการรับมือกับภัยคุกคามไซเบอร์จึงอาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

ภัยคุกคามไซเบอร์โดยลักษณะแล้วเป็นเรื่องระดับโลก ดังนั้น การรับมือกับภัยคุกคามทางไซเบอร์จึงจำเป็นต้องดำเนินการในระดับโลกเช่นกัน บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและรัฐบาลไทยที่เปิดรับฟังความคิดเห็นจากภาคเอกชนและผู้มีส่วนได้เสียอื่นๆ ในการจัดทำกฎหมายนี้ และขอสนับสนุนให้ยังคงมีการเปิดโอกาสให้มีการสื่อสารและหารือกับภาคเอกชนต่อไป ซึ่งรวมถึงบริษัทระดับโลก ด้วยเหตุนี้ ทางบีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอให้กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ระบุให้ชัดเจนว่า บทบัญญัติที่กล่าวถึงการประสานความร่วมมือระหว่างภาครัฐและเอกชนนั้น (เช่น ตามมาตรา 5(4) และ มาตรา 7(5) เป็นต้น) เป็นการอนุญาตและส่งเสริมให้มีการประสานความร่วมมือกับเอกชนที่เป็นบริษัทที่ประกอบธุรกิจในหลายประเทศด้วย

บีเอสเอและสภาธุรกิจฯ ทราบและซาบซึ้งในความพยายามที่จะแก้ไขปัญหาของร่าง พ.ร.บ. ปี 2558 ตามที่ได้มีการเสนอความเห็นไว้ อย่างไรก็ดี 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. ที่มาจากหน่วยงานด้านการรักษาความปลอดภัยและความมั่นคง ทั้งนี้ เพื่อให้แน่ใจว่า ในการจัดทำกลยุทธ์หรือแผนรับมือด้านความมั่นคงปลอดภัยไซเบอร์ กปช. จะพิจารณาประเด็นเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชนในทุกมิติ

บีเอสเอและสภาธุรกิจฯ ทราบว่ามาตรา 6 แห่งร่าง พ.ร.บ. ปี 2561 ได้กำหนดให้กรรมการใน กปช. มาจากหลากหลายหน่วยงานมากขึ้น โดยมีผู้แทนจากหลายกระทรวง รวมถึงกระทรวงคมนาคม กระทรวงศึกษาธิการ และกระทรวงสาธารณสุข ซึ่งย่อมทำให้ได้มุมมองที่หลากหลายและสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผ่านการพิจารณาอย่างรอบด้านเพื่อเสนอต่อคณะรัฐมนตรีได้ อย่างไรก็ดี เนื่องจาก กปช. ไม่มีกรรมการที่จะดูแลรักษาผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชน มุมมองของ กปช. จึงยังคงเน้นไปที่ประเด็นเรื่องการบังคับใช้กฎหมายและความมั่นคง โดยมีรัฐมนตรีว่าการกระทรวงกลาโหมเป็นรองประธาน กปช.

บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า คณะทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่ควรนำโดยรัฐมนตรีว่าการกระทรวงกลาโหมแต่เพียงผู้เดียว แต่ควรให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีส่วนร่วมในการนำคณะทำงานดังกล่าวด้วย เนื่องจากภัยคุกคามทางไซเบอร์อาจส่งผลกระทบต่อผลประโยชน์ทางด้านเศรษฐกิจทั้งในระดับชาติและระดับนานาชาติได้ในวงกว้าง กปช. จึงควรมีกรรมการที่จะดูแลรักษาผลประโยชน์ของประชาชนอยู่ด้วย

บี. การมีอำนาจอย่างกว้างขวางของ กปช.

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

ในฐานะที่ กปช. เป็นศูนย์กลางในการประสานงานดังกล่าว กปช. จึงมีอำนาจอย่างกว้างขวางในการจัดการกับภัยคุกคามไซเบอร์ที่กฎหมายนี้กำหนดให้ต้องมีการดำเนินการอย่างหนึ่งอย่างใด ตัวอย่างเช่น ตามมาตรา 36 และมาตรา 37 แห่งร่าง พ.ร.บ. ปี 2561 กปช. มีอำนาจสั่งการให้หน่วยงานเอกชน[3]ดำเนินการอย่างหนึ่งอย่างใดเมื่อมีเหตุฉุกเฉินหรือภยันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ บีเอสเอและสภาธุรกิจฯ 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 ซึ่งเป็นกรณีที่ยอมรับได้ว่าหน่วยงานผู้บังคับใช้กฎหมายจะมีอำนาจอย่างกว้างขวาง ดังเช่นที่ปรากฏในร่าง พ.ร.บ. ปี 2561 ดังนั้น เพื่อให้สอดคล้องกับกฎหมายที่ใช้ในทั่วโลก บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอคำจำกัดความดังนี้
  - โครงสร้างพื้นฐานที่สำคัญ หมายความว่า **“ทรัพย์สิน บริการ และระบบ ไม่ว่าที่จับต้องได้หรือเสมือนจริง ที่หากถูกทำลาย ถูกทำให้เสียหาย หรือไม่สามารถใช้การได้เป็นระยะเวลานานแล้ว จะส่งผลกระทบในวงกว้างต่อความมั่นคงของชาติ สาธารณสุข ความปลอดภัยของประชาชน ความมั่นคงด้านเศรษฐกิจของชาติ หรือการปฏิบัติงานหลักของหน่วยงานในระดับท้องถิ่นหรือระดับชาติ”**

  ในการกำหนดว่าโครงสร้างใดเป็นโครงสร้างพื้นฐานที่สำคัญ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า กปช. ควรพิจารณาจากความสำคัญ ความจำเป็น และความเสี่ยงที่เกี่ยวข้อง

[3] “หน่วยงานเอกชน” เป็นคำที่เพิ่มคำจำกัดความเข้ามาใหม่ในมาตรา 3 ซึ่งหมายความว่า “หน่วยงานที่จัดตั้งขึ้นจากการรวมตัวของบุคคล หรือคณะบุคคลเข้าด้วยกัน ไม่ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือที่ไม่แสวงหากำไร 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 ขอเรียนเสนอว่า คำสั่งศาลไม่ควรมีผลบังคับโดยไม่จำกัดระยะเวลา เนื่องจากอาจก่อให้เกิดความไม่ชัดเจนต่อหน่วยงานเอกชน
- **ข้อยกเว้นของการขอคำสั่งศาลควรใช้ถ้อยคำที่ชัดเจน** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า กรณี “จำเป็นเร่งด่วน” ที่เป็นข้อยกเว้นดังกล่าวนั้นควรระบุให้ชัดเจนว่าต้องเป็นกรณีที่อาจก่อให้เกิดความเสียหายต่อความมั่นคงของชาติเท่านั้น
- **ควรกำหนดให้มีหน่วยงานอิสระควบคุมดูแลการใช้อำนาจของ กปช. ตามมาตรา 47** บีเอสเอและสภาธุรกิจฯ ขอเรียนย้ำว่า หน่วยงานอิสระ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เสนอให้มีการแต่งตั้งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ควรมีอำนาจในการตรวจสอบดูแลการใช้อำนาจของ กปช. ตามมาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 เพื่อให้แน่ใจว่ามีการถ่วงดุลระหว่างผลประโยชน์ของเอกชนกับความจำเป็นในการใช้อำนาจสอดส่องดูแล

อี. ความรับผิดทางอาญา

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

บีเอสเอและสภาธุรกิจฯ เห็นว่า การกำหนดโทษทางอาญาต่อหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำขอของ กปช. ตามมาตรา 47 นั้นเป็นบทลงโทษที่รุนแรงเกินควร อันอาจทำให้บริษัทต่างชาติระงับแผนที่จะเข้ามาประกอบธุรกิจในประเทศไทยหากมีความเสี่ยงว่าบุคลากรของตนจะต้องมีความรับผิดทางอาญาสำหรับการกระทำความผิดโดยไม่ได้จงใจหรือการกระทำความผิดเพียงเล็กน้อย

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

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมรัฐบาลไทยอีกครั้งสำหรับความพยายามในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดี บีเอสเอและสภาธุรกิจฯ ใคร่ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาประเด็นที่ได้เรียนเสนอไว้ข้างต้น เพื่อที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจะสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งคำนึงถึงเรื่องความเสี่ยงเป็นหลักและสอดคล้องกับแนวปฏิบัติในระดับสากล อันจะช่วยเสริมสร้างความเชื่อมั่นระหว่างภาครัฐและเอกชน และยกระดับความมั่นคงปลอดภัยของข้อมูลและโครงสร้างพื้นฐาน

บีเอสเอและสภาธุรกิจฯ ยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อโดยตรงไปที่ afeldman@usasean.org หรือที่หมายเลข 202-375-4393 หรือที่ jaredr@bsa.org หรือที่หมายเลข +65 6292 9609 หรือติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่** varuneer@bsa.org **หรือที่หมายเลข +668-1840-0591 หรือนางสาวเอลล่า ดวงแก้ว ผู้จัดการประจำประเทศไทยแห่งสภาธุรกิจสหรัฐอเมริกา-อาเซียน ที่** eduangkaew@usasean.org **หรือที่หมายเลข 202-440-3642** บีเอสเอและสภาธุรกิจฯ ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

อเล็กซานเดอร์ ซี. เฟลด์แมน
ประธานและประธานเจ้าหน้าที่บริหาร
สภาธุรกิจสหรัฐอเมริกา-อาเซียน

(ลายมือชื่อ)

เจเร็ด แร้กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย ภูมิภาคเอเชียแปซิฟิก
บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

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

ภาคผนวก

ความเห็นของบีเอสเอต่อร่าง พ.ร.บ. ปี 2558

(กระดาษหัวจดหมายของบีเอสเอ)

วันที่ 6 พฤษภาคม 2558

เป็นความลับและห้ามเผยแพร่

เลขาธิการคณะกรรมการกฤษฎีกา
สำนักงานคณะกรรมการกฤษฎีกา
ถนนพระอาทิตย์ เขตพระนคร
กรุงเทพมหานคร 10200

เรื่อง ความเห็นของบีเอสเอเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านเลขาธิการคณะกรรมการกฤษฎีกา

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (บีเอสเอ)[1] ใคร่ขอขอบพระคุณที่ท่านได้เปิดโอกาสให้มีการเสนอความเห็นต่อคณะกรรมการกฤษฎีกาเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (“**ร่าง พ.ร.บ.**”) และขอแสดงความชื่นชมในความพยายามครั้งสำคัญที่แสดงถึงความมีวิสัยทัศน์ของรัฐบาลไทยในครั้งนี้ที่ดำเนินการให้แน่ใจว่าประเทศจะมีความพร้อมในการระงับยับยั้งและจัดการกับภัยคุกคามทางไซเบอร์ อนึ่ง กลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพต้องจัดทำขึ้นบนพื้นฐานกฎหมายที่ชัดเจน เพื่อเอื้อให้มีการประสานความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมาย ภาครัฐ และภาคเอกชน ซึ่งการประสานความร่วมมือดังกล่าวย่อมต้องอาศัยความไว้เนื้อเชื่อใจกัน ซึ่งจะเกิดขึ้นได้ก็ต่อเมื่อมีมาตรการป้องกันอย่างเพียงพอและภาคเอกชนจะได้รับประโยชน์อย่างเหมาะสม ตัวอย่างเช่น ข้อกำหนดเกี่ยวกับการรักษาความปลอดภัยต้องมีความสมดุลอย่างเหมาะสมระหว่างความจำเป็นในการคุ้มครองความเป็นส่วนตัวกับเสรีภาพของประชาชน เมื่อคำนึงถึงหลักการเหล่านี้เป็นสำคัญ บีเอสเอมีความกังวลว่า บทบัญญัติของร่าง พ.ร.บ. นี้ที่ให้อำนาจในการสอดส่องดูแล

[1] บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอเป็นบริษัทต่างๆ ที่สร้างสรรค์นวัตกรรมที่ทันสมัยที่สุดของโลก ซึ่งนำเสนอโซลูชั่นซอฟต์แวร์ที่ผลักดันให้เศรษฐกิจเติบโตและปรับปรุงคุณภาพชีวิตในยุคปัจจุบัน 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 “การดำเนินการที่ทันท่วงทีและเป็นไปในทิศทางเดียวกัน” 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. นี้จึงควรต้องกำหนดไว้อย่างชัดเจนว่าเหตุการณ์ลักษณะใดที่ถือเป็นภัยคุกคามทางไซเบอร์ที่กฎหมายนี้กำหนดให้ต้องมีการดำเนินการอย่างหนึ่งอย่างใด เช่น เมื่อเกิดภัยคุกคามทางไซเบอร์ มาตรา 33 ได้ให้อำนาจแก่ กปช. ในการสั่งการให้หน่วยงานของรัฐทั้งหมดที่เกี่ยวข้องดำเนินการใดก็ตามอันจะมีผลเป็นการควบคุมหรือบรรเทาความเสียหายที่เกิดขึ้น และมาตรา 34 ได้ขยายอำนาจของ กปช. ให้สามารถสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง และให้รายงานผลการปฏิบัติการต่อ กปช. หากเป็นกรณีที่ภัยคุกคามทางไซเบอร์อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ

จะเห็นได้ว่า บทบัญญัติในมาตราข้างต้นได้ให้อำนาจแก่ กปช. ไว้อย่างกว้างขวาง แต่กฎหมายฉบับนี้กลับไม่ได้กำหนดคำจำกัดความของ “ภัยคุกคามทางไซเบอร์” ไว้อย่างชัดเจน อีกทั้งไม่ได้กำหนดหลักเกณฑ์ในการพิจารณาว่าความเสี่ยงที่เกิดขึ้นนั้นถึงขนาดที่ 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. สามารถเรียกให้หน่วยงานเอกชนดำเนินการอย่างใดอย่างหนึ่งได้ อีกทั้งควรกำหนดว่าบุคคลใดในสำนักงาน 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 เนื่องจากกฎหมายดังกล่าวกำหนดให้รัฐบาลมีดุลพินิจในการใช้อำนาจได้โดยที่ไม่ต้องมีการตรวจสอบความชอบด้วยกฎหมายโดยศาล เช่น ไม่มีบทบัญญัติใดที่กำหนดให้ต้องขอหมายศาลก่อนเข้าถึงการติดต่อสื่อสารส่วนบุคคล กฎหมายนี้เพียงแค่กำหนดว่า 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) ไม่มีมาตรการตรวจสอบและถ่วงดุลอำนาจดังกล่าวนั้นขัดกับมาตรการรักษาความเป็นส่วนตัวของข้อมูลตามกฎหมายที่ใช้บังคับอยู่ในประเทศไทยและตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 (“**พ.ร.บ. การสอบสวนคดีพิเศษ**”) มีการให้อำนาจในการเข้าถึงข้อมูลส่วนบุคคลในทำนองเดียวกันหากมีเหตุอันควรเชื่อได้ว่ามีสื่อใดที่ถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ ประการสำคัญ มาตรา 25 แห่ง พ.ร.บ. การสอบสวนคดีพิเศษดังกล่าวกำหนดให้พนักงานสอบสวนคดีพิเศษต้องยื่นคำขอฝ่ายเดียวต่อศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้ นอกจากนี้ ศาลอาจสั่งอนุญาตดังกล่าวได้คราวละไม่เกิน 90 วันเท่านั้น ในทำนองเดียวกัน ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็ได้กำหนดให้พนักงานเจ้าหน้าที่ผู้บังคับใช้กฎหมายต้องได้รับคำสั่งศาลก่อนจึงจะเรียกให้ผู้ให้บริการเปิดเผยเนื้อหาของการติดต่อสื่อสารของผู้ใช้บริการได้

จากบทบัญญัติข้างต้น มาตรา 35 (3) ของร่าง พ.ร.บ. นี้จึงควรกำหนดให้พนักงานเจ้าหน้าที่ต้องได้รับคำสั่งศาลก่อนจึงจะสามารถเข้าถึงข้อมูลส่วนบุคคลได้เช่นกัน อีกทั้งควรกำหนดให้คำสั่งอนุญาตดังกล่าวมีผลบังคับเพียงช่วงระยะเวลาหนึ่งๆ เท่านั้น นอกจากนี้ ควรกำหนดให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจตามมาตรา 35 (3) ได้เฉพาะในกรณีที่อาจเกิดความเสียหายต่อความมั่นคงของชาติเท่านั้น สุดท้ายนี้ บีเอสเอขอเรียนเสนอให้มีหน่วยงานอิสระ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เสนอให้มีการแต่งตั้งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีอำนาจตรวจสอบการใช้อำนาจของ กปช. ตามมาตรา 35 (3) เพื่อให้แน่ใจว่ามีการถ่วงดุลอย่างเพียงพอระหว่างความเป็นส่วนตัวกับความจำเป็นของการใช้อำนาจในการสอดส่องดูแล

<u>บทสรุป</u>

บีเอสเอเห็นถึงความพยายามของรัฐบาลไทยในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดี พนักงานเจ้าหน้าที่ตามกฎหมายนี้ควรกระทำการอย่างโปร่งใสและไม่ล่วงละเมิดความเป็นส่วนตัวของผู้ใช้ ไม่เช่นนั้นอาจก่อให้เกิดผลเสียต่อแผนด้านดิจิทัลเพื่อเศรษฐกิจได้ นอกจากนี้ ควรเน้นย้ำในเรื่องการให้ความร่วมมือของเอกชนในการรายงานรัฐบาลเมื่อมีการกระทำที่เป็นภัยต่อความปลอดภัยของระบบเพื่อป้องกันภัยคุกคามทางไซเบอร์เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ การที่กฎหมายนี้ให้อำนาจแก่ กปช. และ/หรือพนักงานเจ้าหน้าที่ตามกฎหมายนี้อย่างกว้างขวางอาจนำไปสู่การกระทำที่เป็นการหลอกลวง ความไม่ไว้เนื้อเชื่อใจ และทำให้เอกชนให้ความร่วมมือน้อยลงในการรายงานเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ ในขณะที่มาตรา 5(4) มาตรา 7(8) มาตรา 17(2) มาตรา 17(3) และ มาตรา 18(3) พยายามส่งเสริมให้มีการประสานความร่วมมือระหว่างภาครัฐและเอกชนในการป้องกันภัยคุกคามทางไซเบอร์ แต่ในความเป็นจริงแล้วภาคเอกชนอาจเกิดความลังเลที่จะให้ข้อมูลกับรัฐบาลด้วยเกรงว่ารัฐบาลจะเรียกขอข้อมูลที่ไม่เกี่ยวข้องหรือเข้ายุ่งเกี่ยวกับการ

ติดต่อสื่อสารส่วนบุคคลทางสื่อเทคโนโลยีสารสนเทศ ด้วยเหตุนี้ บีเอสเอจึงใคร่ขอความกรุณาให้คณะกรรมการกฤษฎีกาพิจารณาความเห็นข้างต้นอย่างถี่ถ้วนเพื่อให้เกิดความโปร่งใสและเพื่อสร้างความไว้เนื้อเชื่อใจระหว่างภาครัฐและเอกชน โดยที่ยังสามารถรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ในขณะเดียวกัน

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

ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

บุน โพ มก
ผู้อำนวยการฝ่ายนโยบาย ภูมิภาคเอเชีย-แปซิฟิก
บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง

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