ด่วนที่สุด

ที่ ดศ ๐๑๐๐.๔/๑๑๙๔๑

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๑๓ ธันวาคม ๒๕๖๑

เรื่อง ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ด่วนที่สุด ที่ ดศ ๐๑๐๐.๔/๘๘๕๒ ลงวันที่ ๒๖ กันยายน ๒๕๖๑

สิ่งที่ส่งมาด้วย ๑. หนังสือรองนายกรัฐมนตรีเห็นชอบให้นำเรื่องเสนอคณะรัฐมนตรี
๒. ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
๓. คำชี้แจงตามหลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ
๔. สรุปสาระสำคัญของร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
๕. สรุปการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... และขั้นตอนการปรับปรุง
๖. ตารางเปรียบเทียบร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกากับฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง
๗. แผนการจัดทำกฎหมายลำดับรองของร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

ด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอเสนอเรื่อง ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ต่อคณะรัฐมนตรีเพื่อพิจารณา โดยเรื่องนี้เข้าข่ายที่ต้องเสนอคณะรัฐมนตรีตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๒) ร่างพระราชบัญญัติ ร่างพระราชกำหนด ทั้งนี้ รองนายกรัฐมนตรี (พลอากาศเอก ประจิน จั่นตอง) กำกับการบริหารกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้เห็นชอบให้นำเรื่องดังกล่าวเสนอคณะรัฐมนตรีด้วยแล้ว

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียดดังนี้

๑. <u>เรื่องเดิม</u>

๑.๑ ความเป็นมาของเรื่องที่จะเสนอ

๑.๑.๑ ตามหนังสือที่อ้างถึง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้แจ้งยืนยันร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ตามที่สำนักงานคณะกรรมการกฤษฎีกาได้ตรวจพิจารณาแล้วเสร็จ ไปยังสำนักเลขาธิการคณะรัฐมนตรี

/๑.๑.๒ เนื่องจาก...

๑.๑.๒ เนื่องจากเนื้อหาสาระของร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาได้ตรวจพิจารณาแล้วเสร็จ มีความแตกต่างกับฉบับที่คณะรัฐมนตรีอนุมัติหลักการเป็นอย่างมาก ประกอบกับเพื่อให้เป็นไปตามบทบัญญัติมาตรา ๗๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ ดังนั้น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้จัดให้มีการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ โดยได้จัดให้มีการรับฟังความเห็นจากส่วนราชการ เอกชน และประชาชนทั่วไป ทั้งวิธีการประชุมหารือ การสัมมนา และผ่านทางทางเว็บไซต์ แล้วมีข้อกังวลจากภาคส่วนที่เกี่ยวข้อง กระทรวงฯ จึงได้พิจารณาปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ร่วมกับกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบันมากยิ่งขึ้น (สิ่งที่ส่งมาด้วย ๒)

ทั้งนี้ กระทรวงฯ ได้จัดทำคำชี้แจงตามหลักเกณฑ์การตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist) (สิ่งที่ส่งมาด้วย ๓) สรุปสาระสำคัญของร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... (สิ่งที่ส่งมาด้วย ๔) สรุปการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... และขั้นตอนการปรับปรุง (สิ่งที่ส่งมาด้วย ๕) ตารางเปรียบเทียบพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกากับฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง (สิ่งที่ส่งมาด้วย ๖) และแผนการจัดทำกฎหมายลำดับรอง (สิ่งที่ส่งมาด้วย ๗) มาพร้อมนี้ด้วยแล้ว

๑.๒ ผลการดำเนินการที่ผ่านมา

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดให้มีการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกา และได้จัดตั้งคณะทำงานเพื่อพิจารณาปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบันมากยิ่งขึ้น โดยมีรายละเอียดการดำเนินการ ดังนี้

๑.๒.๑ คณะกรรมการกฤษฎีกาแจ้งการตรวจพิจารณาร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... แล้วเสร็จ เมื่อวันที่ ๒๖ กันยายน ๒๕๖๑ (เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑)

๑.๒.๒ รับฟังความคิดเห็นผ่านเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th ระหว่างวันที่ ๒๗ กันยายน ถึง ๑๒ ตุลาคม ๒๕๖๑

๑.๒.๓ จัดงานประชุมสัมมนาและการประชุมหารือเพื่อรับฟังความคิดเห็นจำนวน ๔ ครั้ง ดังนี้

/(๑) การประชุมสัมมนา...

(๑) การประชุมสัมมนารับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๓ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยมีผู้เข้าร่วมเป็นผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการต่างประเทศ

(๒) การประชุมสัมมนารับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๕ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยมีผู้เข้าร่วมเป็นผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการและหน่วยงานที่เกี่ยวข้องกับระบบการให้บริการที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) การประชุมสัมมนารับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๙ ตุลาคม ๒๕๖๑ ณ วิทยาลัยป้องกันราชอาณาจักร โดยมีผู้เข้าร่วมจากกลุ่มสายงานความมั่นคง

(๔) การประชุมสัมมนารับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๑ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยเปิดรับฟังความคิดเห็นเป็นการทั่วไป

๑.๒.๔ ผลจากการรับฟังความคิดเห็น ปรากฏว่า ผู้มีส่วนได้เสียจากหลายภาคส่วนที่เกี่ยวข้อง ทั้งภาครัฐ ภาคเอกชน และภาคประชาสังคม ได้มีข้อทักท้วงและห่วงใยในหลาย ๆ ประเด็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ ซึ่งสามารถสรุปได้เป็น ๗ ประเด็น ได้แก่ (๑) วันที่มีผลใช้บังคับ (๒) ขอบเขตของกฎหมาย ความซ้ำซ้อน และการเชื่อมโยงกับกฎหมายอื่น (๓) คำนิยาม อาทิ ทรัพย์สินสารสนเทศ (๔) รูปแบบของสำนักงาน (๕) การกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๖) การรับมือภัยคุกคามทางไซเบอร์ และ (๗) บทกำหนดโทษ ทั้งนี้ มีผู้ให้ความเห็นเป็นจำนวนมากว่าสมควรมีการแก้ไขร่างพระราชบัญญัติตามประเด็นดังกล่าว กระทรวงฯ จึงได้ดำเนินการปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ดังนี้

(๑) ได้จัดให้มีการประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๗ – ๒๘ ตุลาคม ๒๕๖๑ ณ โรงแรมแคนทารี จังหวัดพระนครศรีอยุธยา ร่วมกับกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้มีส่วนเกี่ยวข้อง อาทิ สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ (TCT) สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) สมาคมผู้ให้บริการอินเทอร์เน็ตไทย (TISPA) หน่วยงานด้านความมั่นคง กระทรวงการต่างประเทศ ซึ่งสามารถสรุปผลเพื่อนำมาสู่การปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ให้มีความเหมาะสมยิ่งขึ้น

(๒) ได้จัดให้มีการประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีผู้เข้าร่วมเป็นส่วนราชการ เอกชน และผู้มีส่วนเกี่ยวข้อง ทั้งนี้ ได้นำผลสรุปจากการประชุมเมื่อวันที่

๒๗ – ๒๘ ตุลาคม ๒๕๖๑ มาเป็นข้อมูลในการพิจารณาเพื่อปรับปรุงร่างดังกล่าว และได้นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับปรับปรุงเมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ขึ้นรับฟังความคิดเห็นทางเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th เป็นระยะเวลา ๑๕ วัน ระหว่างวันที่ ๑๖ พฤศจิกายน ๒๕๖๑ ถึงวันที่ ๓๐ พฤศจิกายน ๒๕๖๑

(๓) ได้จัดตั้งคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งประกอบด้วยผู้แทนจากภาครัฐ ภาคเอกชน และภาคประชาสังคม และผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ คณะทำงานดังกล่าวได้จัดให้มีการประชุมเพื่อพิจารณาและปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และมีรองนายกรัฐมนตรี (พลอากาศเอก ประจิน จั่นตอง) เข้าร่วมการประชุมดังกล่าวด้วย โดยที่ประชุมได้นำผลจากการพิจารณาและปรับปรุงร่างรวมทั้งประเด็นข้อห่วงใยและความคิดเห็นจากภาคส่วนที่เกี่ยวข้องที่ส่งมาเพิ่มเติมมาพิจารณาปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบันมากยิ่งขึ้น

(๔) ได้จัดให้มีการประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๐ พฤศจิกายน ๒๕๖๑ ณ วิทยาลัยป้องกันราชอาณาจักร โดยผู้เข้าร่วมเป็นกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้แทนจากคณะกรรมการจัดทำยุทธศาสตร์ชาติ โดยได้นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่คณะทำงานฯ ได้ร่วมกันพิจารณาปรับปรุงเมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ มาปรับปรุงให้เหมาะสมยิ่งขึ้น

๑.๒.๕ ได้จัดส่งร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง ให้คณะทำงานฯ พิจารณาก่อนที่กระทรวงฯ จะได้ดำเนินการเสนอคณะรัฐมนตรีเพื่อพิจารณาให้ความเห็นชอบและเสนอต่อสภานิติบัญญัติแห่งชาติต่อไป

๒. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

๒.๑ เพื่อให้เป็นไปตามนโยบายที่คณะรัฐมนตรีได้แถลงต่อสภานิติบัญญัติแห่งชาติ เมื่อวันที่ ๑๒ กันยายน ๒๕๕๗ ข้อ ๖.๑๘ การเพิ่มศักยภาพทางเศรษฐกิจของประเทศ ส่งเสริมภาคเศรษฐกิจดิจิทัลและวางรากฐานของเศรษฐกิจดิจิทัลให้เริ่มขับเคลื่อนได้อย่างจริงจัง การใช้ดิจิทัลรองรับการให้บริการของภาคธุรกิจการเงินและธุรกิจบริการอื่น ๆ รองรับการผลิตสินค้าอุตสาหกรรมและการพัฒนาเศรษฐกิจสร้างสรรค์ และจัดให้มีคณะกรรมการระดับชาติเพื่อขับเคลื่อนอย่างจริงจัง ดังนั้น ปัจจัยสำคัญคือการมีโครงสร้างพื้นฐานทางกฎหมายที่เอื้อต่อการพัฒนาประเทศไปสู่ยุคของสังคมดิจิทัลอย่างสมบูรณ์แบบ ซึ่งร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... มีสาระสำคัญเพื่อให้ประเทศสามารถ

/ป้องกันและรับมือ...

ป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และเพื่อกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ ซึ่งจะทำให้สามารถนำเทคโนโลยีดิจิทัลไปใช้ในการขับเคลื่อนการพัฒนาประเทศได้อย่างมีประสิทธิภาพ

๒.๒ ร่างพระราชบัญญัติดังกล่าวเป็นเรื่องที่ต้องนำเสนอคณะรัฐมนตรีตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๒) ร่างพระราชบัญญัติ ร่างพระราชกำหนด

๓. <u>ความเร่งด่วนของเรื่อง</u>

การส่งเสริมภาคเศรษฐกิจดิจิทัลและการวางรากฐานของเศรษฐกิจดิจิทัลตามนโยบายของคณะรัฐมนตรีถือเป็นเรื่องเร่งด่วนที่ต้องเร่งผลักดัน เนื่องจากจะเป็นรากฐานในการพัฒนาประเทศในด้านต่าง ๆ ซึ่งปัจจุบันมีความจำเป็นต้องใช้เทคโนโลยีดิจิทัลอย่าหลีกเลี่ยงไม่ได้ ดังนั้น การมีกฎหมายที่จะสามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และการกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ จึงมีความจำเป็นเร่งด่วนเพื่อให้การขับเคลื่อนการพัฒนาประเทศเป็นไปได้อย่างมีประสิทธิภาพ

๔. <u>สาระสำคัญหรือข้อเท็จจริงและข้อกฎหมาย</u>

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุงนี้ มีสาระสำคัญสรุปได้ดังนี้

(๑) หมวด ๑ คณะกรรมการ

ส่วนที่ ๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กำหนดให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ ซึ่ง กปช. มีหน้าที่และอำนาจดังนี้ (๑) เสนอนโยบาย ส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้คณะรัฐมนตรีให้ความเห็นชอบ (๒) กำหนดนโยบายให้หน่วยงานรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมถึงนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) กำกับดูแลการจัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงานเพื่อเสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ (๔) แต่งตั้งและถอดถอนเลขาธิการ (๕) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ อำนาจหน้าที่ และกรอบการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงาน

/ควบคุมหรือกำกับดูแล...

ควบคุมหรือกำกับดูแล หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๖) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และการรักษาความมั่นคงปลอดภัยไซเบอร์ (๗) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๘) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงประมวลแนวทางปฏิบัติ และกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๙) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางนโยบายในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

ส่วนที่ ๒ คณะกรรมการเฉพาะด้าน กำหนดให้มีคณะกรรมการเฉพาะด้านเพื่อปฏิบัติหน้าที่เกี่ยวกับการดำเนินการต่าง ๆ ตามหน้าที่และอำนาจของ กชป. ดังนี้

(๑) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กกช.) มีรองนายกรัฐมนตรีฝ่ายความมั่นคงเป็นประธานกรรมการ โดยมีหน้าที่และอำนาจ ดังนี้ (๑) ติดตามการดำเนินการตามนโยบายและแผนในส่วนที่เกี่ยวข้อง (๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ (๓) กำกับดูแลการดำเนินงานเพื่อเป็นศูนย์กลางการประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (THAI CERT) และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ (๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน (๕) ประสานงานและให้ความร่วมมือในการตั้งหน่วยงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (CERT) ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ (๖) ร่วมกันประสานงานกับหน่วยงานอื่นๆ ในการกำหนดกรอบและความร่วมมือที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานในประเทศและต่างประเทศ (๗) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อ กปช. (๘) วิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อ กปช. พิจารณาสั่งการเมื่อมีภัยคุกคามระดับร้ายแรงขึ้น

(๒) คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส.) มีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ โดยมีหน้าที่และอำนาจ ดังนี้ (๑) ติดตามการดำเนินการตามนโยบายและแผนในส่วนที่เกี่ยวข้อง (๒) ดำเนินการ

/เพื่อรักษา...

เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของผู้ควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้ผู้ควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๔) ส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดมาตรฐานบังคับขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมใบรับรองมาตรฐานความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชน (๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานรัฐและหน่วยงานเอกชน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) คณะกรรมการเฉพาะด้านอื่น ซึ่ง กปช. แต่งตั้งโดยความเห็นชอบของคณะรัฐมนตรีเพื่อปฏิบัติหน้าที่ตามที่ กปช. กำหนด

๒) หมวด ๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐมีฐานะเป็นนิติบุคคล ที่ไม่เป็นส่วนราชการและรัฐวิสาหกิจ รับผิดชอบงานธุรการ งานวิชาการ และงานเลขานุการของ กปช. และคณะกรรมการเฉพาะด้าน และมีหน้าที่หลักในการจัดทำนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงาน จัดทำแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เสริมสร้างความรู้ความเข้าใจและความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ ศึกษาและวิจัย ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

/๓) หมวด ๓...

๓) หมวด ๓ การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑ นโยบายและแผน กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ และต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ กำหนดให้ กปช. จัดทำนโยบายส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามเป้าหมายและแนวทางที่กฎหมายกำหนด เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้จัดให้มีการรับฟังความคิดเห็นด้วย และกำหนดให้หน่วยงานที่เกี่ยวข้องจัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนดังกล่าว

ส่วนที่ ๒ การบริหารจัดการ กำหนดให้หน่วยงานที่เกี่ยวข้องมีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ กำหนดความสำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้ กปช. มีอำนาจประกาศกำหนดให้หน่วยงานที่มีลักษณะดังต่อไปนี้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๑) ด้านความมั่นคงของรัฐ (๒) ด้านบริการภาครัฐที่สำคัญ (๓) ด้านการเงินการธนาคาร (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (๕) ด้านการขนส่งและโลจิสติกส์ (๖) ด้านพลังงานและสาธารณูปโภค (๗) ด้านสาธารณสุข (๘) ด้านอื่นตามที่ กปช.ประกาศกำหนดเพิ่มเติม รวมทั้งให้ กปช. มีอำนาจประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของหน่วยงานศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงานเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหมดหรือบางส่วนก็ได้ โดยในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าไม่ได้มาตรฐานให้ส่งเรื่องให้ กปช. หรือ กสส. พิจารณา ทั้งนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

/ส่วนที่ ๔...

ส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์ กำหนดให้ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว ทั้งนี้ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานซึ่งทำหน้าที่เป็นศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และแจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

กปช. และหรือ กกช. จะกำหนดลักษณะของภัยคุกคามทางไซเบอร์โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงภัยจนอาจทำให้คอมพิวเตอร์ ระบบคอมพิวเตอร์ที่ให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงของรัฐ การป้องกันประเทศ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน ถูกแทรกแซงอย่างมีนัยสำคัญหรือถูกระงับการทำงาน

/(ค) เป็นภัยคุกคาม...

(ค) เป็นภัยคุกคามที่มีความรุนแรงที่ก่อหรืออาจก่อให้เกิดความเสียงภัยหรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่สำคัญหรือมีจำนวนมาก

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

(ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์จำนวนมากถูกทำลายในวงกว้างในระดับประเทศ

(ค) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ (๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง (๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ (๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่ (๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์ (๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยให้ กปช. หรือ กกช. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง หรือผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรงในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

/ในการป้องกัน...

ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ในเรื่อง (๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ (๒) เข้าถึงทรัพย์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ (๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น (๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์ สำหรับการดำเนินการตาม (๓) และ (๔) ให้ กปช. หรือ กกช. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงาน เจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

สำหรับผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้ และในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายนี้

๔) หมวด ๔ บทกำหนดโทษ กำหนดข้อปฏิบัติ ข้อห้าม และบทกำหนดโทษสำหรับพนักงานเจ้าหน้าที่และพนักงานสอบสวน รวมถึงหน่วยงานโครงสร้างพื้นฐานและบุคคลที่เกี่ยวข้อง

๕) บทเฉพาะกาล กำหนดให้ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงาน ให้นายกรัฐมนตรีอาศัยอำนาจตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ จัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว และแต่งตั้งคณะกรรมการผู้ทรงคุณวุฒิหรือดำเนินการอื่นใดเป็นการชั่วคราวกำหนดให้ กปช. ขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการ รัฐวิสาหกิจหรือองค์กรอื่นของรัฐมาปฏิบัติงานในสำนักงานเป็นการชั่วคราวได้ ทั้งนี้ เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรี (นายกรัฐมนตรี) เสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว ไปเป็นของสำนักงานตามพระราชบัญญัตินี้

/๕. ค่าใช้จ่ายและแหล่งที่มา...

๕. <u>ค่าใช้จ่ายและแหล่งที่มา</u>

ได้รับการสนับสนุนจากงบประมาณของแผ่นดิน

๖. <u>ผลกระทบ</u>

การตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... จะทำให้สามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และทำให้การขับเคลื่อนการพัฒนาประเทศด้วยเทคโนโลยีดิจิทัลเป็นไปตามนโยบายของรัฐบาล

๗. <u>ความเห็นของคณะกรรมการหรือหน่วยงานของรัฐที่เกี่ยวข้อง</u>

กระทรวงฯ ได้แต่งตั้งคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ประกอบด้วยผู้แทนจากภาครัฐ ภาคเอกชน และภาคประชาสังคม เพื่อพิจารณาปรับปรุงร่างพระราชบัญญัติดังกล่าวให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบันมากยิ่งขึ้น โดยร่างพระราชบัญญัติที่ได้นำเสนอนี้ได้ผ่านการพิจารณาให้ความเห็นจากคณะทำงานดังกล่าวและปรับปรุงให้มีความเหมาะสมยิ่งขึ้นด้วยแล้ว รวมทั้งได้ผ่านการพิจารณาจากกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติแล้วด้วย

๘. <u>ข้อเสนอของส่วนราชการ</u>

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาแล้ว เห็นควรนำเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ความเห็นชอบร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุงจากฉบับที่สำนักงานคณะกรรมการกฤษฎีกาได้ตรวจพิจารณาซึ่งหลักการส่วนใหญ่เป็นไปตามร่างพระราชบัญญัติฯ ที่ได้ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกา แต่มีการปรับปรุงประเด็นบางส่วนตามผลการรับฟังความคิดเห็น โดยเสนอให้เห็นชอบแทนร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกา (เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑) ซึ่งกระทรวงได้แจ้งยืนยันไปเมื่อวันที่ ๒๖ กันยายน ๒๕๖๑ เพื่อนำเสนอต่อสภานิติบัญญัติแห่งชาติต่อไป

จึงเรียนมาเพื่อโปรดนำกราบเรียนนายกรัฐมนตรีเพื่อนำเสนอคณะรัฐมนตรีพิจารณาต่อไป

ขอแสดงความนับถือ

(นายพิเชฐ ดุรงคเวโรจน์)
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานปลัดกระทรวง กองกฎหมาย
โทร. ๐ ๒๑๔๑ ๖๗๖๓, ๖๖ โทรสาร ๐ ๒๑๔๓ ๘๐๑๓
ไปรษณีย์อิเล็กทรอนิกส์ sataporn.s@mdes.go