สรุปผลการรับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑

ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้จัดให้มีการรับฟังความคิดเห็นและข้อเสนอแนะต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เพื่อให้เป็นไปตามมติคณะรัฐมนตรีเมื่อวันที่ ๔ เมษายน ๒๕๖๑ เรื่อง แนวทางการจัดทำและเสนอร่างกฎหมาย ตามบทบัญญัติมาตรา ๗๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย นั้น

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงขอสรุปผลการรับฟังความคิดเห็นและข้อเสนอแนะต่อร่างพระราชบัญญัติดังกล่าว ดังนี้

๑. วิธีการในการรับฟังความคิดเห็น

ในการดำเนินการตามหลักเกณฑ์และวิธีการที่กำหนดในมติคณะรัฐมนตรีเมื่อวันที่ ๔ เมษายน ๒๕๖๐ โดยเห็นชอบให้หน่วยงานของรัฐถือปฏิบัติตามแนวทางการจัดทำและการเสนอร่างกฎหมายตามบทบัญญัติตามมาตรา ๗๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และหลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist) ในการเปิดรับฟังความคิดเห็นต่อ (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้จัดให้มีการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... โดยมีวิธีการรับฟังความคิดเห็น ดังนี้

(๑) การรับฟังความคิดเห็นผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th โดยกระทรวงฯ ได้จัดให้มีการรับฟังความคิดเห็นต่อ (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ ผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th ระหว่างวันที่ ๒๗ กันยายน ถึง ๑๒ ตุลาคม ๒๕๖๑

(๒) การจัดสัมมนารับฟังความคิดเห็นจำนวน ๓ ครั้ง ดังนี้

(๒.๑) การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๕ ตุลาคม ๒๕๕๘ เวลา ๑๔.๐๐ ถึง ๑๖.๐๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยเป็นการเชิญผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการและหน่วยงานที่เกี่ยวข้องกับระบบการให้บริการที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เข้าร่วมรับฟังสรุปสาระสำคัญของกฎหมายและแสดงความคิดเห็นต่อร่างกฎหมายดังกล่าว

(๒.๒) การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๙ ตุลาคม ๒๕๕๘ เวลา ๑๕.๐๐ ถึง ๑๗.๓๐ น. ณ วิทยาลัยป้องกันราชอาณาจักร เขตดินแดง กรุงเทพมหานคร โดยเป็นการรับฟังความคิดเห็นจากกลุ่มสายงานความมั่นคงเข้าร่วมแสดงความคิดเห็น

(๒.๓) การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๑๑ ตุลาคม ๒๕๕๘ เวลา ๑๐.๐๐ ถึง ๑๒.๓๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นการเปิดรับฟังความคิดเห็นเป็นการทั่วไป

๒. จำนวนครั้งและระยะเวลาในการรับฟังความคิดเห็น

กระทรวงฯ ได้จัดให้มีการรับฟังความคิดเห็นต่อ (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ จำนวน ๓ ครั้ง ดังนี้

๒.๑ ครั้งที่ ๑ การรับฟังความคิดเห็นผ่านทางเว็บไซต์ www.lawamendment.go.th ระหว่างวันที่ ๒๗ กันยายน ถึง ๑๒ ตุลาคม ๒๕๖๑ รวม ๑๕ วัน

๒.๒ ครั้งที่ ๒ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๕ ตุลาคม ๒๕๕๘ เวลา ๑๔.๐๐ ถึง ๑๖.๐๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๒.๓ ครั้งที่ ๓ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๙ ตุลาคม ๒๕๕๘ เวลา ๑๕.๐๐ ถึง ๑๗.๓๐ น. ณ วิทยาลัยป้องกันราชอาณาจักร เขตดินแดง กรุงเทพมหานคร

๒.๔ ครั้งที่ ๔ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๑๑ ตุลาคม ๒๕๕๘ เวลา ๑๐.๐๐ ถึง ๑๒.๓๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๓. พื้นที่หรือกลุ่มเป้าหมายในการรับฟังความคิดเห็น

๓.๑ การรับฟังความคิดเห็นผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th โดยกระทรวงฯ ได้จัดให้มีการรับฟังความคิดเห็นต่อ (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ ผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th ในระหว่างวันที่ ๒๗ กันยายน ถึง ๑๒ ตุลาคม ๒๕๖๑ โดยกระทรวงฯ ได้เปิดให้มีการรับฟังความคิดเห็นเป็นการทั่วไปซึ่งมีผู้เข้าร่วมแสดงความคิดเห็น ๑๓ ราย

๓.๒ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๕ ตุลาคม ๒๕๕๘ เวลา ๑๔.๐๐ ถึง ๑๖.๐๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยเป็นการเชิญผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการและหน่วยงานที่เกี่ยวข้องกับระบบการให้บริการที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) เข้าร่วมรับฟังสรุปสาระสำคัญของกฎหมายและแสดงความคิดเห็นต่อร่างกฎหมายดังกล่าว โดยมีผู้เข้าร่วมสัมมนาทั้งสิ้น ๑๒๘ คน

๓.๓ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๙ ตุลาคม ๒๕๕๘ เวลา ๑๕.๐๐ ถึง ๑๗.๓๐ น. ณ วิทยาลัยป้องกันราชอาณาจักร เขตดินแดง กรุงเทพมหานคร โดยเป็นการรับฟังความคิดเห็นจากกลุ่มสายงานความมั่นคงเข้าร่วมแสดงความคิดเห็น จำนวน ๒๕ คน

๓.๔ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๑๑ ตุลาคม ๒๕๕๘ เวลา ๑๐.๐๐ ถึง ๑๒.๓๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นการเปิดรับฟังความคิดเห็นเป็นการทั่วไป โดยมีผู้แทนหน่วยงานภาครัฐ ภาคเอกชน ภาควิชาการ สื่อมวลชน และภาคประชาชน เข้าร่วมรับฟังความคิดเห็นจำนวน ๑๒๑ คน

๔. ประเด็นที่มีการแสดงความคิดเห็น

จากการที่กระทรวงฯ ได้จัดให้มีการรับฟังความคิดเห็นต่อ (ร่าง) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ ผ่านทางเว็บไซต์ และโดยการจัดสัมมนารับฟังความคิดเห็น รวมทั้งสิ้นจำนวน ๔ ครั้ง นั้น สามารถสรุปประเด็นความเห็นในภาพรวมได้ ดังนี้

(๑) หลักการและเหตุผล

ควรกำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์ครอบคลุมกว้างที่กำหนดไว้ในกฎหมาย ไม่ใช่เฉพาะความมั่นคงของรัฐและความสงบเรียบร้อยของประเทศ

(๒) ความทับซ้อนหรือขัดแย้งกับกฎหมายอื่น

ร่างกฎหมายนี้มีการทับซ้อนหรือมีผลยกเว้นกฎหมายอื่นหรือไม่ เช่น ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(๓) การเริ่มมีผลบังคับใช้ของกฎหมาย

ไม่ควรให้มีผลบังคับใช้ทันที อย่างน้อยควรเว้นระยะเวลา ๑๘๐ วัน นับแต่วันประกาศในราชกิจจานุเบกษา อย่างไรก็ดี ยังมีความเห็นเพิ่มเติมว่ากำหนดน้อยเกินไปหรือไม่ เนื่องจากหน่วยงานอาจเตรียมตัวไม่ทัน

(๔) การรักษาความมั่นคงปลอดภัยไซเบอร์

ร่างกฎหมายนี้มีความทับซ้อนกับกฎหมายเรื่องอื่นหรือไม่ โดยเฉพาะอย่างยิ่งในเชิงการทำงานที่อาจมีความซ้ำซ้อนกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(๕) คำนิยาม

บางความเห็นต้องการให้ตัดคำบางคำออกในนิยามคำว่า “ทรัพย์สินสารสนเทศ” เช่น ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ เพื่อไม่ให้ร่างกฎหมายนี้รวมถึงการกำกับดูแลเนื้อหา

บางความเห็นต้องการให้เน้นที่โครงข่ายหรือระบบโทรคมนาคมเป็นหลัก

(๖) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.)

ควรพิจารณาทบทวนองค์ประกอบของคณะกรรมการเพื่อให้มีความรอบด้าน

(๗) หน่วยงานกำกับดูแล

เนื่องจากเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ในบางกลุ่มธุรกิจมีหน่วยงานกำกับดูแลที่ให้ความสำคัญหรือกำหนดกฎเกณฑ์ในเรื่องนี้อยู่แล้ว ซึ่งอาจมีการขัดหรือแย้งกับคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ ดังนั้น จึงควรกำหนดเรื่องนี้ให้ชัดเจน

นอกจากนี้ ร่างกฎหมายนี้เน้นที่การดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) จึงมีความห่วงกังกลว่า การทำงานของคณะกรรมการฯ จะมีความทับซ้อนกับหน่วยงานอื่นหรือไม่

(๘) การทำงานด้านการประสานงาน

เนื่องจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Computer Emergency Response Team : CERT) ของประเทศไทย มีด้วยกันหลาย CERT เช่น National CERT ของ สพธอ. หรือ Sector-based CERT ในแต่ละกลุ่มบริการ เช่น ธนาคารหรือสถาบันการเงินซึ่งมี CERT ของกลุ่มเอง จึงมีความกังวลว่าจะมีความทับซ้อนในการทำงานระหว่างกันหรือไม่

(๙) การรายงานเหตุภัยคุกคาม

เนื่องจากมีประเด็นเรื่องการรายงานให้แก่หลายหน่วยงาน เช่น กลุ่มธนาคาร โดยหน้าที่หลักต้องรายงานไปยัง ธปท. ซึ่งเป็นหน่วยงานกำกับดูแล และยังต้องรายงานไปยัง กปช. ตามร่างกฎหมายนี้ จึงควรกำหนดมาตรการที่ไม่ก่อให้เกิดภาระให้กับหน่วยงานที่มีหน้าที่ต้องรายงาน และในการรายงานเหตุภัยคุกคามไซเบอร์ ควรมีการกำหนดแนวทางการรายงานร่วมกับหน่วยงานกำกับดูแลอื่น

มีการเสนอให้ใช้ “Data flow configuration” ในขั้นตอนการรายงานเหตุภัยคุกคามทางไซเบอร์ ซึ่งเข้าใจว่าผู้เสนอประสงค์จะให้รูปแบบการทำงานต้องเสนอข้อมูลเกี่ยวกับการปรับแต่งระบบหรือการตั้งค่าของระบบเพื่อให้บริหารจัดการง่ายสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๐) โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

มีประเด็นว่าโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) หมายถึงหน่วยงานใดบ้าง จึงควรมีการกำหนดให้ชัดเจน

(๑๑) การรับมือภัยคุกคามทางไซเบอร์

เสนอให้ตัดคำว่า “คาดว่าน่าจะเกิด” เนื่องจากเปิดช่องให้มีการใช้ดุลพินิจและอำนาจอย่างกว้างขวาง ซึ่งมีการเสนอให้ใช้คำว่า “มีเหตุอันควรเชื่อได้ว่า” แทน เพื่อให้มีความชัดเจนมากขึ้น

ทั้งนี้ สามารถสรุปประเด็นจากการรับฟังความคิดเห็นในแต่ละครั้งได้ดังนี้

๔.๑ การรับฟังความคิดเห็นผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th ในระหว่างวันที่ ๒๗ กันยายน ถึง ๑๒ ตุลาคม ๒๕๖๑

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๑	ประเด็นหลักการของกฎหมาย	● ขอบเขตของกฎหมายนี้มีลักษณะคล้ายกับเป็นการกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอยู่ในตัว ซึ่งหน่วยงานดังกล่าวอาจเป็นหน่วยงานที่อยู่ภายใต้การกำกับดูแลของหน่วยงานอื่น	ในการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติตามร่างกฎหมายนี้

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		อยู่แล้ว นอกจากนี้ การใช้อำนาจของพนักงานเจ้าหน้าที่มีลักษณะเช่นเดียวกันกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงมีข้อพิจารณาว่าจะทำให้เกิดความซ้ำซ้อนหรือไม่	ครอบคลุมการดูแลในมิติทางเศรษฐกิจร่วมด้วย ประกอบกับในการทำงานต้องทำร่วมกับหน่วยงานต่างๆ ที่เกี่ยวข้อง รวมถึงสภาความมั่นคงแห่งชาติ ดังนั้น หลักการของร่างกฎหมายจึงไม่ได้ซ้ำซ้อนกับกฎหมายที่มีอยู่
๒.	ความไม่ชัดเจนของถ้อยคำในกฎหมาย	● ถ้อยคำในกฎหมายส่วนใหญ่ ยังขาดความชัดเจนอันจะก่อให้เกิดปัญหาการตีความ และทำให้ผู้ปฏิบัติไม่สามารถปฏิบัติได้อย่างถูกต้อง ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง, อย่างมีนัยสำคัญ, ที่สำคัญ, มีจำนวนมาก, ผู้ดูแลระบบ ดังนั้น ในหลายกรณีที่ปรากฏความไม่ชัดเจนในร่างกฎหมายฉบับนี้ ควรมีการกำหนดประกาศ หรือหลักเกณฑ์ที่มีขอบเขตและความชัดเจนเพื่อให้ผู้ที่ต้องปฏิบัติตามกฎหมายสามารถดำเนินการไปได้อย่างราบรื่น	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ
๓.	องค์ประกอบคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ	● ควรมีเลขาธิการสนง.คณะกรรมการสิทธิมนุษยชนแห่งชาติ และผู้ตรวจการแผ่นดิน เข้าร่วมเป็นกรรมการ เพื่อเป็นหลักประกันการพิจารณาเรื่องสิทธิและเสรีภาพส่วนบุคคล ● เนื่องจากการดำเนินกิจการบางอย่างภายใต้ขอบเขตของกฎหมายฉบับนี้เป็นการดำเนินการโดยเอกชนแต่ฝ่ายเดียว จึงควรมีต้วแทนจากภาคเอกชนเข้าร่วมในคณะกรรมการดังกล่าวด้วย	กระทรวงฯ จะได้รับความเห็น/ข้อเสนอแนะดังกล่าวมาประกอบการพิจารณาร่างพระราชบัญญัติฯ ต่อไป ทั้งนี้ สำหรับตัวแทนภาคเอกชนสามารถเข้ามาเป็นคณะกรรมการได้โดยช่องทางของการแต่งตั้งกรรมการผู้ทรงคุณวุฒิ
๔.	หน้าที่และอำนาจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	● การจัดทำนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ควรจัดให้มีการรับฟังความคิดเห็นด้วย รวมถึงควรเปิดเผยและสร้างความเข้าใจในแผนดังกล่าวต่อสาธารณะ	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๕.	โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	● กรณีที่มีข้อโต้แย้งเกี่ยวหน่วยงานที่จะถือเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ควรให้ กปช. เป็นผู้วินิจฉัยชี้ขาด ● เรื่องการขอข้อมูลจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีข้อสังเกตเกี่ยวกับข้อยกเว้นตามความในมาตรา ๔๖ วรรคสอง ว่า เรื่องสัญญาส่วนมากจะมีเรื่องการรักษาความลับของลูกค้า ทรัพย์สินทางปัญญา และเรื่อง privacy ซึ่งการเขียนห้ามยกเอาหน้าที่ตามกฎหมายหรือตามสัญญาขึ้นอ้างเพื่อไม่เปิดเผยข้อมูลเท่ากับว่ากฎหมายนี้ยกเว้นกฎหมายอื่นทั้งหมด ● การขอข้อมูลโครงสร้างของระบบควรผ่านกระบวนการตรวจสอบโดยศาล และควรดำเนินการเฉพาะเท่าที่จำเป็นและตามสมควรแก่กรณี ● การประเมินความเสี่ยงตามมาตรา ๔๘ เปิดโอกาสให้เลขาธิการฯ ใช้ดุลพินิจได้อย่างกว้างขวาง เนื่องจากกำหนดว่า หากการประเมินความเสี่ยง “ไม่เป็นที่น่าพอใจ” เลขาธิการฯ อาจมีคำสั่งให้ดำเนินการใหม่ได้ จึงควรมีการกำหนดกรอบและหลักเกณฑ์ที่มีความชัดเจน ● การได้ไปซึ่งข้อมูลโครงสร้างการทำงานของระบบคอมพิวเตอร์นั้น ยังขาดบทกำกับหน้าที่และความรับผิดของพนักงานเจ้าหน้าที่และสำนักงานที่ได้ไปซึ่งข้อมูลดังกล่าว	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ
๖.	การรายงานเหตุภัยคุกคามของหน่วยงานเอกชน	● จะทราบได้อย่างไรว่าเมื่อใดจึงจะถือว่าเป็นภัยคุกคามทางไซเบอร์อย่างร้ายแรง แม้ในร่างกฎหมายจะกำหนดลักษณะของคำว่า ร้ายแรง ไว้ แต่ก็ยังขาดความชัดเจนพอที่จะทำให้เข้าใจได้ อันจะส่งผลต่อการดำเนินการตามภาระหน้าที่ที่กฎหมายกำหนด	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		● การรายงานเหตุภัยคุกคาม ควรมีรูปแบบและวิธีการที่ชัดเจน ● จำเป็นต้องรายงานเหตุในทุกกรณีหรือไม่ เนื่องจากโดยปกติ การโจมตีทั่วไปๆ สามารถเกิดขึ้นได้ทุกวันและเกิดซ้ำๆ เป็นประจำ หากว่าการโจมตีเยอะมากและมีลักษณะเดียวกันทุกวันจะต้องรายงานอย่างไร	
๗.	การใช้อำนาจของพนักงานเจ้าหน้าที่	● มาตรา ๕๗ ให้อำนาจเลขาธิการในการหยุดการใช้งานระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วน และในมาตรา ๕๘ ให้อำนาจเลขาธิการให้ทำการหรือสั่งให้พนักงานเจ้าหน้าที่ทำการยึดคอมพิวเตอร์หรืออุปกรณ์ใดๆ ที่มีเหตุอันควรว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์แม้จะมีการจ่ายค่าชดเชย หากมีค่าจำกัดสูงสุดก็มีความเสี่ยงที่ค่าชดเชยนั้นจะน้อยเกินไปสำหรับผลกระทบทางเศรษฐกิจของผู้ประกอบการ นอกจากนี้ ยังส่งผลเรื่องความไม่เชื่อใจจากผู้ใช้และผู้ลงทุนต่างประเทศในความเป็นส่วนตัว ดังนั้น จึงควรพิจารณาอย่างรอบคอบว่ามีอุปกรณ์หรือกระบวนการใดบ้างที่ควรเป็น "ที่พึ่งสุดท้าย" ในกรณีเร่งด่วนและสำคัญที่สุดใน และมีอุปกรณ์หรือกระบวนการใดบ้างที่ควรเป็นวิธีการแรกๆ ที่ถูกใช้ที่จะไม่ก่อให้เกิดปัญหาความเสียหายของอุปกรณ์และข้อมูล หรือความเสียหายต่อภาพลักษณ์และเศรษฐกิจ ● มีวิธีการใดที่จะทำให้มั่นใจว่าเลขาธิการหรือพนักงานเจ้าหน้าที่ที่ได้รับอำนาจจากมาตรา ๕๗ และ ๕๘ ไม่นำอำนาจนี้มาใช้เพื่อค้นข้อมูลหรือบังคับการกระทำใดๆ โดยมิชอบ หรือเพื่อผลประโยชน์นอกเหนือจากการปกป้องสังคมและประเทศจากภัยคุกคามทางไซเบอร์ที่แท้จริงหรือไม่	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		● มีข้อเสนอให้แก้ไขเพิ่มเติมโดยขอให้เพิ่มวรรคสาม(วรรคท้าย)ว่า “การดำเนินของเลขาธิการตามวรรคหนึ่ง ต้องรายงานให้คณะกรรมการ กปช.ทราบโดยเร็ว” เพื่อให้คณะกรรมการ กปช. รับทราบถึงการใช้อำนาจของ เลขาธิการ และเป็นการตรวจสอบโดยคณะกรรมการกปช.ถึงการใช้ดุลยพินิจของเลขาธิการฯ ● ควรกำหนดลักษณะหรือรูปแบบของการกระทำความผิดที่เข้าข่ายต่อการกระทำความผิดหรือมีผลต่อความมั่นคงของประเทศเพื่อให้เจ้าหน้าที่ร้องขอต่อศาลเพื่อให้ได้หมายศาลก่อน แล้วจึงเจ้าไปตรวจสอบคอมพิวเตอร์ของผู้สงสัยได้ ● การปฏิบัติงานของพนักงานเจ้าหน้าที่แม้จะกำหนดให้มีบัตรประจำตัวและต้องแสดงบัตรในการปฏิบัติหน้าที่ แต่จะทราบได้อย่างไรว่าเป็นพนักงานเจ้าหน้าที่ตามกฎหมายจริง ควรกำหนดให้มีช่องทางในการตรวจสอบหรือยืนยันตัวบุคคลได้	

๔.๒ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๕ ตุลาคม ๒๕๕๘ เวลา ๑๔.๐๐ ถึง ๑๖.๐๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยเป็นการเชิญผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการและหน่วยงานที่เกี่ยวข้องกับระบบการให้บริการที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) เข้าร่วมรับฟังสรุปสาระสำคัญของกฎหมายและแสดงความคิดเห็นต่อร่างกฎหมายดังกล่าว

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๑	การมีผลบังคับใช้ของกฎหมาย	● ร่างกฎหมายฉบับนี้กำหนดหน้าที่ให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ต้องดำเนินการในหลายสิ่ง จึงควรเว้นระยะเวลาให้หน่วยงานต่างๆ ได้เตรียมตัว เตรียมความพร้อมสำหรับการปฏิบัติตามกฎหมาย ไม่ควรให้กฎหมายมีผลบังคับใช้ทันที	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๒.	องค์ประกอบของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	● องค์ประกอบของ กปช. ยังขาดผู้เกี่ยวข้องที่เป็นส่วนกลางน้ำของกระบวนการยุติธรรม จึงเสนอให้เพิ่มเติม (๑) อัยการสูงสุด (๒) เลขาธิการสำนักงานศาลยุติธรรม เข้าเป็นองค์ประกอบในคณะกรรมการระดับชาติด้วย ● ไม่ปรากฏองค์ประกอบของ DSI และศูนย์ไซเบอร์ทางทหาร ก.กลาโหม	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ
๓	บทบาทและการทำงานของศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (CERT)	● การกำหนดหน้าที่เรื่อง CERT ซึ่งจะทำงานประสานกันระหว่าง National CERT กับ Sector CERT นั้น ควรมีการกำหนดกลไกอำนาจหน้าที่ ของทั้งสองฝ่ายไว้ในกฎหมายด้วย ● นอกจากนี้ ปัจจุบันในบาง sector มี CERT แล้ว และมีประสิทธิภาพในการทำงานด้วย แต่ไม่มีการพูดถึงในกฎหมายนี้ แนวทางของรัฐมีแนวทางในการประสานงานกับ CERT และ Sector CERT อย่างไร เพราะเอกชนนั้นมีภาระต้องใช้งบประมาณในการเตรียมตัวรวมถึงการวางแผนการทำงาน ● รัฐมีแนวทางในการส่งเสริมสนับสนุน Sector CERT อย่างไร	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ
๔.	การจัดทำนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์	● ในการกำหนดนโยบายและแผนซึ่งร่างมาตรา ๙ (๓) และมาตรา ๓๘ กำหนดให้ กปช. กำหนดแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นข้อกำหนดขั้นต่ำสำหรับหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีขอเสนอว่าอาจกำหนดเพิ่มเติมในเรื่องดังนี้ ○ ควรกำหนดอุปกรณ์และเครื่องมือขั้นต่ำที่หน่วยงานควรต้องมี เพื่อให้สำนักงานสามารถนำไปกำหนดนโยบายและงบประมาณเพื่อรับการจัดสรรเงินได้ ทั้งนี้ ควรเพิ่มเติมเรื่องดังกล่าวไว้ใน มาตรา ๙ (๖) และเพิ่มไว้ในคำนิยาม “ทรัพย์สินสารสนเทศ” ด้วย	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		○ ควรกำหนดมาตรฐานการทำงานและต้องมีการอบรมพนักงานเจ้าหน้าที่ของหน่วยงาน ○ ควรกำหนดให้หน่วยงานทำการ encrypt ข้อมูล ● การตรวจสอบและการประเมินความเสี่ยงตามร่างมาตรา ๓๘ มีการกำหนดมาตรฐานของผู้ตรวจสอบหรือไม่ ● การรับฟังความคิดเห็นในการจัดทำนโยบายและแผน ตามมาตรา ๓๗ ถ้ารัฐมองว่าเป็นเรื่องกระทบหลายภาคส่วน ก็ควรเปิดให้รับฟังความคิดเห็นสาธารณะไม่น้อยกว่า ๓๐ วัน	
๕.	การบริหารจัดการ	● การบริหารจัดการ ม.๓๙ หน่วยงานของรัฐมีหน้าที่ต้องทำตนให้เท่ากับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งในทางปฏิบัติหน่วยงานรัฐบางแห่งอาจมีการบริการที่ไม่จำเป็นต้องดูแลเข้มข้นในทำนองเดียวกันก็เป็นได้ แต่กลับปรากฏว่าเรื่องของการรับมือหน่วยงานรัฐกลับมีโทษเท่ากับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ● การกำหนด Point of Contact ตามมาตรา ๔๐ ควรกำหนดจำนวนเจ้าหน้าที่เพื่อให้องค์กรเกิดความตระหนัก	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ
๖.	โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	● ผู้แทนสำนักงาน กลต. เห็นว่าการกำหนดกลุ่มภารกิจหรือการให้บริการที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในมาตรา ๔๓ (๓) ด้านการเงินการธนาคาร ถ้อยคำยังไม่ครอบคลุม ตลาดทุน และ ประกัน จึงเสนอให้ใช้คำว่า "ภาคการเงิน" ซึ่งจะกว้างและครอบคลุมมากกว่า (Financial Sector ประกอบด้วย ๓ ส่วน การเงินและการธนาคาร ตลาดทุน ประกัน จึงกังวลว่าจะไม่ครอบคลุม ตลาดทุน และ ประกัน)	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		● มาตรา ๔๕ ที่กำหนดให้มีการแจ้งรายชื่อ “ผู้ดูแลระบบ” นั้น ยังขาดความชัดเจนว่าหมายถึงบุคลากรในระดับใดขององค์กร เพราะแม้จะกำหนดว่า ผู้ดูแลระบบอย่างน้อยต้องเป็นบุคคลผู้ซึ่งรับผิดชอบในการบริหารงาน แต่ในองค์กรขนาดใหญ่มีผู้บริหารหลายระดับ จึงมีการเสนอให้มีช่องทางการติดต่อมากกว่า ๑ ช่องทาง โดยให้มีทั้งระดับบริหาร และ ระดับปฏิบัติการ ● ตามมาตรา ๔๖ การขอข้อมูลการออกแบบหรือข้อมูลการทำงานของระบบ o การขอข้อมูลค่อนข้างกว้างและข้อมูลดังกล่าวเป็นเรื่องที่มีความอ่อนไหวอย่างมาก ซึ่งควรมีกระบวนการในการดูแลข้อมูล และกำหนดความรับผิดของพนักงานเจ้าหน้าที่ที่ได้รับข้อมูลนั้นไป o นอกจากนี้ข้อยกเว้นตามความในวรรคสอง มีข้อสังเกตว่า เรื่องสัญญาส่วนมากจะมีเรื่องการรักษาความลับของลูกค้า ทรัพย์สินทางปัญญา และเรื่อง privacy ซึ่งการเขียนห้ามยกเอาหน้าที่ตามกฎหมายหรือตามสัญญาขึ้นอ้างเพื่อไม่เปิดเผยข้อมูลเท่ากับว่ากฎหมายนี้ยกเว้นกฎหมายอื่นทั้งหมด	
๗.	การใช้อำนาจหน้าที่เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์	● การใช้อำนาจในการออกคำสั่ง หรือเพื่อการปฏิบัติการต่างๆ ตามมาตรา๕๗, ๕๘ ควรมีกระบวนการกลั่นกรองความเหมาะสมและจำเป็น โดยควรให้ศาลเป็นผู้ตรวจสอบการใช้อำนาจ จึงควรขอหมายศาลก่อนการดำเนินการ ทั้งนี้ เนื่องจากเป็นการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ จึงควรดำเนินการที่ “ศาลอาญา” ● ตามร่างกฎหมายฉบับนี้พนักงานเจ้าหน้าที่มีอำนาจในการขอและเข้าถึงข้อมูล ซึ่งไม่ปรากฏว่ามีการกำหนดหน้าที่และความรับผิดของพนักงานเจ้าหน้าที่ในการดูแลข้อมูล	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		ที่ได้มาแต่อย่างใด นอกจากนี้ หากเกิด data breach กับข้อมูลที่ได้มา ความรับผิดชอบจะตกกับใคร ซึ่งรับผิดตามประมวลกฎหมายอาญา อาจจะไม่เพียงพอสำหรับกรณีความรับผิดของพนักงานเจ้าหน้าที่ เนื่องจากความเสียหายที่เกิดขึ้นอาจจะสูงมาก ยกตัวอย่าง เช่น พ.ร.บ.โรคติดต่อฯ หากเจ้าหน้าที่ขอข้อมูลโรคติดต่อได้ เมื่อได้มาแล้วรั่วไหล ก็เป็นความรับผิดชอบของพนักงานเจ้าหน้าที่ ● การแสดงตัวพนักงานเจ้าหน้าที่ จะรู้ได้อย่างไรว่าเป็นพนักงานเจ้าหน้าที่จริง แล้วหากบุคคลดังกล่าวเข้าไปทำอะไรสักอย่างที่ก่อให้เกิดความเสียหาย จะทำอย่างไร จะมีกระบวนการตรวจสอบได้อย่างไรว่าเป็นพนักงานเจ้าหน้าที่จริง ● การเรียกให้ส่งข้อมูล ควรมีการกำหนดมาตรการการจัดเก็บ ระยะเวลาในการจัดเก็บ กระบวนการทำลายข้อมูล มาตรการป้องกันการรั่วไหล การรักษาความลับของข้อมูล และเปิดโอกาสให้ชี้แจงในกรณีที่ไม่สามารถส่งข้อมูลให้ได้	
๘.	การรับมือภัยคุกคาม และบทลงโทษ	● กรณีที่กำหนดให้เป็นหน้าที่หน่วยงานต้องทำแผนปฏิบัติการ และดำเนินการป้องกันรับมือ และ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งหากมีข้อติดขัดหรืออุปสรรคอาจร้องขอความช่วยเหลือไปยังสำนักงานได้นั้น หากปรากฏว่าหน่วยงานทำเต็มที่ตามความสามารถที่มีแล้วและร้องขอความช่วยเหลือไปยังสำนักงาน แต่ปรากฏว่าก็ยังโดนโจมตีหรือมีภัยคุกคามเกิดขึ้น เช่นนี้จะต้องรับผิดอย่างไร ควรจะต้องให้สำนักงานแชร์ความรับผิดด้วยหรือไม่ ● ความรับผิดกรณีไม่แจ้งเหตุภัยคุกคามทางไซเบอร์ ○ จะรู้ได้อย่างไรว่าเป็นภัยคุกคามทางไซเบอร์ และอย่างไรจะถือว่าร้ายแรง	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		จะระบุได้อย่างไรว่าระดับไหนต้องแจ้ง ระดับไหนไม่ต้องแจ้ง o หากสามารถป้องกันเหตุภัยคุกคามทางไซเบอร์ได้ ยังมีหน้าที่ต้องรายงานอีกหรือไม่ o ควรกำหนดแบบรายงาน ● การกำหนดบทลงโทษ ควรพิจารณาความพร้อมของหน่วยงานด้วย เนื่องจากเรื่องนี้ถือเป็นเรื่องใหม่และต้องให้เวลาในการปรับตัว ซึ่งแต่ละหน่วยงานมีความสามารถและความรู้ความเข้าใจไม่เท่าเทียมกัน ● การกำหนดผู้ต้องรับโทษ ในร่างกฎหมายประกอบด้วยคำว่า “ผู้ดูแลระบบ / หน่วยงาน / เจ้าของ / ผู้ครอบครอง / ผู้ใช้” ซึ่งในบางกรณียังขาดความชัดเจน ดังนั้นจึงควรกำหนดตัวบุคคลผู้ที่ต้องรับผิดให้ชัดเจน o ความรับผิดควรรับผิดเฉพาะในกรณีที่เป็นการกระทำโดยจงใจหรือประมาทเลินเล่อเท่านั้น หากได้ดำเนินการตามที่กฎหมายกำหนดแล้ว แต่ก็ยังไม่สามารถป้องกันได้ เช่นนี้ไม่ควรจะต้องรับโทษ	

๔.๓ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๙ ตุลาคม ๒๕๕๘ เวลา ๑๕.๐๐ ถึง ๑๗.๓๐ น. ณ วิทยาลัยป้องกันราชอาณาจักร เขตดินแดง กรุงเทพมหานคร โดยเป็นการรับฟังความคิดเห็นจากกลุ่มสายงานความมั่นคงเข้าร่วมแสดงความคิดเห็น

ลำดับ	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๑.	**กองทัพบก** (๑) ตามมาตรา ๓ “การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์” ขอเสนอแนะให้เพิ่มคำว่า เฝ้าระวังภัยคุกคามทางไซเบอร์ด้วย	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกต

ลำดับ	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
	(๒) ขอเสนอแนะว่า คำนิยามคำว่า ไซเบอร์ ให้รวมถึงวิธีการทางอิเล็กทรอนิกส์ด้วย เพราะตามมาตรา ๓ บัญญัติว่า“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือเหตุการณ์ที่กระทำด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์	ประกอบการพิจารณาร่างพระราชบัญญัติฯ
๒.	**กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร** (๑) ตามมาตรา ๕ “ให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า“กปช.”และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cybersecurity Committee”เรียกโดยย่อว่า “NCSC” ประกอบด้วยนายกรัฐมนตรี เป็นประธานกรรมการ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงยุติธรรม ผู้บัญชาการตารวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย....” จึงมีข้อเสนอแนะว่า เนื่องจากกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรมีหน้าที่ในเรื่องยุทธศาสตร์ชาติ ซึ่งในยุทธศาสตร์ชาติก็มีเรื่อง cyber security ด้วย จึงประสงค์จะขอร่วมในคณะกรรมการโดยตำแหน่งด้วย นอกจากนี้คณะกรรมการโดยตำแหน่ง ๖ ท่านนี้ เสนอแนะให้พิจารณาใหม่ให้รอบคอบ โดยทุกส่วนราชการที่เกี่ยวข้อง ควรเพิ่มเข้ามาในคณะกรรมการโดยตำแหน่งตามมาตรานี้ด้วย (๒) ขอเสนอแนะให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติควรใช้อำนาจผ่านทางคณะอนุกรรมการโดยคณะอนุกรรมการจะเป็นผู้ทำงานในรายละเอียด และคณะกรรมการทำหน้าที่เป็นผู้กำกับดูแล	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ
๓.	**กองบัญชาการกองทัพไทย** (๑) ตามมาตรา ๙ (๒) “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” หรือ “กปช.” มีหน้าที่และอำนาจ จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงานเพื่อเสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ นั้น เห็นว่า ต้องมีกรอบการทำงานก่อนที่จะมียุทธศาสตร์ แผนแม่บท แผนงาน ต้องหากรอบ	สำหรับประเด็นเรื่องกรอบการมาตรฐานนั้น ในร่างในมาตรา ๓๖ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... นี้กำหนดว่า การดำเนินการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรประกอบด้วยหลักอย่างน้อย ๘ ด้าน ซึ่งยังสามารถเพิ่มเติมเรื่องอื่นๆ ที่จำเป็นได้

ลำดับ	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
	การทำงานด้าน Cyber เพื่อให้สอดคล้องกับยุทธศาสตร์ชาติ แล้วจึงตรากฎหมายรองรับสิ่งเหล่านี้ จะได้เป็นเรื่องเดียวกัน (๒) ในร่างมาตรา ๔๖ ในการขอข้อมูล เห็นว่า กองบัญชาการกองทัพไทย ไม่อาจให้ข้อมูลได้ เนื่องจากเป็นข้อมูลด้านความปลอดภัยและความลับระดับชาติ ดังนั้น หากจะขอข้อมูลอะไร ควรยกเว้นข้อมูลของกระทรวงกลาโหม เนื่องจากกองทัพไทยได้ดำเนินการด้านนี้มาแล้ว ๒ ปี จึงมีความเชี่ยวชาญมากกว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นหน่วยงานตั้งขึ้นใหม่ จึงเป็นไปได้ยากที่กองทัพไทยจะให้ข้อมูลแก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จนกว่าจะมีการพิสูจน์ได้ว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีความเชี่ยวชาญมากกว่ากระทรวงกลาโหม (๓) การคัดเลือกบุคลากรเข้ามาทำงานด้านนี้ มีกระบวนการอย่างไร นอกจากนี้ กระบวนการมีความเกี่ยวข้องกับข้อมูลความลับจะมีมาตรการดูแลบุคลากรอย่างไร คนที่เข้ามาแล้วมีสิทธิลาออกหรือไม่ หากลาออกแล้วจะกลายสภาพเป็นอย่างไร หากเอาข้อมูลไปเปิดเผยแล้วเสียหายจะดำเนินการอย่างไร จะมั่นใจได้อย่างไรว่าชั้นความลับจะไม่สูญเสีย (๔) ในร่างมาตรา ๕๘ (๔) ให้อำนาจพนักงานเจ้าหน้าที่ ยึดคอมพิวเตอร์หรืออุปกรณ์ใด ๆ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ จึงต้องฝึกพนักงานเจ้าหน้าที่ให้ยิงปืนด้วย หากให้ตำรวจหรือทหารเข้าไปช่วยดำเนินการน่าจะเหมาะสมกว่า (๕) ในร่างมาตรา ๑๗ (๖) กำหนดให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีอำนาจ เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน นอกจากนี้ ร่างมาตรา ๑๘ ยังกำหนดว่า รายได้ของยังไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน เห็นว่า ในเรื่องของความมั่นคงของชาติ ไม่ควรมีรายได้อาจต้องของบประมาณพิเศษหรือไม่ (๖) ในร่างมาตรา ๕๙ กำหนดว่า ผู้ดูแลระบบผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๔๗ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบกำหนดระยะเวลาที่พนักงานเจ้าหน้าที่ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง เห็นว่า ไม่ควรมีบทลงโทษ ผู้ดูแลระบบเพราะจะทำให้ไม่มีใครอยากทำหน้าที่นี้ (๗) ในร่างมาตรา ๖๒ และมาตรา ๖๓ ให้อำนาจเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	นอกจากนี้ คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ ที่มีอำนาจหน้าที่สำคัญในการจัดทำนโยบาย แผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตลอดจนการเตรียมการจัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดกรอบการดำเนินการ ๘ ด้าน เช่นเดียวกับ ร่างในมาตรา ๓๖ แห่ง พ.ร.บ. ฉบับนี้ ทั้งนี้ กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ ต่อไป

ลำดับ	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
	มากเกินไป ควรมีกลไกมาถ่วงดุลอำนาจของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	
๔.	**กองทัพอากาศ** (๑) ตามมาตรา ๑๔ “ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคลและไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ หรือกฎหมายอื่น” ในฐานะที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นนิติบุคคล มิใช่ส่วนราชการ อำนาจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะมีความเพียงพอหรือไม่ และถ้าไม่ใช่หน่วยงานของรัฐจะบังคับใช้กฎหมายได้หรือไม่ ควรขึ้นกับสำนักนายกรัฐมนตรีจะมีสะดวกรวดเร็วกว่าหรือไม่ (๒) อยากให้รัฐทำ Cloud เป็นหน่วยงานกลางเพื่อดูแลระบบกลางของ Cyber Security ของทุกหน่วยงาน (๓) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะขอบุคคลากรมาจากไหน	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ มี ๒ แนวทาง คือ (๑) ใช้ผู้เชี่ยวชาญเฉพาะด้านโดยจ้างมาดำเนินการ ให้วิธีขอยืมตัวมาจากหน่วยงานอื่น โดยในร่างมาตรา ๖๘ กำหนดว่า ภายในระยะเวลาสองปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ เลขาธิการอาจขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการ รัฐวิสาหกิจหรือองค์กรอื่นของรัฐมาปฏิบัติงานในสำนักงานเป็นการชั่วคราวได้ โดยทำความตกลงกับหน่วยงานของรัฐนั้นให้ถือว่าข้าราชการ พนักงาน หรือลูกจ้างที่มาปฏิบัติงานในสำนักงานเป็นการชั่วคราวตามวรรคหนึ่งไม่ขาดจาก

ลำดับ	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		สถานภาพเดิมและคงได้รับเงินเดือนหรือค่าจ้าง แล้วแต่กรณี จากสังกัดเดิม
๕.	**สำนักข่าวกรองแห่งชาติ** (๑) ถ้าดูในยุทธศาสตร์ทั้ง ๘ ด้านแล้ว เน้นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เน้นการบังคับใช้กฎหมาย ซึ่งใกล้เคียงกับคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มี ๘ ด้าน เช่นเดียวกัน ปัจจุบันสำนักงานตำรวจแห่งชาติทราบดี มีหลายหน่วยงานที่เกี่ยวข้อง ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น ศูนย์ปราบปรามอาชญากรรมด้านเทคโนโลยีสารสนเทศ (๒) ภาคเอกชนกังวลใจในร่างมาตรา ๔๖ วรรคท้าย ที่กำหนดว่าหน่วยงานที่ได้รับหนังสือตามวรรคหนึ่ง ไม่อาจยกเอาหน้าที่ตามกฎหมายอื่นหรือตามสัญญามาเป็นข้ออ้างเพื่อไม่เปิดเผยข้อมูล ทั้งนี้ มิให้ถือว่าการกระทำตามความในมาตรานี้โดยสุจริตเป็นการผิดกฎหมายหรือผิดสัญญา จึงขอเสนอให้ตัดออกร่างมาตรา ๔๖ วรรคท้าย ออก (๓) ควรแยกประเภทการรักษาความมั่นคงปลอดภัยไซเบอร์ในแต่ละด้าน เช่น ให้ทหารดูแลความมั่นคงปลอดภัยไซเบอร์เฉพาะด้านทหาร พลเรือนดูแลความมั่นคงปลอดภัยไซเบอร์เฉพาะด้านพลเรือน และเอกชนดูแลความมั่นคงปลอดภัยไซเบอร์เฉพาะด้านเอกชน น่าจะเหมาะสมกว่า (๔) พนักงานเจ้าหน้าที่ ถือว่าเป็นพลเรือนหน่วยหนึ่ง แต่กลายเป็น Law enforcement หน่วยงานของรัฐคุมเอกชน เช่น ขอข้อมูลจาก ดีแทค หรือ เอไอเอส ถ้า ดีแทค หรือ เอไอเอส ไม่ให้ข้อมูลรัฐจะมีบทลงโทษ จึงอยากสอบถามว่า พนักงานเจ้าหน้าที่จำกัดเฉพาะของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือไม่ เนื่องจากในกฎหมายฉบับอื่นเปิดกว้างให้แต่งตั้งพนักงานเจ้าหน้าที่ที่มีความชำนาญด้านคอมพิวเตอร์ และดูแลด้านความมั่นคงปลอดภัยด้าน Cyber ด้วย	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ

๔.๔ การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๑๑ ตุลาคม ๒๕๕๘ เวลา ๑๐.๐๐ ถึง ๑๒.๓๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นการเปิดรับฟังความคิดเห็นเป็นการทั่วไป

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๑	การมีผลบังคับใช้ของกฎหมาย	● มาตรา ๒ “พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป” ทางภาคเอกชนมีความกังวลในเรื่องความพร้อมของผู้ประกอบการในการปฏิบัติตามกฎหมาย	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ ต่อไป
๒.	ขอบเขตของกฎหมาย	● กรณีของข้อมูล มีกฎหมายอื่นกำกับอยู่แล้ว ดังนั้น กฎหมายนี้ควรจำกัดขอบเขตเฉพาะเรื่องของโครงสร้างและเครือข่าย ทั้งนี้ ข้อมูล น่าจะเป็นเรื่องผลกระทบจากภัยคุกคามมากกว่า หากพิจารณาบนกรอบมาตรฐานดูแลความมั่นคงปลอดภัยในการเข้าถึง ข้อมูลจึงน่าจะเป็นผลของการเกิด cyber attack ดังนั้น การกำกับข้อมูลจึงน่าจะไม่เหมาะสมและตรงตามเจตนารมณ์ของกฎหมาย ● ภาพรวมของโครงสร้างกฎหมาย น่าจะมีลักษณะเหมือนกฎหมายในสถานการณ์พิเศษ จึงควรมีการกำหนดนิยามให้ชัดเจนว่าอะไรคือสถานการณ์พิเศษ ขอบเขต และห้วงเวลา	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวไว้เป็นข้อสังเกตประกอบการพิจารณาร่างพระราชบัญญัติฯ ต่อไป
๒.	บทนิยามคำว่า “ความมั่นคงปลอดภัยไซเบอร์”	● คำนิยาม “ทรัพย์สินสารสนเทศ” นั้นกว้างเกินไป เมื่อประกอบกับ “ภัยคุกคามทางไซเบอร์” นั้นอาจตีความได้ว่า รวมไปถึงทรัพย์สินสารสนเทศของประชาชนทั่วไปด้วย จึงเสนอให้ระบุให้ชัดเจนและกระชับ ● คำนิยาม “ภัยคุกคามทางไซเบอร์” ควรใช้ข้อความที่รัดกุมของคำว่า “พยายามเข้าถึง” เพราะจะเป็นการกำหนดผู้กระทำความผิด	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวมาประกอบการพิจารณาปรับปรุงแก้ไขร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๓.	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	● การให้บริการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการใช้ผู้เชี่ยวชาญ ในมุมมองที่เป็นบริการสาธารณะ ประกอบกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องจัดเก็บรายได้ จะมีการคิดค่าใช้จ่ายอย่างไร ● มาตรา ๑๔ บัญญัติว่า “ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมาย ว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ หรือกฎหมายอื่น” และมาตรา ๑๗ บัญญัติว่า “ในการปฏิบัติหน้าที่ตามมาตรา ๑๖ ให้สำนักงานมีหน้าที่และอำนาจดังต่อไปนี้ (๔) ถือหุ้นหรือเข้าเป็นหุ้นส่วนหรือเข้าร่วมทุนกับนิติบุคคลอื่นในกิจการที่เกี่ยวกับวัตถุประสงค์ของสำนักงานและมาตรา๑๘ ทุนและทรัพย์สินในการดำเนินงานของสำนักงาน ประกอบด้วย ๕) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้อันเกิดจากการดำเนินการตามหน้าที่และอำนาจของสำนักงาน” จากบทบัญญัติข้างต้นเห็นว่าเป็นการขัดต่อหลักธรรมาภิบาล	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวมาประกอบการพิจารณาปรับปรุงแก้ไขร่างพระราชบัญญัติฯ
๔.	การรายงานเหตุภัยคุกคามของหน่วยงานเอกชน	● เนื่องจากมีประเด็นเรื่องการรายงานให้แก่หลายหน่วยงาน เช่น กลุ่มธนาคารโดยหน้าที่หลักต้องรายงานไปยัง ธปท. ซึ่งเป็นหน่วยงานกำกับดูแล และยังต้องรายงานไปยัง กปช. ตามร่างกฎหมายนี้ จึงควรกำหนดมาตรการที่ไม่ก่อให้เกิดภาระให้กับหน่วยงานที่มีหน้าที่ต้องรายงาน และในการรายงานเหตุภัยคุกคามไซเบอร์	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวมาประกอบการพิจารณาปรับปรุงแก้ไขร่างพระราชบัญญัติฯ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
๕.	การทำงานด้านการประสานงาน	● การทำงานด้านการประสานงาน เนื่องจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Computer Emergency Response Team : CERT) ของประเทศไทย มีด้วยกันหลาย CERT เช่น National CERT ของ สพธอ. หรือ Sector-based CERT ในแต่ละกลุ่มบริการ เช่น ธนาคารหรือสถาบันการเงินซึ่งมี CERT ของกลุ่มเอง จึงมีความกังวลว่าจะมีความทับซ้อนในการทำงานระหว่างกันหรือไม่	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวมาประกอบการพิจารณาปรับปรุงแก้ไขร่างพระราชบัญญัติฯ
๖.	การใช้อำนาจของเลขาธิการ และพนักงานเจ้าหน้าที่	● เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจมาก แต่ยังขาดกระบวนการตรวจสอบการใช้อำนาจ ซึ่งอาจก่อให้เกิดการใช้ดุลพินิจไปในทางที่มิชอบได้ ● การขอข้อมูลของพนักงานเจ้าหน้าที่ซึ่งใช้กับกรณีที่คาดว่าจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์นั้น เสนอให้ตัดคำว่า “คาดว่าน่าจะเกิด” เนื่องจากเปิดช่องให้มีการใช้ดุลพินิจและอำนาจอย่างกว้างขวาง จึงมีการเสนอให้ใช้คำว่า “มีเหตุอันควรเชื่อได้ว่า” แทน เพื่อให้มีความชัดเจนมากขึ้น ● ความละเอียดของข้อมูลที่จะต้องส่งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องระบุรายละเอียดมากน้อยเพียงใด อีกทั้งในองค์กรหนึ่งจะมีโครงข่ายหลายส่วน มีทั้งโครงข่ายที่มีความเสี่ยงสูงและโครงข่ายที่ไม่มีความเสี่ยง โครงข่ายที่ไม่มีความเสี่ยงนั้นต้องส่งข้อมูลให้ด้วยหรือไม่ ● ข้อมูลที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติร้องขอควรกำหนดให้ชัดเจนว่าเป็นข้อมูลอะไรบ้าง เพราะบางกรณีข้อมูลที่ส่งให้เป็นข้อมูลส่วนบุคคลของผู้ที่ได้รับความเสียหาย	กระทรวงฯ ได้รับความเห็น/ข้อเสนอแนะดังกล่าวมาประกอบการพิจารณาปรับปรุงแก้ไขร่างพระราชบัญญัติฯ ทั้งนี้ การใช้อำนาจของเลขาธิการฯ อาจถูกยับยั้งได้โดยรัฐมนตรีผู้รักษาการตามกฎหมาย ดังปรากฏในร่างมาตรา ๓๕

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ
		● การขอข้อมูลนั้น ยังขาดเรื่องการควบคุม การทำลาย การจัดเก็บข้อมูล	
	บทกำหนดโทษ	● ม.๖๓ ถ้าไม่อำนวยความสะดวก หมายถึงอย่างไร หากว่าเป็นการขัดขวาง เพราะมีหน้าที่ต้องทำตามกฎหมายอื่น จะทำอย่างไร	กระทรวงฯ ได้รับความเห็น/ ข้อเสนอแนะดังกล่าวมา ประกอบการพิจารณา ปรับปรุงแก้ไขร่าง พระราชบัญญัติฯ