สำนักงานรองนายกรัฐมนตรี
ตึกบัญชาการ ๑ ทำเนียบรัฐบาล
ถนนพิษณุโลก เขตดุสิต
กรุงเทพฯ ๑๐๓๐๐

วันที่ ๖ พฤษภาคม พ.ศ. ๒๕๕๘

สำคัญและเป็นความลับ

เรื่อง	ข้อคิดเห็นเกี่ยวกับ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
เรียน	พณ. ท่าน ดร. วิษณุ เครืองาม รองนายกรัฐมนตรี
สิ่งที่แนบมาด้วย	(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

บีเอสเอ พันธมิตรธุรกิจซอฟต์แวร์ (BSA)[1] ขอขอบคุณคณะกรรมการกฤษฎีกาเป็นอย่างยิ่งสำหรับการเปิดโอกาสให้ผู้มีส่วนเกี่ยวข้องนำเสนอข้อคิ

[1] กลุ่มพันธมิตรธุรกิจซอฟต์แวร์ หรือ บีเอสเอ (www.bsa.org) เป็นตัวแทนให้กับอุตสาหกรรมซอฟต์แวร์ทั่วโลกให้กับอุตสาหกรรมซอฟต์แวร์ทั่วโลกในการติดต่อกับรัฐบาล หรือในตลาดทั่วโลก สมาชิกของบีเอสเอเป็นบริษัทที่มีนวัตกรรมล้ำหน้ามากที่สุดหลายบริษัทของโลก ซึ่งได้สร้างระบบซอฟต์แวร์ที่กระตุ้นเศรษฐกิจและปรับปรุงชีวิตสมัยใหม่ให้ดีขึ้น บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดีซี และมีการดำเนินงานอยู่ในประเทศต่างๆ มากกว่า 60 ประเทศทั่วโลก โดยบีเอสเอเป็นผู้นำในเรื่องแผนงานในการตรวจสอบและกำกับดูแลการปฏิบัติงานซึ่งสนับสนุนการใช้ซอฟต์แวร์อย่างถูกกฎหมาย และให้ความสนับสนุนเกี่ยวกับนโยบายสาธารณะที่สร้างเสริมนวัตกรรมด้านเทคโนโลยี และผลักดันความเจริญเติบโตของเศรษฐกิจที่กิจกรรมทางเศรษฐกิจอาศัยเทคโนโลยีสารสนเทศ (Digital Economy) สมาชิกของบีเอสเอมีมากมายหลายบริษัทซึ่งรวมทั้ง 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 และ The MathWorks และ Trend Micro

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

ดเห็นเกี่ยวกับ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ("**ร่าง พรบ.**") รัฐบาลไทยควรได้รับการยกย่องสำหรับความพยายามที่จะทำให้แน่ใจว่าประเทศมีการเตรียมความพร้อมเพื่อป้องกันและจัดการภัยคุกคามต่อระบบความมั่นคงปลอดภัยบนโลกไซเบอร์ ถือเป็นความพยายามที่สำคัญและเป็นการมองการณ์ไกล ทั้งนี้ยุทธศาสตร์เพื่อรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพต้องสร้างจากฐานรากทางกฎหมายที่แข็งแกร่ง ที่จะอำนวยความสะดวกสำหรับการทำงานร่วมกันระหว่างการบังคับใช้กฎหมาย หน่วยงานของรัฐ และภาคเอกชน การทำงานร่วมกันดังกล่าวต้องการความไว้วางใจ ซึ่งเป็นไปได้ก็ต่อเมื่อมีการวางมาตรการป้องกันและสิ่งจูงใจที่เหมาะสมเท่านั้น ยกตัวอย่างเช่น ข้อกำหนดเรื่องความมั่นคงปลอดภัยต้องสมดุลกับความจำเป็นเรื่องการคุ้มครองความเป็นส่วนตัวและเสรีภาพของพลเมืองอย่างลงตัว เมื่อคำนึงถึงหลักการเหล่านี้ บีเอสเอจึงมีความกังวลว่าบทบัญญัติในเรื่องการเฝ้าระวัง (มาตรา 35) ในร่าง พรบ. อาจก่อให้เกิดผลต่อเนื่องที่ไม่ได้ตั้งใจขึ้น รวมถึงอาจทำลายความมั่นใจของผู้บริโภคต่อระบบเทคโนโลยีสารสนเทศ (ไอที) ของประเทศไทย ดังนั้นบีเอสเอขอนำเสนอข้อคิดเห็นดังปรากฏตามหนังสือฉบับนี้ เพื่อสนับสนุนการบรรลุวัตถุประสงค์ของร่าง พรบ. นี้ ได้แก่ ให้มี "การดำเนินการอย่างรวดเร็วและเป็นอันหนึ่งอันเดียวกัน" เพื่อตอบโต้กับภัยคุกคามต่อระบบความมั่นคงปลอดภัยบนโลกไซเบอร์

มาตรา 6: สมาชิกของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

จากที่กำหนดให้คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ("**กปช.**") ประกอบด้วยหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยและการป้องกันเป็นหลัก เช่น กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม กระทรวงกลาโหม และกองบังคับการปราบปรามการกระทำความผิดทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ บีเอสเอมีข้อคิดเห็นว่าเพื่อให้มุมมองต่างๆ ของ กปช. เกิดความสมดุล และเพื่อให้แน่ใจว่ามีการพิจารณาเรื่องข้อกังวลเกี่ยวกับความเป็นส่วนตัวของบุคคลและเสรีภาพของพลเมือง กปช. ควรจะประกอบด้วยกรรมการที่มาจากคณะกรรมการสิทธิมนุษยชนแห่งชาติและสำนักงานผู้ตรวจการแผ่นดินด้วย การมีกรรมการที่มีภูมิหลังหลากหลายจะทำให้แน่ใจว่าจะไม่มีกรณีการกระทบสิทธิของบุคคลธรรมดาอย่างไม่เหมาะสม

มาตรา 7 ถึงมาตรา 34: อำนาจอย่างกว้างของ กปช. ตามร่าง พรบ.

บีเอสเอสนับสนุนความคิดเรื่องที่ กปช. ทำหน้าที่ผู้อำนวยความสะดวกแบบรวมศูนย์เพื่อประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องทั้งห

มดในกรณีเกิดภัยคุกคามไซเบอร์ ตามมาตรา 7 กปช. "จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ" โดยเป็นหนึ่งในงานอื่นๆ ส่วนสำนักงาน กปช. มีหน้าที่จัดทำแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 27 และมาตรา 28 อย่างไรก็ตามเนื่องจาก กปช. ได้รับอำนาจอย่างกว้างให้ดำเนินการเกี่ยวกับแผนการรักษาความมั่นคงปลอดภัยไซเบอร์และแนวทางที่เกี่ยวข้อง จึงเป็นเรื่องสำคัญที่ร่าง พรบ. ต้องกำหนดแนวทางที่ชัดเจนว่าสิ่งใดถือเป็นภัยคุกคามทางไซเบอร์ที่พึงต้องดำเนินการจัดการ ยกตัวอย่างเช่น เมื่อเกิดภัยคุกคามทางไซเบอร์ มาตรา 33 ระบุว่า กปช. สามารถสั่งการให้หน่วยงานของรัฐทั้งหมดดำเนินการอย่างใดอย่างหนึ่งเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้น เช่นกันมาตรา 34 ให้อำนาจ กปช. สามารถสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่งและให้แจ้งผลการกระทำต่อ กปช. ในกรณีที่ภัยคุกคามดังกล่าวอาจกระทบต่อเสถียรภาพทางการเงินและการพาณิชย์หรือความมั่นคงปลอดภัยของชาติ

แม้ว่า กปช. มีอำนาจอย่างกว้างตามมาตราดังกล่าว แต่กลับไม่มีคำจำกัดความที่ชัดเจนของคำว่า "ภัยคุกคามทางไซเบอร์" อีกทั้งไม่มีจุดเริ่มต้นเพื่อกำหนดระดับความเสี่ยงหรือภัยคุกคามไซเบอร์ซึ่งจำเป็นต่อการตัดสินความมีเหตุผลของการกระทำของ กปช. ในทำนองเดียวกัน ร่าง พรบ. ขาดแนวทางสำหรับตัดสินว่าเมื่อใดที่ความเสี่ยงหรือภัยคุกคามไซเบอร์ต่อ "ความมั่นคงทางการการเงินและการพาณิชย์ หรือความมั่นคงปลอดภัยของประเทศ" มีความร้ายแรงเพียงพอที่จะเป็นเหตุผลให้ กปช. สั่งให้เอกชนกระทำการได้ ดังนั้นควรระบุคำจำกัดความที่ชัดเจนของคำต่างๆ ที่มีความหมายอย่างกว้าง ไว้ในร่าง พรบ. เพื่อที่หน่วยงานที่ได้รับผลกระทบทั้งหมดตามร่าง พรบ. จะมีความเข้าใจอย่างชัดเจนและไม่มีความคลุมเครืออีกต่อไป

มาตรา 35 (1) และ (2): การที่รัฐขอข้อมูลและการดำเนินการ

มาตรา 35 (1) ของร่าง พรบ. ให้อำนาจพนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สามารถส่งหนังสือสอบถาม หรือเรียกให้หน่วยงานของรัฐหรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบหรือให้ข้อมูล เพื่อประโยชน์ในการปฏิบัติการตามร่าง พรบ.

นอกจากนี้มาตรา 35 (2) ยังให้อำนาจพนักงานเจ้าหน้าที่ในการส่งหนังสือขอให้หน่วยงานราชการหรือหน่วยงานเอกชน "ดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช."

เพื่อไม่ให้มีการนำอำนาจอย่างกว้างนี้ไปใช้โดยมิชอบ จึงเป็นเรื่องจำเป็นอย่างยิ่งสำหรับรัฐบาลไทยที่ต้องกำหนดคำสั่งเฉพาะที่ระบุประเภทและขอบเขตของข้อมูลที่พนักงานเจ้าหน้าที่สามารถขอได้ และระบุกรณีที่สำนักงาน กปช. สามารถบังคับให้องค์กรเอกชนต้องดำเนินการอย่างใดอย่างหนึ่งโดยเฉพาะ คำสั่งเฉพาะดังกล่าวควรระบุไว้ว่าบุคคลใดในสำนักงาน กปช. ที่อาจขอข้อมูลและวางข้อจำกัดในการดำเนินการ เพื่อให้แน่ใจว่าข้อมูลที่มีความเป็นส่วนตัวที่ กปช. ได้รับนั้น ได้รับการปกป้องคุ้มครองอย่างเหมาะสม นอกจากนี้การใช้อำนาจอย่างกว้างเหล่านี้ควรถูกจำกัดไว้อย่างเข้มงวด โดยใช้กับกรณีที่ความเสี่ยงหรือภัยคุกคามไซเบอร์ต่อความมั่นคงปลอดภัยมีความเฉพาะเจาะจงและมีความเป็นไปได้เท่านั้น

มาตรา 35 (3): อำนาจการเฝ้าระวัง

มาตรา 35 (3) ให้อำนาจพนักงานเจ้าหน้าที่ของ กปช. เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารอิเล็กทรอนิกส์หรือสื่อเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ การมอบอำนาจการเฝ้าระวังอย่างกว้างในลักษณะนี้ทำให้ กปช. เข้าถึงเครือข่ายการติดต่อสื่อสารโดยปราศจากการควบคุม ด้วยเหตุนี้ยิ่งเพิ่มความกังวลเรื่องความเป็นส่วนตัวของบุคคลเป็นอย่างมาก
มาตรา 35 (3) ขาดความสมดุลที่พึงมีระหว่างความมั่นคงปลอดภัยของชาติกับความเป็นส่วนตัวของข้อมูล เนื่องจากรัฐบาลอาจใช้ดุลยพินิจของตนโดยปราศจากการพิจารณาทบทวนผ่านกระบวนการยุติธรรมทางศาล เช่น ไม่มีบทบัญญัติกำหนดให้ต้องขอหมายจากศาลก่อนจะเข้าถึงข้อมูลการติดต่อสื่อสารของภาคเอกชน มีเพียงบทบัญญัติให้พนักงานเจ้าหน้าที่เข้าถึงข้อมูลดังกล่าว หากมีหนังสืออนุญาตจากเลขาธิการสำนักงาน กปช.

จากมุมมองในเชิงพาณิชย์ มีความเป็นไปได้ที่มาตรา 35 (3) ของร่าง พรบ. จะเป็นอุปสรรคต่อการลงทุนด้านเทคโนโลยีสารสนเทศในประเทศไทย ธุรกิจใดๆ ที่ใช้ระบบเทคโนโลยีสารสนเทศอาจตกอยู่ใต้บังคับของมาตรา 35 (3) นี้ ไม่ว่าจะเป็นธุรกิจการธนาคาร การเงิน ไปจนถึงธุรกิจค้าปลีก ดังนั้นผู้ให้บริการธุรกิจเหล่านี้ไม่สามารถรับประกันได้ว่าข้อมูลส่วนบุคคล ความลับทางการค้า หรือประวัติการซื้อขายหุ้นของลูกค้าของตนจะถูกเก็บเป็นความลับได้ ด้วยเหตุนี้ธุรกิจด้านเทคโนโลยีสารสนเทศอาจปฏิเสธที่จะใช้หรือลงทุนในระบบเทคโนโลยีสารสนเทศในประเทศไทย

เรื่องนี้จะทำลายความพยายามที่จะทำให้ประเทศไทยกลายเป็นศูนย์กลางเทคโนโลยีสารสนเทศของประชาคมเศรษฐกิจอาเซียนต่อไป

การขาดการถ่วงดุลอำนาจในมาตรา 35 (3) ยังขัดแย้งกับแนวทางปฏิบัติของประเทศไทยเรื่องการรักษาความเป็นส่วนตัวของข้อมูลในกฎหมายที่มีอยู่เดิม และในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ยกตัวอย่างเช่น มาตรา 25 ของพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ("**พรบ. คดีพิเศษ**") ได้ระบุอำนาจลักษณะเดียวกันเพื่อเข้าถึงข้อมูลของบุคคล หากมีเหตุอันควรเชื่อได้ว่ามีการใช้สื่อใดเพื่อกระทำความผิดที่เป็นคดีพิเศษ ที่สำคัญมาตรา 25 ของ พรบ. คดีพิเศษกำหนดให้พนักงานสอบสวนคดีพิเศษต้องยื่นคำขอฝ่ายเดียวเพื่อขอคำสั่งศาลอาญาเพื่อจะเข้าถึงข้อมูลดังกล่าว นอกจากนี้ศาลอาจสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน เช่นเดียวกันตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ เจ้าพนักงานที่บังคับใช้กฎหมายต้องขอคำสั่งศาลเพื่อบังคับให้ตัวกลาง (Intermediaries) เปิดเผยเนื้อหาการติดต่อสื่อสารของผู้ใช้

จากข้อความข้างต้น บีเอสเอขอเสนอให้มาตรา 35 (3) ของร่าง พรบ. กำหนดให้ต้องมีคำสั่งศาลเพื่อเข้าถึงข้อมูลของเอกชน และคำสั่งดังกล่าวมีผลใช้บังคับในระยะเวลาที่จำกัดไว้เท่านั้น และควรจะมีเหตุอันควรสงสัยเกี่ยวกับภัยคุกคามทางไซเบอร์ต่อความมั่นคงปลอดภัยของชาติก่อนที่พนักงานเจ้าหน้าที่ตามร่าง พรบ. จะอาศัยอำนาจมาตรา 35 สุดท้ายนี้บีเอสเอขอเสนอให้หน่วยงานอิสระเช่นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเสนอไว้ ได้รับอำนาจในการตรวจสอบการใช้อำนาจของ กปช. ตามมาตรา 35 (3) เพื่อให้แน่ใจว่าประโยชน์ในเรื่องความเป็นส่วนตัวมีความสมดุลกับความจำเป็นในการเฝ้าระวังอย่างเพียงพอ

<u>สรุป</u>

บีเอสเอขอขอบคุณเป็นอย่างยิ่งสำหรับความพยายามของรัฐบาลไทยเพื่อปกป้องโครงสร้างพื้นฐานใดๆ จากภัยคุกคามไซเบอร์ และจากผู้ก่อการร้ายบนโลกไซเบอร์ อย่างไรก็ตามอำนาจของทางการตามร่าง พรบ. นี้ควรมีความโปร่งใสและไม่ทำลายความเป็นส่วนตัวของผู้ใช้ ซึ่งอาจจะส่งผลเสียต่อแผนเศรษฐกิจดิจิตอลได้ นอกจากนี้ควรให้ความสำคัญต่อเรื่องความร่วมมือของภาคเอกชนในการรายงานให้รัฐทราบเมื่อมีการละเมิดความมั่นคงปลอดภัยของระบบของตน เพื่อที่จะป้องกันภัยคุกคามไซเบอร์และเพื่อประโยชน์ของการรักษาความมั่นคงปลอดภัยของชาติ น่าเสียดายที่อำนาจอย่างกว้างของ กปช. และ/หรือพนักงานเจ้าหน้าที่ตามร่าง พรบ.

อาจก่อให้เกิดการฉ้อฉล ความไม่ไว้วางใจ และการลดความร่วมมือของภาคเอกชนในการรายงานเรื่องการละเมิดความมั่นคงปลอดภัยบนโลกไซเบอร์ แม้ว่าการมีมาตรา 5 (4) มาตรา 7 (8) มาตรา 17 (2) มาตรา 17 (3) และมาตรา 18 (3) ดูเหมือนจะส่งเสริมความร่วมมือกันระหว่างภาครัฐและภาคเอกชนในการป้องกันภัยคุกคามไซเบอร์ก็ตาม แต่ภาคเอกชนอาจเกิดความลังเลที่จะแบ่งปันข้อมูลให้รัฐ เนื่องจากเกรงว่ารัฐจะขอข้อมูลที่ไม่เกี่ยวข้องหรือดักจับการติดต่อสื่อสารส่วนบุคคลผ่านสื่อเทคโนโลยีสารสนเทศของตน ดังนั้น บีเอสเอใคร่ขอความกรุณาจากคณะกรรมการกฤษฎีกาโปรดพิจารณาข้อคิดเห็นข้างต้นอย่างถี่ถ้วน เพื่อความโปร่งใสและเพื่อสร้างความไว้วางใจกันระหว่างภาครัฐและภาคเอกชน พร้อมไปกับการรักษาความมั่นคงปลอดภัยไซเบอร์

บีเอสเอยินดีเข้าพบเพื่อปรึกษาหารือกับคณะกรรมการกฤษฎีกาเพิ่มเติม หากมีคำถามหรือความเห็นประการใด กรุณาติดต่อ **คุณวารุณี รัชตพัฒนากุล ผู้แทนประจำประเทศไทยของบีเอสเอ ที่** varuneer@bsa.org **หรือ** +668-1840-0591

บีเอสเอขอขอบพระคุณที่คณะกรรมการกฤษฎีกาสละเวลาให้การพิจารณามา ณ ที่นี้

ขอแสดงความนับถือ

บูน โพ มอก (Boon Poh Mok)
ผู้บริหาร ฝ่ายนโยบาย ประจำภูมิภาคเอเชียแปซิฟิก (Director, Policy, APAC)
บีเอสเอ | พันธมิตรซอฟต์แวร์ (BSA | The Software Alliance)

สำเนาส่งถึง
๑. เลขาธิการ คณะกรรมการกฤษฎีกา
๒. คุณสุรางคณา วายุภาพ ผู้อำนวยการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)