ที่ นร ๐๕๐๓/๔๓๐๔๒

สำนักนายกรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๖ ธันวาคม ๒๕๖๑

เรื่อง ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

กราบเรียน ประธานสภานิติบัญญัติแห่งชาติ

สิ่งที่ส่งมาด้วย ร่างพระราชบัญญัติฯ และเอกสารประกอบในเรื่องนี้

ด้วยคณะรัฐมนตรีได้ประชุมปรึกษาลงมติให้เสนอร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ต่อสภานิติบัญญัติแห่งชาติเป็นเรื่องด่วน ดังที่ได้ส่งมาพร้อมนี้

จึงขอเสนอร่างพระราชบัญญัติดังกล่าว พร้อมด้วยบันทึกหลักการและเหตุผล บันทึกวิเคราะห์สรุปสาระสำคัญ และเอกสารเกี่ยวกับการดำเนินการตามมาตรา ๗๗ วรรคสอง ของรัฐธรรมนูญแห่งราชอาณาจักรไทย มาเพื่อขอได้โปรดนำเสนอสภานิติบัญญัติแห่งชาติพิจารณาเป็นเรื่องด่วนต่อไป

ขอแสดงความนับถืออย่างยิ่ง

พลเอก

(ประยุทธ์ จันทร์โอชา)
นายกรัฐมนตรี

สำนักเลขาธิการคณะรัฐมนตรี
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๑๓๔๒
โทรสาร ๐ ๒๒๘๐ ๙๐๕๘ (wa034/D/ส/๗ศ)

บันทึกหลักการและเหตุผล
ประกอบร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ....

หลักการ

ให้มีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เหตุผล

โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้

ร่าง

พระราชบัญญัติ

การรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ....

.....

.....

.....

.....

.....

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๒๘ มาตรา ๓๒ มาตรา ๓๓ มาตรา ๓๔ มาตรา ๓๖ และมาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

.....

.....

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ...."

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

"การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

(โปรดพลิก)

"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"ไซเบอร์" หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

"หน่วยงานของรัฐ" หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

"ประมวลแนวทางปฏิบัติ" (Code of Practice) หมายความว่า ระเบียบกฎเกณฑ์ใดๆ ที่ออกหรืออนุมัติโดยคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมถึงประกาศแนวทางต่างๆ ที่จะเพิ่มเติมหรือแก้ไขภายหลัง

"เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์" (Cybersecurity Incident) หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของเครื่องคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

"มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์" (Cybersecurity Solution) หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร (people) กระบวนการ (process) และเทคโนโลยี (technology) โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใดๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

"โครงสร้างพื้นฐานสำคัญทางสารสนเทศ" หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

"หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ" หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

"หน่วยงานควบคุมหรือกำกับดูแล" หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชนหรือบุคคลซึ่งมีกฎหมายหรือระเบียบกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานภาครัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

"คณะกรรมการ" หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"เลขาธิการ" หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"สำนักงาน" หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกประกาศ และแต่งตั้งพนักงานเจ้าหน้าที่ เพื่อปฏิบัติการตามพระราชบัญญัตินี้

ประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

(โปรดพลิก)

หมวด ๑
คณะกรรมการ

ส่วนที่ ๑
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๕ ให้มีคณะกรรมการคณะหนึ่งเรียกว่า "คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ" เรียกโดยย่อว่า "กปช." และให้ใช้ชื่อเป็นภาษาอังกฤษว่า "National Cybersecurity Committee" เรียกโดยย่อว่า "NCSC" ประกอบด้วย

(๑) นายกรัฐมนตรี เป็นประธานกรรมการ

(๒) รองนายกรัฐมนตรีฝ่ายความมั่นคง เป็นรองประธานกรรมการ

(๓) กรรมการโดยตำแหน่ง ประกอบด้วย รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รัฐมนตรีว่าการกระทรวงการคลัง รัฐมนตรีว่าการกระทรวงการต่างประเทศ รัฐมนตรีว่าการกระทรวงคมนาคม รัฐมนตรีว่าการกระทรวงพลังงาน รัฐมนตรีว่าการกระทรวงมหาดไทย รัฐมนตรีว่าการกระทรวงยุติธรรม เลขาธิการ กอ.รมน. ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(๔) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมาย หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นกรรมการ

ให้เลขาธิการ เป็นกรรมการและเลขานุการโดยตำแหน่ง และให้แต่งตั้งผู้ช่วยเลขานุการได้ตามความจำเป็น

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อเสนอคณะรัฐมนตรีแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิรวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๗ วรรคสอง ให้เป็นไปตามระเบียบที่คณะรัฐมนตรีกำหนดโดยการเสนอแนะของ กปช.

มาตรา ๖ กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องมีสัญชาติไทยและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง หรือเคยถูกถอดถอนจากตำแหน่ง

(๕) เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น หรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ของพรรคการเมือง

มาตรา ๗ กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีวาระการดำรงตำแหน่งคราวละสามปี

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ คณะรัฐมนตรีอาจแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างได้ และให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมิได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่

มาตรา ๘ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๗ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออก

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๖

มาตรา ๙ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ กปช. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) เสนอนโยบาย ส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา ๔๑

(๒) กำหนดนโยบายให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) จัดทำ กำกับ และดูแลแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อเสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

(๔) แต่งตั้งและถอดถอนเลขาธิการ

(โปรดพลิก)

(๕) มีอำนาจมอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนดวัตถุประสงค์ อำนาจหน้าที่ และกรอบการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๖) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(๗) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๘) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงประมวลแนวทางปฏิบัติและกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๙) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางนโยบายในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

(๑๐) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย

มาตรา ๑๐ ให้มีคณะที่ปรึกษาคณะหนึ่ง มีหน้าที่และอำนาจในการรวบรวมความคิดเห็น ให้คำปรึกษาและข้อเสนอแนะ หรือดำเนินการอย่างหนึ่งอย่างใดตามที่ กปช. มอบหมาย

หลักเกณฑ์และวิธีการแต่งตั้ง คุณสมบัติและลักษณะต้องห้าม องค์ประกอบและวิธีการปฏิบัติหน้าที่ และวาระการดำรงตำแหน่งและการพ้นจากตำแหน่งของคณะที่ปรึกษา ให้เป็นไปตามระเบียบที่ กปช. กำหนด

ส่วนที่ ๒
คณะกรรมการเฉพาะด้าน

มาตรา ๑๑ ในการดำเนินการตามอำนาจหน้าที่ของ กปช. ตามมาตรา ๙ ให้มีคณะกรรมการเฉพาะด้าน เพื่อปฏิบัติหน้าที่ในส่วนที่เกี่ยวข้องกับเรื่อง ดังต่อไปนี้

(๑) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกซ.” ประกอบด้วย

(ก) รองนายกรัฐมนตรีฝ่ายความมั่นคง เป็นประธานกรรมการ

(ข) กรรมการโดยตำแหน่ง ประกอบด้วย รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงกลาโหม ปลัดกระทรวงการคลัง ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคม ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(ค) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่ง กปช. แต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ ประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการ เป็นกรรมการและเลขานุการโดยตำแหน่ง และให้แต่งตั้งผู้ช่วยเลขานุการได้ตามความจำเป็น

(๒) คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เรียกโดยย่อว่า "กสส." ประกอบด้วย

(ก) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

(ข) กรรมการโดยตำแหน่ง ประกอบด้วย ปลัดกระทรวงการคลัง ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพาณิชย์ กรรมการคนหนึ่งในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติที่คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติแต่งตั้ง ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(ค) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่ง กปช. แต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ ประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการ เป็นกรรมการและเลขานุการโดยตำแหน่ง และให้แต่งตั้งผู้ช่วยเลขานุการได้ตามความจำเป็น

(๓) คณะกรรมการเฉพาะด้านอื่น ซึ่ง กปช. แต่งตั้งโดยความเห็นชอบของคณะรัฐมนตรีเพื่อปฏิบัติหน้าที่ตามที่ กปช. กำหนด

หลักเกณฑ์และวิธีการสรรหาบุคคลที่เห็นสมควรเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิให้เป็นไปตามระเบียบที่ กปช. กำหนด

มาตรา ๑๒ ให้ กกซ. ตามมาตรา ๑๑ (๑) มีหน้าที่และอำนาจ ดังนี้

(๑) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๔๑ (๒) (๔) และ (๗)

(๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ตามมาตรา ๖๐ มาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ และมาตรา ๖๕

(๓) กำกับดูแลการดำเนินงานเพื่อเป็นศูนย์กลางการประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (THAI CERT) และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(โปรดพลิก)

(๕) ประสานงานและให้ความร่วมมือในการตั้งหน่วยงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (CERT) ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) ร่วมกันประสานงานกับหน่วยงานอื่นๆ ในการกำหนดกรอบและความร่วมมือที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานในประเทศและต่างประเทศ

(๗) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อ กปช.

(๘) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อ กปช. พิจารณาสั่งการ เมื่อมีภัยคุกคามระดับร้ายแรงขึ้น

ในการกำหนดกรอบมาตรฐานตาม (๓) ให้คำนึงถึงหลักการบริหารความเสี่ยงโดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

มาตรา ๑๓ ให้ กสส. ตามมาตรา ๑๑ (๒) มีหน้าที่และอำนาจ ดังนี้

(๑) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๔๑ (๓) และ (๗)

(๒) ดำเนินการเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๕๒ และ มาตรา ๕๓

(๓) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของผู้ควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้ผู้ควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๔) ส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดมาตรฐานบังคับขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมใบรับรองมาตรฐานความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชน

(๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานรัฐและหน่วยงานเอกชน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๔ ให้นำบทบัญญัติมาตรา ๖ มาตรา ๗ และ มาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเฉพาะด้านโดยอนุโลม

มาตรา ๑๕ ให้คณะกรรมการเฉพาะด้านมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการเฉพาะด้านมอบหมาย

ในกรณีจำเป็นตามข้อผูกพันหรือตามลักษณะของกิจการของสำนักงาน คณะกรรมการเฉพาะด้านอาจแต่งตั้งชาวต่างประเทศเป็นอนุกรรมการได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่ กปช.กำหนด

มาตรา ๑๖ การประชุมของ กปช. คณะกรรมการเฉพาะด้าน คณะที่ปรึกษา และคณะอนุกรรมการ ให้เป็นไปตามระเบียบที่ กปช. กำหนด โดยอาจประชุมด้วยวิธีการทางอิเล็กทรอนิกส์ก็ได้

มาตรา ๑๗ ให้ประธานกรรมการ รองประธานกรรมการ กรรมการ ที่ปรึกษา กรรมการเฉพาะด้าน และอนุกรรมการ ได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๑๘ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจออกคำสั่ง และต้องแสดงบัตรประจำตัวต่อบุคคลที่เกี่ยวข้องด้วย

ในการแต่งตั้งพนักงานเจ้าหน้าที่ ให้รัฐมนตรีพิจารณาแต่งตั้งจากผู้มีความรู้ความชำนาญ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นพนักงานเจ้าหน้าที่เพื่อปฏิบัติการอย่างหนึ่งอย่างใดตามพระราชบัญญัตินี้

ระดับความรู้ความชำนาญ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของพนักงานเจ้าหน้าที่ ให้เป็นไปตามที่ กปช. ประกาศกำหนดบัตรประจำตัวพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่คณะกรรมการกำกับสำนักงานประกาศกำหนด

หมวด ๒
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๑๙ ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

มาตรา ๒๐ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

(โปรดพลิก)

มาตรา ๒๑ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กปช. และคณะกรรมการเฉพาะด้าน และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

(๑) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงานตามมาตรา ๙ ต่อ กปช.

(๒) จัดทำแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ (๓) เสนอต่อ กปช. เพื่อให้ความเห็นชอบ

(๓) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจาก กปช.

(๔) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๕) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของ กปช.

(๖) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๗) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

(๘) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

(๙) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

(๑๐) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจาก กปช.

(๑๑) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

(๑๒) ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๓) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค และจัดทำรายงานสรุปผลการดำเนินงานประจำปีให้คณะรัฐมนตรีทราบ

(๑๔) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่ กปช. หรือคณะรัฐมนตรีมอบหมาย

เพื่อประโยชน์ในการดำเนินการตามหน้าที่และอำนาจตาม (๔) ให้สำนักงานจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงาน และให้มีหน้าที่และอำนาจตามที่ กปช. กำหนด

มาตรา ๒๒ ในการปฏิบัติหน้าที่ตามมาตรา ๒๑ ให้สำนักงานมีหน้าที่และอำนาจดังต่อไปนี้

(๑) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพยสิทธิต่าง ๆ

(๒) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินกิจการของสำนักงาน

(๓) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน

(๔) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของคณะกรรมการกำกับสำนักงาน

(๕) ดำเนินการอื่นใดที่จำเป็นหรือต่อเนื่องเพื่อให้เป็นไปตามหน้าที่และอำนาจของสำนักงาน

(๖ ปฏิบัติการใด ๆ ให้เป็นไปตามพระราชบัญญัตินี้ หรือตามที่ กปช. หรือ คกส. มอบหมาย

มาตรา ๒๓ ทุนและทรัพย์สินในการดำเนินงานของสำนักงาน ประกอบด้วย

(๑) เงินและทรัพย์สินที่ได้รับโอนมาตามมาตรา ๗๗

(๒) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี

(๓) เงินอุดหนุนจากหน่วยงานอื่นในประเทศหรือจากต่างประเทศ

(๔) เงินหรือทรัพย์สินที่มีผู้บริจาคหรือมอบให้ ทั้งนี้ ต้องไม่มีเงื่อนไขหรือภาระผูกพัน

(๕) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้อันเกิดจากการดำเนินการตามหน้าที่และอำนาจของสำนักงาน

(๖) ดอกผลของเงินหรือรายได้จากทรัพย์สินของสำนักงาน

รายได้ของสำนักงานตามวรรคหนึ่ง ต้องนำส่งคลังเป็นรายได้แผ่นดิน

มาตรา ๒๔ ให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์เรียกโดยย่อว่า “คกส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคน

ให้เลขาธิการเป็นกรรมการและเลขานุการของ คกส. และให้แต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ตามความจำเป็น

กรรมการผู้ทรงคุณวุฒิ ตามวรรคหนึ่ง ให้รัฐมนตรีแต่งตั้งจากบุคคล ซึ่งมีความรู้ความเชี่ยวชาญ และความสามารถเป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(โปรดพลิก)

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการดำเนินงานของ คกส. ตามหลักเกณฑ์และวิธีการที่ กปช. กำหนด

ให้นำบทบัญญัติมาตรา ๖ และมาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิโดยอนุโลม

มาตรา ๒๕ ให้กรรมการผู้ทรงคุณวุฒิ ใน คกส. มีวาระการดำรงตำแหน่งคราวละสี่ปี

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ รัฐมนตรีอาจแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างได้ และให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมิได้แต่งตั้ง กรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้น อยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่

มาตรา ๒๖ ให้ คกส. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

(๒) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

(๓) อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

(๔) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

(๕) วินิจฉัยคำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

(๖) ประเมินผลการดำเนินงานของสำนักงานและการปฏิบัติงานของเลขาธิการ

(๗) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการกำกับสำนักงาน หรือตามที่ กปช. หรือคณะรัฐมนตรีมอบหมาย

ในการปฏิบัติงานตามวรรคหนึ่ง คกส. อาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาเสนอแนะ หรือกระทำการอย่างหนึ่งอย่างใดตามที่ คกส. มอบหมายได้ ทั้งนี้ การปฏิบัติงานและการประชุมให้เป็นไปตามหลักเกณฑ์และวิธีการที่ คกส. กำหนด

คกส. อาจแต่งตั้งผู้ทรงคุณวุฒิซึ่งมีความเชี่ยวชาญในด้านที่เป็นประโยชน์ต่อการดำเนินงานของสำนักงานเป็นที่ปรึกษา คกส. ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่ กปช.กำหนด

ในกรณีจำเป็นตามข้อผูกพันหรือตามลักษณะของกิจการของสำนักงาน คกส. อาจแต่งตั้งชาวต่างประเทศเป็นอนุกรรมการหรือที่ปรึกษา คกส. ได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่ กปช.กำหนด

มาตรา ๒๗ ให้ประธานกรรมการ และกรรมการ ประธานอนุกรรมการ อนุกรรมการ ที่ คกส. แต่งตั้ง ได้รับเบี้ยประชุมและค่าตอบแทนอื่นตามหลักเกณฑ์ที่ กปช. กำหนด

มาตรา ๒๘ ให้สำนักงานมีเลขาธิการคนหนึ่ง รับผิดชอบการปฏิบัติงานของสำนักงาน และเป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน

มาตรา ๒๙ เลขาธิการต้องมีคุณสมบัติดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) มีอายุไม่เกินหกสิบปีบริบูรณ์

(๓) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงานและการบริหารจัดการ

มาตรา ๓๐ ผู้มีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ ต้องห้ามมิให้เป็นเลขาธิการ

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เป็นข้าราชการ พนักงาน หรือลูกจ้าง ของส่วนราชการหรือรัฐวิสาหกิจหรือหน่วยงานอื่นของรัฐหรือของราชการส่วนท้องถิ่น

(๕) เป็นหรือเคยเป็นข้าราชการการเมือง ผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๖) เป็นหรือเคยเป็นกรรมการหรือผู้ดำรงตำแหน่งอื่นในพรรคการเมืองหรือเจ้าหน้าที่ของพรรคการเมือง เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๗) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง หรือเคยถูกถอดถอนจากตำแหน่ง

(๘) เคยถูกให้ออกเพราะไม่ผ่านการประเมินผลการปฏิบัติงานตามมาตรา ๓๔ (๕)

มาตรา ๓๑ ให้ กปช. เป็นผู้กำหนดอัตราเงินเดือนและค่าตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๓๒ เลขาธิการอยู่ในตำแหน่งคราวละสี่ปี

เลขาธิการซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้ แต่ต้องไม่เกินสองวาระติดต่อกัน

มาตรา ๓๓ ในแต่ละปี ให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่ กปช. กำหนด

(โปรดพลิก)

มาตรา ๓๔ นอกจากการพ้นจากตำแหน่งตามวาระ เลขาธิการพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ขาดคุณสมบัติตามมาตรา ๒๙ หรือมีลักษณะต้องห้ามตามมาตรา ๓๐

(๔) กปช. มีมติให้ออก เพราะบกพร่องหรือทุจริตต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ

(๕) กปช. ให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน

(๖) ออกตามกรณีที่กำหนดไว้ในสัญญาจ้างหรือข้อตกลงระหว่าง กปช.กับเลขาธิการ

มาตรา ๓๕ ให้เลขาธิการภายใต้การควบคุมดูแลของ กปช. และกรรมการตามมาตรา ๑๑ ต้องดำเนินการตามคำสั่งของ กปช. และกรรมการตามมาตรา ๑๑ ภายใต้หน้าที่และอำนาจ ดังต่อไปนี้

(๑) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและ กปช. และข้อบังคับ นโยบาย มติ และประกาศของคณะกรรมการกำกับสำนักงาน

(๒) วางระเบียบภายใต้นโยบายของ กปช. และกรรมการตามมาตรา ๑๑ โดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และข้อบังคับ นโยบาย มติ และประกาศที่ กปช. หรือกรรมการตามมาตรา ๑๑ กำหนด

(๓) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามข้อบังคับของคณะกรรมการกำกับสำนักงานและระเบียบของสำนักงาน

(๔) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของ กปช. หรือกรรมการตามมาตรา ๑๑ เพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(๕) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงานและลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามข้อบังคับของคณะกรรมการกำกับสำนักงานและระเบียบของสำนักงาน

(๖) ปฏิบัติการอื่นใดตามข้อบังคับ นโยบาย มติ หรือประกาศของคณะกรรมการกำกับสำนักงานหรือกรรมการตามมาตรา ๑๑

ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็นผู้แทนของสำนักงาน ภายใต้ขอบเขตที่ได้รับการแต่งตั้งโดย กปช.

เลขาธิการอาจมอบอำนาจให้บุคคลใดในสังกัดของสำนักงาน ปฏิบัติงานเฉพาะอย่างแทนก็ได้ ทั้งนี้ ตามข้อบังคับที่ คกส. หรือกรรมการตามมาตรา ๑๑ กำหนด

ในกรณีที่ไม่มีเลขาธิการหรือเลขาธิการไม่อาจปฏิบัติหน้าที่ได้ ให้รองเลขาธิการที่มีอาวุโสตามลำดับรักษาการแทน ถ้าไม่มีรองเลขาธิการหรือรองเลขาธิการไม่อาจปฏิบัติหน้าที่ได้ ให้ กปช. แต่งตั้งบุคคลที่เหมาะสมมารักษาการแทน

มาตรา ๓๖ การบัญชีของสำนักงานให้จัดทำตามแบบและหลักเกณฑ์ที่ คกส. กำหนดโดยให้คำนึงถึงหลักสากลและมาตรฐานการบัญชี

มาตรา ๓๗ ให้สำนักงานจัดทำงบดุล งบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในเก้าสิบวันนับแต่วันสิ้นปีบัญชี

ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงาน และประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานทุกรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อ คกส. เพื่อรับรอง

มาตรา ๓๘ ให้สำนักงานจัดทำรายงานการดำเนินงานประจำปีเสนอ กปช. และรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

รายงานการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว

การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่คณะกรรมการกำกับสำนักงานให้ความเห็นชอบ

มาตรา ๓๙ ให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล และมติคณะรัฐมนตรีที่เกี่ยวข้อง เพื่อการนี้ให้รัฐมนตรีมีอำนาจสั่งให้เลขาธิการชี้แจงข้อเท็จจริง แสดงความคิดเห็น หรือทำรายงานเสนอ และมีอำนาจสั่งยับยั้งการกระทำของสำนักงานที่ขัดต่อหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง ตลอดจนสั่งสอบสวนข้อเท็จจริงเกี่ยวกับการดำเนินการของสำนักงานได้

หมวด ๓
การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑
นโยบายและแผน

มาตรา ๔๐ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

(โปรดพลิก)

การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

มาตรา ๔๑ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อยดังต่อไปนี้

(๑) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(๒) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๓) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(๔) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน

(๗) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๘) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๔๒ ให้ กปช. จัดทำนโยบายส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๑ เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้ประกาศในราชกิจจานุเบกษา และเมื่อได้ประกาศแล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว

ในการจัดทำนโยบายและแผนตามวรรคหนึ่ง ให้สำนักงานจัดให้มีการรับฟังความเห็นหรือประชุมร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย

ไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของ กปช. จัดทำแนวปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นแนวปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับแนวปฏิบัติและกรอบมาตรฐาน ให้นำแนวปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

ส่วนที่ ๒
การบริหารจัดการ

มาตรา ๔๔ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๒ (๔) ด้วย

ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๔๕ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

ในกรณีที่มีการเปลี่ยนแปลงเจ้าหน้าที่ตามวรรคหนึ่ง ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งให้สำนักงานทราบโดยเร็ว

มาตรา ๔๖ ในกรณีที่การปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ต้องอาศัยความรู้ความเชี่ยวชาญ กปช. หรือคณะกรรมการตามมาตรา ๑๑ อาจมอบหมายให้ เลขาธิการว่าจ้างผู้เชี่ยวชาญตามความเหมาะสมเฉพาะงานได้

ผู้เชี่ยวชาญตามวรรคหนึ่งต้องมีคุณสมบัติหรือประสบการณ์ที่เหมาะสมตามที่ กปช. ประกาศกำหนด

(โปรดพลิก)

เลขาธิการต้องออกบัตรประจำตัวผู้เชี่ยวชาญให้แก่บุคคลที่ได้รับการแต่งตั้ง และในการปฏิบัติหน้าที่ บุคคลดังกล่าวต้องแสดงบัตรหรือหลักฐานประจำตัวในฐานะผู้เชี่ยวชาญ และเมื่อพ้นจากหน้าที่แล้วจะต้องคืนบัตรประจำตัวแก่สำนักงานโดยเร็ว

ส่วนที่ ๓
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๗ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ และเป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๘ ให้ กปช. มีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข

(๘) ด้านอื่นตามที่ กปช. ประกาศกำหนดเพิ่มเติม

การพิจารณาประกาศกำหนดภารกิจหรือบริการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่ กปช. กำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ กปช. จะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราวๆ ไปตามความเหมาะสม

มาตรา ๔๙ ให้ กปช. มีอำนาจประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของหน่วยงานศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๘ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๘ ทั้งหมดหรือบางส่วนก็ได้

การพิจารณาประกาศกำหนดภารกิจหรือบริการของหน่วยงานตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่ กปช. กำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ กปช. จะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราวๆ ไปตามความเหมาะสม

มาตรา ๕๐ กรณีมีข้อสงสัยหรือข้อโต้แย้งเกี่ยวกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่มีการประกาศกำหนดตามมาตรา ๔๘ หรือ มาตรา ๔๙ ให้ กปช. เป็นผู้วินิจฉัยชี้ขาด

มาตรา ๕๑ เพื่อประโยชน์ในการติดต่อประสานงาน ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งรายชื่อและข้อมูลการติดต่อของ เจ้าของกรรมสิทธิ์ ผู้ดูแลและครอบครองคอมพิวเตอร์และระบบคอมพิวเตอร์ไปยังสำนักงานหน่วยงานควบคุมหรือกำกับดูแลของตนและหน่วยงานตามมาตรา ๔๙ ภายในสามสิบวันนับแต่วันที่ กปช. ประกาศตามมาตรา ๔๘ วรรคสอง และมาตรา ๔๙ วรรคสอง หรือนับแต่วันที่ กปช. มีคำวินิจฉัยตามมาตรา ๕๐ แล้วแต่กรณี โดยอย่างน้อย เจ้าของกรรมสิทธิ์ ผู้ดูแลและครอบครองคอมพิวเตอร์และระบบคอมพิวเตอร์ต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น

ในกรณีที่มีการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ดูแลและครอบครองคอมพิวเตอร์และระบบคอมพิวเตอร์ตามวรรคหนึ่ง ให้แจ้งการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้องตามวรรคหนึ่งก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่าเจ็ดวัน เว้นแต่มีเหตุจำเป็นอันไม่อาจก้าวล่วงได้ให้แจ้งโดยเร็ว

มาตรา ๕๒ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าไม่ได้มาตรฐานให้ส่งเรื่องให้ กปช. หรือ กสส. พิจารณา

หาก กปช. หรือ กสส. เห็นว่า มีเหตุอันควรเชื่อได้จริงว่าคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดภายใต้หน่วยงานควบคุมหรือกำกับดูแล ไม่ได้ดำเนินการตามมาตรฐานขั้นต่ำตามประมวลแนวทางปฏิบัติ หรือหลักเกณฑ์ของการทำหน้าที่ในฐานะโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือมีเหตุอันควรเชื่อได้ว่า หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการผิดเงื่อนไขที่ กปช. หรือ กสส. กำหนด จนอาจทำให้เกิดภัยคุกคามไซเบอร์ กปช. หรือ กสส. อาจมีคำสั่งให้เลขาธิการ ดำเนินการดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้ กปช. เสนอต่อนายกรัฐมนตรี หรือคณะรัฐมนตรีเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐาน

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล เพื่อใช้มาตรการต่างๆ ตามหน้าที่และอำนาจ เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นดำเนินการแก้ไขจนได้มาตรฐาน

มาตรา ๕๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

(โปรดพลิก)

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงาน ภายในสามสิบวัน นับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๔ ในกรณีที่ กปช. หรือ กสส. เห็นว่า การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๔๖ ไม่เป็นไปตามมาตรฐานตามรายงานของหน่วยงานควบคุมหรือกำกับดูแล กปช. หรือ กสส. อาจสั่งให้เลขาธิการมีคำสั่งให้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นจัดให้มีการดำเนินการอีกครั้งหนึ่ง รวมทั้งอาจมอบหมายให้ผู้เชี่ยวชาญดำเนินการประเมินความเสี่ยงหรือตรวจสอบในด้านอื่น ๆ ที่มีผลต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ได้จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่งแล้ว แต่ กปช. หรือ กสส. เห็นว่ายังไม่เป็นไปตามมาตรฐาน กปช. หรือ กสส. อาจมีคำสั่งให้เลขาธิการดำเนินการดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้ กปช. เสนอต่อนายกรัฐมนตรี หรือคณะรัฐมนตรี เพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐาน

(๒) กรณีเป็นหน่วยงานภาคเอกชน ให้แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล เพื่อใช้มาตรการต่างๆ ตามหน้าที่และอำนาจ เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นดำเนินการแก้ไขจนได้มาตรฐาน

มาตรา ๕๕ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กปช. หรือ กสส. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๖ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงาน และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์ ทั้งนี้ กปช. หรือ กกซ. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

ส่วนที่ ๔
การรับมือกับภัยคุกคามทางไซเบอร์

มาตรา ๕๗ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

มาตรา ๕๘ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา ๕๗ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานตามมาตรา ๔๙ รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการดังต่อไปนี้

(๑) สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๒) แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

มาตรา ๕๙ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ กปช. และหรือ กกช. จะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(โปรดพลิก)

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

(ค) เป็นภัยคุกคามที่มีความรุนแรงที่ก่อหรืออาจก่อให้เกิดความเสียงภัยหรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่สำคัญหรือมีจำนวนมาก

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

(ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์จำนวนมากถูกทำลายในวงกว้างในระดับประเทศ

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

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้ กปช. เป็นผู้ประกาศกำหนด

มาตรา ๖๐ เมื่อปรากฏแก่ กปช. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กปช. ดำเนินการ หรือมอบหมายให้ กกช. ออกคำสั่งให้สำนักงานดำเนินการดังต่อไปนี้

(๑) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๒) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๓) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากการคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๔) สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๕) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

(๖) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชนเพื่อจัดการความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๖๑ ในการดำเนินการตามตามมาตรา ๖๐ เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ กกซ. อาจสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ ดังต่อไปนี้

(๑) มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์

(๒) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(๓) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวพันกับภัยคุกคามทางไซเบอร์

(๔) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่ามีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น

ผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

มาตรา ๖๒ ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ กปช. หรือ กกซ. อาจขอให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

กปช. หรือ กกซ. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาตามวรรคหนึ่งในลักษณะที่อาจก่อให้เกิดความเสียหาย และให้ กกซ. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว

ให้นำความในวรรคหนึ่งและวรรคสองมาใช้บังคับในการร้องขอต่อเอกชนโดยความยินยอมของเอกชนนั้นด้วย

มาตรา ๖๓ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง กกซ. อาจให้เลขาธิการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตามวรรคหนึ่ง ให้ กปช. หรือ กกซ. มีอำนาจสั่งให้เลขาธิการมีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการใดหรือระงับการดำเนินการใดๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้

(โปรดพลิก)

อย่างเหมาะสมและมีประสิทธิภาพตามที่เห็นสมควร รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที

ให้เลขาธิการรายงานการดำเนินการตามมาตรานี้ต่อ กปช. หรือ กกช. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กปช. หรือ กกช. โดยเร็ว

มาตรา ๖๔ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการดังต่อไปนี้

(๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใดๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (๕) ให้ กปช. หรือ กกช. มอบหมายให้เลขาธิการ ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง หรือผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๕ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ในเรื่องดังต่อไปนี้

(๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (๓) และ (๔) ให้ กปช. หรือ กกช. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงาน เจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๖ ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายนี้

มาตรา ๖๗ ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ กปช. มีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้ทันทีโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าวแล้วเสร็จ ให้ กปช. หรือ กกช. แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

ในกรณีร้ายแรงหรือวิกฤติเพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือ ปราบปราม ระงับ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการโดยความเห็นชอบของ กปช. หรือ กกช. มีอำนาจขอข้อมูลเวลาจริงจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยผู้นั้นต้องให้ความร่วมมือและให้ความสะดวกแก่ กปช. หรือ กกช. โดยเร็ว

มาตรา ๖๘ ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวังเท่านั้น

หมวด ๔
บทกำหนดโทษ

มาตรา ๖๙ ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามพระราชบัญญัติฉบับนี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามพระราชบัญญัติฉบับนี้ให้แก่บุคคลใด

(โปรดพลิก)

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบหรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่โดยมิชอบหรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๐ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนตามพระราชบัญญัติฉบับนี้ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ได้มาตามตามพระราชบัญญัติฉบับนี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๗๑ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามพระราชบัญญัติฉบับนี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ต่อสำนักงานตามมาตรา ๕๖ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

มาตรา ๗๓ ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ตามมาตรา ๖๑ (๑) หรือ (๒) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๗๔ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กปช. หรือ กกช. ตามมาตรา ๖๔ (๑) และ (๒) โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบกำหนดระยะเวลาที่พนักงานเจ้าหน้าที่ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กปช. หรือ กกช. ตามมาตรา ๖๔ (๓) และ (๔) ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นห้าพันบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๕ ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่ง หรือไม่ให้ความสะดวกแก่เลขาธิการหรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติการตามคำสั่งของเลขาธิการตามมาตรา ๖๕ โดยไม่มีเหตุอันสมควร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหนึ่งแสนห้าหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๖ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ

หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

บทเฉพาะกาล

มาตรา ๗๗ ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้ ให้นายกรัฐมนตรีอาศัยอำนาจตามข้อ ๖ (๙) (๑๐) และ (๑๑) ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ จัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว และแต่งตั้งกรรมการผู้ทรงคุณวุฒิ หรือดำเนินการอื่นใดเป็นการชั่วคราวไปด้วย

มาตรา ๗๘ กปช. อาจขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการ รัฐวิสาหกิจหรือองค์กรอื่นของรัฐมาปฏิบัติงานในสำนักงานเป็นการชั่วคราวได้ โดยทำความตกลงกับหน่วยงานของรัฐนั้น

ให้ถือว่าข้าราชการ พนักงาน หรือลูกจ้างที่มาปฏิบัติงานในสำนักงานเป็นการชั่วคราวตามวรรคหนึ่งไม่ขาดจากสถานภาพเดิมและคงได้รับเงินเดือนหรือค่าจ้าง แล้วแต่กรณี จากสังกัดเดิม ทั้งนี้ กปช. อาจกำหนดค่าตอบแทนพิเศษให้แก่ข้าราชการ พนักงาน หรือลูกจ้างของหน่วยงานของรัฐตามวรรคหนึ่ง ในระหว่างปฏิบัติงานในสำนักงานด้วยก็ได้

มาตรา ๗๙ เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรีเสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราวตามมาตรา ๗๗ ที่มีอยู่ในวันที่พระราชบัญญัตินี้ใช้บังคับ ไปเป็นของสำนักงานตามพระราชบัญญัตินี้

มาตรา ๘๐ ในระหว่างที่ยังไม่มีข้อบังคับ ระเบียบ หรือประกาศของสำนักงานตามพระราชบัญญัตินี้ ให้นำข้อบังคับ ระเบียบ ประกาศ หรือข้อกำหนดของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราวตามมาตรา ๗๗ ในส่วนที่เกี่ยวกับการปฏิบัติงานหรืออำนาจหน้าที่ที่จะเป็นของสำนักงานตามพระราชบัญญัตินี้ มาใช้บังคับโดยอนุโลม

กรณีที่มีปัญหาในการบังคับใช้หรือการตีความข้อบังคับ ระเบียบ ประกาศ หรือข้อกำหนดตามวรรคหนึ่ง ให้คณะกรรมการกำกับสำนักงานเป็นผู้วินิจฉัยชี้ขาดหรือมีมติตามที่เห็นสมควร

ผู้รับสนองพระราชโองการ

.....

นายกรัฐมนตรี

บันทึกวิเคราะห์สรุป
สาระสำคัญของร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

คณะรัฐมนตรีได้มีมติให้เสนอพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ต่อสภานิติบัญญัติแห่งชาติ และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดทำบันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติฯ ดังต่อไปนี้

๑. เหตุผลและความจำเป็นในการเสนอร่างพระราชบัญญัติ

โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้

๒. สาระสำคัญของร่างพระราชบัญญัติ

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... แบ่งออกเป็น ๔ หมวด จำนวน ๘๐ มาตรา มีสาระสำคัญสรุปได้ ดังต่อไปนี้

๒.๑ บททั่วไป

๒.๑.๒ กำหนดวันใช้บังคับ โดยให้พระราชบัญญัตินี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป (ร่างมาตรา ๒)

๒.๑.๒ กำหนดบทนิยามคำว่า "การรักษาความมั่นคงปลอดภัยไซเบอร์" คำว่า "ภัยคุกคามทางไซเบอร์" คำว่า "ไซเบอร์" คำว่า "ประมวลแนวทางปฏิบัติ (Code of Practice)" คำว่า "เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident)" คำว่า "มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Solution)" เพื่อให้ทราบถึงมาตรการในการดำเนินการเพื่อที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และลักษณะภัยที่จะถือว่าเป็นภัยคุกคามทางไซเบอร์ และกำหนดบทนิยามคำว่า "โครงสร้างพื้นฐานสำคัญทางสารสนเทศ" คำว่า "หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ"และคำว่า "หน่วยงานควบคุมหรือกำกับดูแล" เพื่อกำหนดลักษณะและขอบเขตของหน่วยงานที่มีภารกิจหรือให้บริการในกิจการอันเป็นโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ อันจะต้องมีการกำกับดูแล

(โปรดพลิก)

เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นพิเศษ นอกจากนี้ ได้กำหนดบทนิยามคำอื่น ๆ เพื่อรองรับบทบัญญัติต่าง ๆ ในพระราชบัญญัตินี้ (ร่างมาตรา ๓)

๒.๑.๓ กำหนดให้นายกรัฐมนตรีเป็นผู้รักษาการตามพระราชบัญญัตินี้ (ร่างมาตรา ๔)

๒.๒ หมวด ๑ คณะกรรมการ

๒.๒.๑ ส่วนที่ ๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(๑) กำหนดให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) ประกอบด้วยนายกรัฐมนตรี เป็นประธานกรรมการ รองนายกรัฐมนตรีฝ่ายความมั่นคงเป็นรองประธานกรรมการ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รัฐมนตรีว่าการกระทรวงการคลัง รัฐมนตรีว่าการกระทรวงการต่างประเทศ รัฐมนตรีว่าการกระทรวงคมนาคม รัฐมนตรีว่าการกระทรวงพลังงาน รัฐมนตรีว่าการกระทรวงมหาดไทย รัฐมนตรีว่าการกระทรวงยุติธรรม เลขาธิการ กอ.รมน. ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เป็นกรรมการ โดยมีเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นกรรมการและเลขานุการ (ร่างมาตรา ๕ ถึงร่างมาตรา ๘)

(๒) กำหนดหน้าที่และอำนาจของ กปช. โดยให้มีหน้าที่และอำนาจดังนี้ ๑) เสนอนโยบาย ส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้คณะรัฐมนตรีให้ความเห็นชอบ ๒) กำหนดนโยบายให้หน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมถึงนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ๓) กำกับดูแลการจัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงานเพื่อเสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ๔) แต่งตั้งและถอดถอนเลขาธิการ ๕) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ อำนาจหน้าที่และกรอบการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๖) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ ๗) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรีเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ๘) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงประมวลแนวทางปฏิบัติ และกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ๙) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางนโยบายในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ (ร่างมาตรา ๙)

(๓) กำหนดให้มีคณะที่ปรึกษา มีหน้าที่และอำนาจในการรวบรวมความคิดเห็น ให้คำปรึกษาและข้อเสนอแนะ หรือดำเนินการอย่างหนึ่งอย่างใดตามที่ กปช. มอบหมาย (ร่างมาตรา ๑๐)

๒.๒.๒ ส่วนที่ ๒ คณะกรรมการเฉพาะด้าน

(๑) กำหนดให้มีคณะกรรมการเฉพาะด้านเพื่อปฏิบัติหน้าที่เกี่ยวกับการดำเนินการต่าง ๆ ตามหน้าที่และอำนาจของ กชป. ดังนี้

(๑.๑) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กกช.) มีรองนายกรัฐมนตรีฝ่ายความมั่นคงเป็นประธานกรรมการ โดยมีหน้าที่และอำนาจดังนี้ ๑) ติดตามการดำเนินการตามนโยบายและแผนในส่วนที่เกี่ยวข้อง ๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์(๓) กำกับดูแลการดำเนินงานเพื่อเป็นศูนย์กลางการประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (THAI CERT) และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ ๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน ๕) ประสานงานและให้ความร่วมมือในการตั้งหน่วยงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (CERT) ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ ๖) ร่วมกันประสานงานกับหน่วยงานอื่น ๆ ในการกำหนดกรอบและความร่วมมือที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานในประเทศและต่างประเทศ ๗) กำหนดระดับของภัยคุกคามทางไซเบอร์พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อ กปช. ๘) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อ กปช. พิจารณาสั่งการเมื่อมีภัยคุกคามระดับร้ายแรงขึ้น

(๑.๒) คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส.) มีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ โดยมีหน้าที่และอำนาจ ดังนี้ ๑) ติดตามการดำเนินการตามนโยบายและแผนในส่วนที่เกี่ยวข้อง ๒)ดำเนินการเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๓) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของผู้ควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้ผู้ควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๔) ส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดมาตรฐานบังคับขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมใบรับรองมาตรฐานความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชน ๕) กำหนดมาตรการและแนวทาง

(โปรดพลิก)

ในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานรัฐและหน่วยงานเอกชน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑.๓) คณะกรรมการเฉพาะด้านอื่น ซึ่ง กปช. แต่งตั้งโดยความเห็นชอบของคณะรัฐมนตรีเพื่อปฏิบัติหน้าที่ตามที่ กปช. กำหนด
(ร่างมาตรา ๑๑ ถึงร่างมาตรา ๑๕)

๒.๓ หมวด ๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒.๓.๑ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(๑) กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ หรือกฎหมายอื่น (ร่างมาตรา ๑๙ ถึงร่างมาตรา ๒๐)

(๒) กำหนดหน้าที่และอำนาจของสำนักงาน โดยให้รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กปช. และให้มีหน้าที่และอำนาจต่าง ๆ อันเป็นการสนับสนุนการทำงานของ กปช. และปฏิบัติการต่าง ๆ เพื่อรองรับการทำงานในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที (ร่างมาตรา ๒๑ ถึงร่างมาตรา ๒๒)

๒.๓.๒ คณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (คกส.)

(๑) กำหนดให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคน เป็นกรรมการ และให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นกรรมการและเลขานุการของ คกส. ทั้งนี้ กรรมการผู้ทรงคุณวุฒินั้น ให้รัฐมนตรีแต่งตั้งจากบุคคล ซึ่งมีความรู้ ความเชี่ยวชาญ และความสามารถตามที่กำหนด และมีวาระการดำรงตำแหน่งคราวละสี่ปี (ร่างมาตรา ๒๔ ถึงร่างมาตรา ๒๕)

(๒) กำหนดหน้าที่และอำนาจของคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้มีหน้าที่และอำนาจในการกำหนดนโยบายการบริหารงาน ให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน ออกข้อบังคับเกี่ยวกับการจัดการองค์กรและการบริหารงานบุคคลของสำนักงาน อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปี ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการ และอำนาจในการบริหารงานในเรื่องอื่น ๆ ตามที่กำหนด รวมทั้งกำหนดบทบัญญัติเกี่ยวกับการประชุม การแต่งตั้งอนุกรรมการและที่ปรึกษาของคณะกรรมการกำกับสำนักงาน การกำหนดเบี้ยประชุมและค่าตอบแทนอื่น (ร่างมาตรา ๒๖ ถึงร่างมาตรา ๒๗)

๒.๓.๓ กำหนดให้มีเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรับผิดชอบการปฏิบัติงานของสำนักงานขึ้นตรงต่อ กปช. และกรรมการเฉพาะด้าน โดยมีหน้าที่และอำนาจในการบริหารงานของสำนักงาน วางระเบียบภายใต้นโยบายของ กปช. และ

กรรมการเฉพาะด้าน และเป็นผู้บังคับบัญชาและประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงาน (ร่างมาตรา ๒๘ ถึงร่างมาตรา ๓๕)

๒.๓.๔ กำหนดแบบและหลักเกณฑ์เกี่ยวกับการบัญชีของสำนักงาน ระยะเวลาในการจัดทำงบดุล งบการเงินและบัญชี ของสำนักงาน (ร่างมาตรา ๓๖ ถึงร่างมาตรา ๓๗)

๒.๓.๕ กำหนดให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล และมติคณะรัฐมนตรีที่เกี่ยวข้อง (ร่างมาตรา ๓๙)

๒.๔ หมวด ๓ การรักษาความมั่งคงปลอดภัยไซเบอร์

๒.๔.๑ ส่วนที่ ๑ นโยบายและแผน

(๑) กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์จะต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและเอกชนต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ โดยการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งหมายเพื่อสร้างศักยภาพในการตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ร่างมาตรา ๔๐)

(๒) กำหนดเป้าหมายและแนวทางของนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (ร่างมาตรา ๔๑)

(๓) กำหนดให้ กปช. จัดทำนโยบายส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยเมื่อได้ประกาศในราชกิจจานุเบกษาแล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนด ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว (ร่างมาตรา ๔๒)

(๔) กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยแผนการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และ แผนการรับมือกับภัยคุกคามทางไซเบอร์ โดยให้นำแนวปฏิบัติและกรอบมาตรฐานที่สำนักงานจัดทำขึ้นไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นแนวปฏิบัติของหน่วยงานของตน และหากหน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับแนวปฏิบัติและกรอบมาตรฐาน ให้นำแนวปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ (ร่างมาตรา ๔๓)

๒.๔.๒ ส่วนที่ ๒ การบริหารจัดการ

(๑) กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีหน้าที่ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานและจะต้องดำเนินการให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ นอกจากนี้จะต้องแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานด้วย (ร่างมาตรา ๔๔ และร่างมาตรา ๔๕)

(โปรดพลิก)

(๒) กำหนดให้เลขาธิการสามารถว่าจ้างผู้เชี่ยวชาญตามความเหมาะสมเฉพาะงานได้ (ร่างมาตรา ๔๖)

๒.๔.๓ ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) กำหนดความสำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศและกำหนดให้เป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ (ร่างมาตรา ๔๗)

(๒) กำหนดให้ กปช. มีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข หรือด้านอื่นตามที่ กปช. ประกาศกำหนดเพิ่มเติมเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ กปช. จะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม (ร่างมาตรา ๔๘)

(๓) กำหนดให้ กปช. มีอำนาจประกาศกำหนดลักษณะ หน้าที่ และความรับผิดชอบของหน่วยงานศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ และกรณีมีข้อสงสัยหรือข้อโต้แย้งเกี่ยวกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่มีการประกาศกำหนดตามมาตรา ๔๘ หรือมาตรา ๔๙ ให้ กปช. เป็นผู้วินิจฉัยชี้ขาด (ร่างมาตรา ๔๙ และร่างมาตรา ๕๐)

(๔) กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งรายชื่อและข้อมูลการติดต่อของ เจ้าของกรรมสิทธิ์ ผู้ดูแลและครอบครองคอมพิวเตอร์และระบบคอมพิวเตอร์ไปยังสำนักงานหน่วยงานควบคุมหรือกำกับดูแลของตนและหน่วยงานตามมาตรา ๔๙ โดยอย่างน้อยต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น (ร่างมาตรา ๕๑)

(๕) กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่งคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน (ร่างมาตรา ๕๒)

(๖) กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดส่งสรุปรายงานการดำเนินการต่อสำนักงานภายในระยะเวลาที่กฎหมายกำหนด และในกรณีที่ กปช. หรือ กสส. เห็นว่า การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ไม่เป็นไปตามมาตรฐานตามรายงานของหน่วยงานควบคุมหรือกำกับดูแล กปช. หรือ กสส. อาจสั่งให้เลขาธิการมีคำสั่งให้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นจัดให้มีการดำเนินการอีกครั้งหนึ่ง ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ได้จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่งแล้ว แต่ กปช. หรือ กสส. เห็นว่ายังไม่เป็นไปตามมาตรฐาน กปช. หรือ กสส. อาจมีคำสั่งให้เลขาธิการดำเนินการดังต่อไปนี้

๑) กรณีเป็นหน่วยงานของรัฐ ให้ กปช. เสนอต่อนายกรัฐมนตรี หรือคณะรัฐมนตรี เพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐาน ๒) กรณีเป็นหน่วยงานภาคเอกชน ให้แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแล เพื่อใช้มาตรการต่างๆ ตามหน้าที่และอำนาจ เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นดำเนินการแก้ไขจนได้มาตรฐาน (ร่างมาตรา ๕๓ และร่างมาตรา ๕๔)

(๗) กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น (ร่างมาตรา ๕๕)

(๘) ในกรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดังกล่าวรายงานต่อสำนักงาน และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์ (ร่างมาตรา ๕๖)

๒.๔.๔ ส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์

(๑) กำหนดหน้าที่และอำนาจของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานนั้น ๆ โดยให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว และในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน (ร่างมาตรา ๕๗)

(๒) กำหนดหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล ในกรณีปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา ๕๗ โดยให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานตามมาตรา ๔๙ รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการสนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมทั้งแจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว (ร่างมาตรา ๕๘)

(๓) กำหนดอำนาจให้ กปช. และหรือ กกช. ในกรณีการพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ โดยให้ กปช. และหรือ กกช. มีอำนาจกำหนดลักษณะ

(โปรดพลิก)

ของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ได้แก่ ๑) ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง ๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และ ๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ทั้งนี้ รายละเอียดของลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้ กปช. เป็นผู้ประกาศกำหนด (ร่างมาตรา ๕๙)

(๔) กำหนดหน้าที่และอำนาจของ กปช. ในกรณีปรากฏแก่ กปช. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยให้ กปช. ดำเนินการ หรือมอบหมายให้ กกช. ออกคำสั่งให้สำนักงานดำเนินการรวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้อง เพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากการคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น และให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชนเพื่อจัดการความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และในการดำเนินการดังกล่าว เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ กกช. อาจสั่งให้พนักงานเจ้าหน้าที่มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูล มีหนังสือขอข้อมูล เอกสาร ซึ่งอยู่ในความครอบครองของผู้อื่น สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ และเข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องโดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น (ร่างมาตรา ๖๐ และร่างมาตรา ๖๑)

(๕) กำหนดหน้าที่และอำนาจของ กปช. หรือ กกช. ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยให้ กปช. หรือ กกช. อาจขอให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และ กปช. หรือ กกช. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาในลักษณะที่อาจก่อให้เกิดความเสียหาย และให้ กกช. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว (ร่างมาตรา ๖๒)

(๖) กำหนดหน้าที่และอำนาจของ กปช. กกช. และเลขาธิการ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง โดย กกช. อาจให้เลขาธิการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินการตามมาตรการที่จำเป็น และให้ กปช. หรือ กกช. มีอำนาจสั่งให้เลขาธิการมีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอรให้กระทำการใดหรือระงับการดำเนินการใด ๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามที่เห็นสมควร และให้เลขาธิการรายงานการดำเนินการต่อ กปช. หรือ กกช. อย่างต่อเนื่อง (ร่างมาตรา ๖๓)

(๗) กำหนดอำนาจของ กปช. หรือ กกช. ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยให้ กปช. หรือ กกช. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการเฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่ รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์ เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ให้ กปช. หรือ กกช. มอบหมายให้เลขาธิการ ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง หรือผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว (ร่างมาตรา ๖๔)

(๘) กำหนดอำนาจของ กปช. และ กกช. ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยให้ กปช. หรือ กกช. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ในเรื่องดังต่อไปนี้ ได้แก่ ๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น ๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ในการดำเนินการตาม ๓) และ ๔) ให้ กปช. หรือ กกช. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง

(โปรดพลิก)

ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว (ร่างมาตรา ๖๕)

(๙) กำหนดให้กรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายนี้ ส่วนกรณีที่เป็นเหตุจำเป็นเร่งด่วน ให้ กปช. มีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้ทันทีโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าวแล้วเสร็จ ให้ กปช. หรือ กกช. แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว และในกรณีร้ายแรงหรือวิกฤติเพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือ ปราบปราม ระงับ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการโดยความเห็นชอบของ กปช. หรือ กกช. มีอำนาจขอข้อมูลเวลาจริงจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยผู้นั้นต้องให้ความร่วมมือและให้ความสะดวกแก่ กปช. หรือ กกช. โดยเร็ว (ร่างมาตรา ๖๖ และร่างมาตรา ๖๗)

(๑๐) กำหนดให้ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวังเท่านั้น (ร่างมาตรา ๖๘)

๒.๕ หมวด ๗ บทกำหนดโทษ

กำหนดโทษทางอาญาในกรณีพนักงานเจ้าหน้าที่และพนักงานสอบสวนเปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการที่ได้มาตามพระราชบัญญัติฉบับนี้ให้แก่บุคคลใด และในกรณีกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่ได้มาตามพระราชบัญญัติฉบับนี้ และผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามพระราชบัญญัติฉบับนี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด กรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ต่อสำนักงาน และกรณีที่บุคคลใดขัดขวางหรือไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ที่ใช้อำนาจตามกฎหมาย ต้องได้รับโทษทางอาญาตามที่กำหนดไว้ ตลอดจนกำหนดความรับผิดในทางอาญาของผู้แทนนิติบุคคล (ร่างมาตรา ๖๙ ถึงร่างมาตรา ๗๕)

๒.๖ บทเฉพาะกาล

กำหนดให้ในวาระเริ่มแรกที่ยังไม่มีการจัดตั้งสำนักงาน ให้นายกรัฐมนตรีอาศัยอำนาจตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ จัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว และแต่งตั้งคณะกรรมการผู้ทรงคุณวุฒิหรือดำเนินการอื่นใดเป็นการชั่วคราว กำหนดให้ กปช. ขอให้ข้าราชการ พนักงาน หรือลูกจ้างของส่วนราชการรัฐวิสาหกิจหรือองค์กรอื่นของรัฐมาปฏิบัติงานในสำนักงานเป็นการชั่วคราวได้ ทั้งนี้ เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรี (นายกรัฐมนตรี) เสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษา

ความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติชั่วคราว ไปเป็นของสำนักงานตามพระราชบัญญัตินี้ (ร่างมาตรา ๗๗ ถึงร่างมาตรา ๘๐)

๓. ประโยชน์ที่ประชาชนจะได้รับ

การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง จะส่งผลดีและสร้างความเชื่อมั่นในการขับเคลื่อนเศรษฐกิจดิจิทัลของประเทศไทยต่อประเทศอื่น และนำไปสู่การพัฒนาเศรษฐกิจสังคมได้อย่างยั่งยืนต่อไป โดยเฉพาะอย่างยิ่งจะทำให้ประชาชนได้รับบริการจากระบบที่เป็นบริการอันเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัย รวมทั้งมีหน่วยงานและกลไกในการให้ความช่วยเหลือ สนับสนุน ในการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ มีเจตนารมณ์เพื่อเป็นการป้องกัน รับมือ และลดความเสี่ยงภัยจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งเป็นการสร้างความเข้มแข็งให้ระบบการให้บริการผ่านออนไลน์ของหน่วยงานรัฐและเอกชนให้ดียิ่งขึ้น โดยมีหน่วยงานรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการให้บริการเป็นไปอย่างมีประสิทธิภาพและต่อเนื่อง

แผนการจัดทำกฎหมายลำดับรอง
ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

ที่	ร่างมาตรา	กฎหมายลำดับรอง	สาระสำคัญ	ระยะเวลา
๑	มาตรา ๔	ประกาศที่นายกรัฐมนตรีกำหนดเกี่ยวกับหลักเกณฑ์การแต่งตั้งพนักงานเจ้าหน้าที่	กำหนดคุณสมบัติของบุคคลที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ เพื่อปฏิบัติการตามพระราชบัญญัตินี้	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๒	มาตรา ๕	ระเบียบที่รัฐมนตรีกำหนดเกี่ยวกับหลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิ	กำหนดคุณสมบัติและองค์ประกอบของคณะกรรมการผู้ทรงคุณวุฒิ รวมถึงวิธีการได้มาซึ่งกรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๓	มาตรา ๑๐	ระเบียบที่ กปช. กำหนดเกี่ยวกับหลักเกณฑ์และวิธีการแต่งตั้งคณะที่ปรึกษา	กำหนดคุณสมบัติ ลักษณะต้องห้าม องค์ประกอบวิธีปฏิบัติหน้าที่ วาระการดำรงตำแหน่ง และการพ้นจากตำแหน่งของคณะที่ปรึกษา	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๔	มาตรา ๑๑	ระเบียบที่ กปช. กำหนดเกี่ยวกับหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ	กำหนดคุณสมบัติและองค์ประกอบของกรรมการผู้ทรงคุณวุฒิ รวมถึงวิธีการได้มาซึ่งกรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๕	มาตรา ๑๕ มาตรา ๒๖	หลักเกณฑ์และวิธีการที่ กปช. กำหนดเกี่ยวกับการแต่งตั้งอนุกรรมการที่เป็นชาวต่างประเทศ	กำหนดคุณสมบัติและองค์ประกอบของอนุกรรมการที่เป็นชาวต่างประเทศ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๖	มาตรา ๑๖	ระเบียบที่ กปช. กำหนดเกี่ยวกับหลักเกณฑ์การประชุมของคณะกรรมการ	กำหนดหลักเกณฑ์หรือแนวทางเกี่ยวกับวิธีการประชุมของคณะกรรมการ ซึ่งรวมถึงวิธีการทางอิเล็กทรอนิกส์	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๗	มาตรา ๑๗	หลักเกณฑ์ที่คณะรัฐมนตรีกำหนดว่าด้วยเบี้ยประชุมและค่าตอบแทนอื่นของคณะกรรมการ	กำหนดหลักเกณฑ์รายละเอียดเกี่ยวกับการได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นของประธานกรรมการ กรรมการ กรรมการ ที่ปรึกษาคณะกรรมการ ประธานอนุกรรมการและอนุกรรมการ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้

(โปรดพลิก)

ที่	ร่างมาตรา	กฎหมายลำดับรอง	สาระสำคัญ	ระยะเวลา
๘	มาตรา ๑๘	ประกาศที่ กปช. กำหนดเกี่ยวกับระดับความรู้ความชำนาญและบัตรประจำตัวของพนักงานเจ้าหน้าที่	เพื่อกำหนดรายละเอียดเกี่ยวกับความรู้ความชำนาญ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่และลักษณะรูปแบบของบัตรประจำตัวพนักงานเจ้าหน้าที่	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๙	มาตรา ๒๑	ระเบียบที่ กปช. กำหนดเกี่ยวกับอำนาจหน้าที่ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	เพื่อกำหนดหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๐	มาตรา ๒๔	หลักเกณฑ์และวิธีการที่ กปช. กำหนดเกี่ยวกับการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ คกส.	กำหนดคุณสมบัติและองค์ประกอบของคณะกรรมการผู้ทรงคุณวุฒิของ คกส.	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๑	มาตรา ๒๖	หลักเกณฑ์และวิธีการที่กำหนด กปช. กำหนดเกี่ยวกับการแต่งตั้งผู้ทรงคุณวุฒิเป็นที่ปรึกษา	กำหนดคุณสมบัติและองค์ประกอบของผู้ทรงคุณวุฒิเพื่อเป็นที่ปรึกษา คกส.	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๒	มาตรา ๒๗	หลักเกณฑ์ที่ กปช. กำหนดว่าด้วยเบี้ยประชุมและค่าตอบแทนอื่น	กำหนดหลักเกณฑ์รายละเอียดเกี่ยวกับการได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นของประธานกรรมการ กรรมการ ประธานอนุกรรมการ และอนุกรรมการ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราช-บัญญัติประกาศใช้
๑๓	มาตรา ๓๑	หลักเกณฑ์ที่คณะรัฐมนตรีกำหนดเกี่ยวกับการกำหนดหลักเกณฑ์อัตราเงินเดือนและค่าตอบแทนอื่นของเลขาธิการ	กำหนดอัตราเงินเดือนและค่าตอบแทนอื่นของเลขาธิการ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๔	มาตรา ๓๓	ข้อบังคับหรือระเบียบที่ กปช. กำหนดเกี่ยวกับหลักเกณฑ์การประเมิน	กำหนดระยะเวลาและวิธีการประเมินผลการปฏิบัติงานของเลขาธิการ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน

ที่	ร่างมาตรา	กฎหมายลำดับรอง	สาระสำคัญ	ระยะเวลา
		ผลการปฏิบัติงานของเลขาธิการ		หลังจากพระราชบัญญัติประกาศใช้
๑๕	มาตรา ๓๕	ข้อบังคับที่ คกส. กำหนดเกี่ยวกับการมอบอำนาจ	กำหนดรายละเอียดเกี่ยวกับการมอบอำนาจในการปฏิบัติหน้าที่ให้บุคคลใดในสังกัดของสำนักงาน	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๖	มาตรา ๓๖	หลักเกณฑ์ที่ คกส. กำหนดเกี่ยวกับหลักเกณฑ์การบัญชี	กำหนดแบบและหลักเกณฑ์เกี่ยวกับการบัญชีของสำนักงาน ให้เป็นไปตามหลักสากลและมาตรฐานการบัญชี	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๗	มาตรา ๔๖	ประกาศที่ กปช. หรือ กกช. หรือ กสส. กำหนดเกี่ยวกับคุณลักษณะของผู้เชี่ยวชาญ	กำหนดรายละเอียดเกี่ยวกับคุณลักษณะ ความรู้ความเชี่ยวชาญของผู้เชี่ยวชาญที่สามารถได้รับการว่าจ้างเฉพาะงานได้	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๘	มาตรา ๔๘	ประกาศที่ กปช. กำหนดเกี่ยวกับหน่วยงานที่มีภารกิจหรือบริการที่มีลักษณะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	กำหนดประเภทหรือชื่อหน่วยงานที่มีภารกิจหรือบริการที่มีลักษณะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๑๙	มาตรา ๔๙	ประกาศที่ กปช. กำหนดเกี่ยวกับการพิจารณาทบทวนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	กำหนดรายละเอียดเพื่อจะนำมาใช้พิจารณาทบทวนความพร้อมของหน่วยงานที่มีภารกิจหรือบริการที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้
๒๐	มาตรา ๕๖	หลักเกณฑ์และวิธีการที่ กปช. หรือ กกช. กำหนดเกี่ยวกับวิธีการรายงาน	กำหนดรายละเอียดเกี่ยวการรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้

(โปรดพลิก)

ที่	ร่างมาตรา	กฎหมายลำดับรอง	สาระสำคัญ	ระยะเวลา
๒๑	มาตรา ๕๙	ประกาศที่ กปช. กำหนดเกี่ยวกับลักษณะของภัยคุกคามทางไซเบอร์	กำหนดรายละเอียดเกี่ยวลักษณะภัยคุกคาม มาตราป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ	คณะกรรมการกำหนดระเบียบภายใน ๑๒๐ วัน หลังจากพระราชบัญญัติประกาศใช้

หลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist)

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

☑ กฎหมายใหม่ ☐ แก้ไข / ปรับปรุง ☐ ยกเลิก

ส่วนราชการหรือหน่วยงานผู้เสนอ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑. วัตถุประสงค์และเป้าหมายของภารกิจ

๑.๑ วัตถุประสงค์และเป้าหมายของภารกิจ

เพื่อให้ประเทศไทยสามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ และอย่างต่อเนื่อง

เพื่อแก้ไขปัญหาหรือข้อบกพร่องใด

ปัจจุบันประเทศไทยยังไม่มีหน่วยงานรับผิดชอบในระดับประเทศ เพื่อทำหน้าที่เป็นหน่วยงานกลางในบูรณาการการจัดการกับสถานการณ์และภัยคุกคามทางไซเบอร์ จึงส่งผลทำให้การปกป้อง คุ้มครอง ป้องกัน แก้ไข และการรับมือกับสถานการณ์และภัยคุกคามทางไซเบอร์ทั้งในภาครัฐและเอกชนเป็นไปอย่างล่าช้าและขาดการบูรณาการ ไม่เท่าทันต่อสถานการณ์ ขาดความต่อเนื่อง ขาดประสิทธิภาพ และไม่เป็นเอกภาพ

๑.๒ ความจำเป็นที่ต้องทำภารกิจ

เนื่องจากปัจจุบันภัยคุกคามทางไซเบอร์ได้ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมอย่างรุนแรงจนก่อให้เกิดความเสียหายทั้งในระดับบุคคล และระดับประเทศ อันกระทบต่อ ความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคง ทางเศรษฐกิจ ดังนั้น เพื่อปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ตลอดจนการเสริมสร้างความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ จึงจำเป็นต้องมีหน่วยงานกลางในระดับประเทศเพื่อรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งต้องอาศัยความรวดเร็วตลอดจนการบูรณาการ และประสานการปฏิบัติร่วมกันทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน เพื่อป้องกันและรับมือได้ทัน สถานการณ์ เพื่อป้องกันภัยทางไซเบอร์ในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และ สถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการ ตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างมีประสิทธิภาพและเป็นเอกภาพ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

หากไม่ทำภารกิจนั้นจะมีผลประการใด

หากไม่ทำภารกิจจะส่งผลให้การดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ ซึ่งต้องอาศัยความรวดเร็วตลอดจนการบูรณาการและประสานการปฏิบัติร่วมกันของบุคคลที่เกี่ยวข้องกับโลกไซเบอร์ทั้งหน่วยงานของรัฐ หน่วยงานเอกชน ภาคประชาสังคม ภาควิชาการ และผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์เป็นไปอย่างล่าช้า หรืออาจจะไม่สามารถได้รับความร่วมมือจากบุคคลที่เกี่ยวข้องกับโลกไซเบอร์เหล่านั้นจนทำให้ไม่สามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และเป็นเอกภาพ และส่งผลกระทบทั้งด้านสังคม เศรษฐกิจ การเมืองและทางการทหารจนกลายเป็นปัญหาด้านความมั่นคงของประเทศ ต่อไป

(โปรดพลิก)

๑.๓ การดำเนินการเพื่อให้บรรลุวัตถุประสงค์มีกี่ทางเลือก มีทางเลือกอะไรบ้าง

ไม่มีทางเลือกอื่น

๑.๔ มาตรการที่บรรลุวัตถุประสงค์ของภารกิจคืออะไร

(๑) ให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อทำหน้าที่กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ กำหนดขั้นตอนการดำเนินการเพื่อให้มีการประสานความร่วมมือและอำนวยความสะดวกในการดำเนินการกับคณะกรรมการที่ตั้งขึ้นตามกฎหมายฉบับอื่น หน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน กำหนดมาตรการและแนวทางในการยกระดับทักษะความเชี่ยวชาญระดับสูงของเจ้าพนักงานผู้ปฏิบัติหน้าที่จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดทำรายงานสรุปผลการดำเนินงานที่มีผลกระทบอย่างมีนัยสำคัญรายงานให้สภาความมั่นคงแห่งชาติและคณะรัฐมนตรีทราบตามลำดับ สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

(๒) ให้มีหน่วยงานในระดับประเทศ เพื่อทำหน้าที่เป็นหน่วยงานกลางในการบูรณาการการจัดการกับสถานการณ์และรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเป็นหน่วยงานบังคับใช้กฎหมายสั่งการ การบูรณาการและประสานการปฏิบัติร่วมกันทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน เพื่อป้องกันและรับมือได้ทันสถานการณ์ทั้งในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่าง ร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างมีประสิทธิภาพ และเป็นเอกภาพ รวมทั้งมีการดูแลรักษาความมั่นคง ปลอดภัยไซเบอร์อย่างต่อเนื่อง

(๓) ให้มีพนักงานเจ้าหน้าที่เพื่อปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

(๔) กำหนดโทษทางอาญาแก่หน่วยงานของรัฐ และหน่วยงานเอกชนที่กระทำการฝ่าฝืนบทบัญญัติแห่งพระราชบัญญัติฉบับนี้ที่มีผลต่อการบังคับใช้กฎหมายซึ่งอาจก่อให้เกิดผลเสียหายแก่ประเทศ อีกทั้งกำหนดโทษเพื่อมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ให้แก่บุคคลใด

๑.๕ ภารกิจนั้นจะแก้ไขปัญหาหรือข้อบกพร่องนั้นได้เพียงใด

เมื่อมีหน่วยงานกลางในระดับประเทศ เพื่อรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ จะทำให้เกิดความรวดเร็วในการบูรณาการและประสานการปฏิบัติร่วมกันทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน และสามารถป้องกันและรับมือได้ทันสถานการณ์ ทั้งในสถานการณ์เฝ้าระวัง สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างมีประสิทธิภาพ และเป็นเอกภาพ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

๑.๖ ผลสัมฤทธิ์ของภารกิจคืออะไร

สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ และอย่างต่อเนื่อง

ตัวชี้วัดความสัมฤทธิ์ของกฎหมายมีอย่างไร

เมื่อเกิดเหตุวิกฤติหรือเหตุการณ์ร้ายแรงจากภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบต่อข้อมูลและระบบของหน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลอื่นใด จะมีหน่วยงานที่มีศักยภาพในจัดการกับสถานการณ์และรับผิดชอบในการก้ไขสถานการณ์ที่เกิดขึ้น เพื่อระงับ ยับยั้ง หรือบรรเทาผลร้ายจากอันตรายและความเสียหายที่เกิดขึ้นกับข้อมูลและระบบได้อย่างทันท่วงที

๑.๗ การทำภารกิจสอดคล้องกับพันธกรณีและความผูกพันตามหนังสือสัญญาที่ประเทศไทยมีต่อรัฐต่างประเทศหรือองค์กรระหว่างประเทศใด ในเรื่องใด

ไม่มี

๒. ผู้ทำภารกิจ

๒.๑ เมื่อคำนึงถึงประสิทธิภาพ ต้นทุน และความคล่องตัวแล้ว เหตุใดจึงไม่ควรให้เอกชนทำภารกิจนี้

เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจเพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศหรือต่อประชาชนจำนวนมาก และการทำภารกิจนี้จะต้องเป็นแบบเดียวกันทั้งประเทศ ดังนั้น ร่างกฎหมายฉบับนี้จึงกำหนดให้ภาครัฐเป็นผู้ต้องทำภารกิจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยตนเอง เพราะองค์กรของรัฐสามารถจัดสร้างเครือข่ายในการปฏิบัติภารกิจได้อย่างกว้างขวางและครอบคลุมทุกพื้นที่ทั่วประเทศได้ นอกจากนี้ หากเป็นการดำเนินงานเพื่อประโยชน์ของสังคมส่วนรวมแล้ว องค์กรของรัฐยังสามารถขอรับงบประมาณสนับสนุนการดำเนินงานได้อย่างเต็มที่และเพียงพอต่อการปฏิบัติภารกิจให้สำเร็จลุล่วงได้อย่างมีประสิทธิภาพและต่อเนื่อง

ภารกิจนี้ควรทำร่วมกับเอกชนหรือไม่ อย่างไร

ร่างกฎหมายฉบับนี้ได้กำหนดให้ภาคเอกชนมีส่วนร่วมในกรณีเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นในระบบสารสนเทศซึ่งอยู่ในความดูแลของหน่วยงานเอกชน ให้หน่วยงานเอกชนรายงานเหตุดังกล่าวไปยังหน่วยงานที่กำหนดขึ้นโดยเร็ว

๒.๒ เมื่อคำนึงถึงประสิทธิภาพและประโยชน์ที่จะเกิดแก่การให้บริการประชาชน ควรทำภารกิจนี้ร่วมกับหน่วยงานอื่นหรือไม่ เพราะเหตุใด

การดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่ประชาชนจะต้องมีการประสานและการปฏิบัติร่วมกันของบุคคลที่เกี่ยวข้องกับโลกไซเบอร์ทั้งหน่วยงานของรัฐ หน่วยงานเอกชน ภาคประชาสังคม ภาควิชาการ และผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์ในลักษณะการบูรณาการเพื่อร่วมกันจัดการกับสถานการณ์และภัยคุกคามทางไซเบอร์

๒.๓ ภารกิจดังกล่าวหากให้องค์กรปกครองส่วนท้องถิ่นทำ จะได้ประโยชน์แก่ประชาชนมากกว่าหรือไม่

เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจเพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศหรือต่อประชาชนจำนวนมาก และการทำภารกิจนี้จะต้องเป็นแบบเดียวกันทั้งประเทศ ดังนั้น จึงไม่อาจให้องค์กรปกครองส่วนท้องถิ่นทำภารกิจดังกล่าวโดยลำพังได้

๓. ความจำเป็นในการตรากฎหมาย

๓.๑ การจัดทำภารกิจนั้นมีความสอดคล้องกับเรื่องใด อย่างไร

☑ **หน้าที่หลักของหน่วยงานของรัฐ ตามภารกิจพื้นฐาน** (Function) ในเรื่องการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ

(โปรดพลิก)

☑ **หน้าที่ของรัฐและแนวนโยบายแห่งรัฐ** ในเรื่องการเพิ่มศักยภาพทางเศรษฐกิจของประเทศตามนโยบายของคณะรัฐมนตรีที่ได้มีการแถลงต่อสภานิติบัญญัติแห่งชาติ เมื่อวันที่ ๑๒ กันยายน ๒๕๕๗ ภายใต้ข้อ ๖.๑๘

☑ **ยุทธศาสตร์ชาติ** ในเรื่องยุทธศาสตร์ที่ ๑ ด้านความมั่นคง ยุทธศาสตร์ที่ ๒ ด้านการสร้างความสามารถในการแข่งขัน ยุทธศาสตร์ที่ ๔ ด้านการสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม

☑ **แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ (ฉบับที่ ๑๒)**ในเรื่องการพัฒนาเศรษฐกิจดิจิทัล ซึ่งอยู่ภายใต้ยุทธศาสตร์ที่ ๓ การสร้างความเข้มแข็งทางเศรษฐกิจและแข่งขันได้อย่างยั่งยืน และยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่ง

☑ **แนวทางการปฏิรูปประเทศ ในเรื่อง** ในเรื่องวาระการปฏิรูปที่สำคัญและเร่งด่วน (๒๗ วาระ) ในปี ๒๕๕๘ สภาขับเคลื่อนการปฏิรูปประเทศ

๓.๒ การทำภารกิจนั้นสามารถใช้มาตรการทางบริหารโดยไม่ต้องออกกฎหมายได้หรือไม่

ไม่อาจใช้มาตรการทางการบริหารแต่เพียงอย่างเดียวได้ เนื่องจากร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เป็นการตรากฎหมายขึ้นมาเพื่อใช้บังคับกับหน่วยงานของรัฐ ภาคเอกชน และประชาชนทั่วไป ให้ต้องปฏิบัติ ซึ่งมาตรการทางบริหารเป็นมาตรการภายใน ไม่สามารถนำมาบังคับใช้กับหน่วยงานเอกชนและประชาชาชนทั่วไปได้

ถ้าใช้มาตรการทางบริหารจะมีอุปสรรคอย่างไร

ไม่สามารถนำมาบังคับใช้กับหน่วยงานเอกชนและประชาชนทั่วไปได้ เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจเพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศหรือต่อประชาชนจำนวนมาก และการทำภารกิจนี้จะต้องเป็นแบบเดียวกันทั้งประเทศ ซึ่งจำเป็นต้องใช้อำนาจรัฐในการดำเนินการเพื่อการบังคับใช้กฎหมายและการสั่งการ

๓.๓ ในการทำภารกิจนั้น เหตุใดจึงจำเป็นต้องตรากฎหมายในขณะนี้

เนื่องจากผลกระทบอันเกิดจากภัยทางไซเบอร์เกิดขึ้นได้ภายในระยะเวลาอันรวดเร็ว และสร้างความเสียหายด้านต่าง ๆ อย่างร้ายแรงและเป็นวงกว้าง แต่ประเทศไทยยังไม่มีหน่วยงานรับผิดชอบในระดับประเทศเพื่อทำหน้าที่เป็นหน่วยงานกลางในบูรณาการการจัดการกับสถานการณ์และภัยคุกคามทางไซเบอร์ จึงส่งผลทำให้การปกป้อง คุ้มครอง ป้องกัน แก้ไข และการรับมือกับสถานการณ์และภัยคุกคามทางไซเบอร์ทั้งในภาครัฐและเอกชนเป็นไปอย่างล่าช้าและขาดการบูรณาการ ไม่เท่าทันต่อสถานการณ์ ขาดความต่อเนื่อง ขาดประสิทธิภาพและไม่เป็นเอกภาพ จึงจำเป็นต้องตรากฎหมายในขณะนี้ เพื่อให้ประเทศมีแผนยุทธศาสตร์ มาตรการ และแนวทางการปกป้อง ป้องกัน ระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต การสื่อสารโทรคมนาคม และดาวเทียม เพื่อนำมาปฏิบัติในการคุ้มครอง ปกป้อง ป้องกัน แก้ไข และรับมือกับภัยคุกคามต่อระบบเหล่านี้ ไม่ให้ส่งผลกระทบต่อความมั่นคงของชาติในทุกมิติอย่างเร่งด่วน

๓.๔ การใช้บังคับกฎหมายและระยะเวลาในการบังคับใช้กฎหมาย

(ก) การใช้บังคับกฎหมาย

☑ ต้องใช้บังคับพร้อมกันทุกท้องที่ทั่วประเทศ เนื่องจาก เป็นกฎหมายเกี่ยวกับการจัดตั้งหน่วยงานของรัฐเพื่อใช้อำนาจรัฐในการสั่งการ และดำเนินการตามภารกิจเพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศหรือต่อประชาชนจำนวนมากและการดำเนินการตามภารกิจนี้จะต้องเป็นแบบเดียวกันในทุกท้องที่ทั่วทั้งประเทศ

☐ ทยอยใช้บังคับเป็นท้องที่ ๆ ไป เนื่องจาก .....

☐ ใช้บังคับเพียงบางท้องที่ เนื่องจาก .....

(ข) ระยะเวลาในการใช้บังคับกฎหมาย

☐ ใช้บังคับทันทีที่ประกาศในราชกิจจานุเบกษา เนื่องจาก .....

☐ มีการทอดระยะเวลาในการบังคับใช้เป็นเวลานานเท่าใด เพราะเหตุใด .....

☐ ควรกำหนดระยะเวลาการสิ้นสุดไว้ด้วยหรือไม่ เพราะเหตุใด .....

๓.๕ เหตุใดจึงไม่สมควรตราเป็นกฎในลักษณะอื่น เช่น ข้อบัญญัติท้องถิ่น

เนื่องจากภัยคุกคามทางไซเบอร์มีความรุนแรงและส่งผลกระทบต่อประชาชนเป็นวงกว้าง ทั้งในระดับบุคคลและระดับประเทศ การดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศหรือต่อประชาชนจำนวนมากจะต้องเป็นแบบเดียวกันในทุกท้องที่ทั่วทั้งประเทศ จึงไม่อาจตราเป็นกฎในลักษณะอื่นได้

๓.๖ ลักษณะการใช้บังคับ

☐ ควบคุม ☐ กำกับ/ติดตาม (ข้ามไปข้อ ๓.๘) ☐ ส่งเสริม

☑ ระบบผสม (ระบบควบคุม กำกับ/ติดตาม และส่งเสริม)

เหตุใดจึงต้องใช้ระบบดังกล่าว

เนื่องจากภารกิจและการดำเนินการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์อาจใช้ทั้งการสั่งการเพื่อควบคุมสถานการณ์ การกำกับ/ติดตาม เพื่อให้ภาคส่วนที่เกี่ยวข้องกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง หรือให้รายงานผลการปฏิบัติการตามระดับความร้ายแรงของสถานการณ์ และอาจต้องมีมาตรการส่งเสริมเพื่อสร้างแรงจูงใจให้ภาคส่วนที่เกี่ยวข้องดำเนินการ เช่น การใช้มาตรการยกเว้นภาษีสำหรับหน่วยงานเอกชนที่ได้ใช้จ่ายเพื่อจัดให้มีระบบสำหรับการปกป้อง คุ้มครอง ป้องกัน แก้ไข และการรับมือกับสถานการณ์และภัยคุกคามทางไซเบอร์

๓.๗ การใช้ระบบอนุญาตในกฎหมาย

๓.๗.๑ เพราะเหตุใดจึงกำหนดให้ใช้ระบบอนุญาต หรือใช้ระบบอื่นที่มีผลเป็นการควบคุม

.....

๓.๗.๒ มีการกำหนดค่าธรรมเนียมการอนุญาตหรือไม่ ถ้ามี มีความจำเป็นอย่างไร คุ้มค่าต่อภาระที่เกิดแก่ประชาชนอย่างไร

.....

(โปรดพลิก)

๓.๗.๓ มีหลักเกณฑ์การใช้ดุลพินิจในการอนุญาตหรือไม่ อย่างไร

.....

๓.๗.๔ มีขั้นตอนและระยะเวลาที่แน่นอนในการอนุญาตหรือไม่

.....

๓.๗.๕ มีการเปิดโอกาสให้อุทธรณ์การปฏิเสธคำขอ การให้ยื่นขอใหม่หรือไม่ อย่างไร

.....

๓.๗.๖ มีการต่ออายุการอนุญาตหรือไม่

.....

มีการตรวจสอบก่อนการต่อใบอนุญาตหรือไม่

.....

๓.๘ การใช้ระบบคณะกรรมการในกฎหมาย

๓.๘.๑ กฎหมายที่จะตราขึ้นมีการใช้ระบบคณะกรรมการ หรือไม่ มีความจำเป็นอย่างไร

เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจเพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศหรือต่อประชาชนจำนวนมากและเป็นวงกว้าง การทำภารกิจนี้จะต้องเป็นแบบเดียวกันทั้งประเทศ ดังนั้น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ... จึงจำเป็นต้องกำหนดให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อทำหน้าที่ กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ กำหนดขั้นตอนการดำเนินการเพื่อให้มีการประสานความร่วมมือและอำนวยความสะดวกในการดำเนินการกับคณะกรรมการที่ตั้งขึ้นตามกฎหมายฉบับอื่น หน่วยงานของรัฐหรือ หน่วยงานภาคเอกชน กำหนดมาตรการและแนวทางในการยกระดับทักษะความเชี่ยวชาญระดับสูงของเจ้าพนักงานผู้ปฏิบัติหน้าที่ จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดทำรายงานสรุปผลการดำเนินงานที่มีผลกระทบอย่างมีนัยสำคัญรายงานให้สภาความมั่นคงแห่งชาติและคณะรัฐมนตรีทราบตามลำดับ สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

๓.๘.๒ คณะกรรมการที่กำหนดขึ้นมีอำนาจซ้ำซ้อนกับคณะกรรมการอื่นหรือไม่

ไม่มีอำนาจซ้ำซ้อน

หากมีความซ้ำซ้อน จะดำเนินการอย่างไรกับคณะกรรมการอื่นนั้น

-

๓.๘.๓ องค์ประกอบของคณะกรรมการผู้มีอำนาจมีผู้ดำรงตำแหน่งทางการเมือง หรือนายกรัฐมนตรี หรือหัวหน้าส่วนราชการหรือไม่

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกอบด้วยบุคคล ดังต่อไปนี้

- นายกรัฐมนตรี เป็นประธานกรรมการ
- รองนายกรัฐมนตรีฝ่ายความมั่นคง เป็นรองประธานกรรมการ
- กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รัฐมนตรีว่าการกระทรวงการคลัง รัฐมนตรีว่าการกระทรวงการต่างประเทศ

รัฐมนตรีว่าการกระทรวงคมนาคม รัฐมนตรีว่าการกระทรวงพลังงาน รัฐมนตรีว่าการกระทรวงมหาดไทย รัฐมนตรีว่าการกระทรวงยุติธรรม เลขาธิการ กอ.รมน. ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

- กรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้ง

เหตุจึงต้องกำหนดให้บุคคลดังกล่าวเป็นองค์ประกอบของคณะกรรมการ

เพื่อให้มีการประสานนโยบายและเชื่อมโยงการทำงานร่วมกันระหว่างหน่วยงานของรัฐที่เกี่ยวข้องทั้งมิติด้านความมั่นคงและด้านเศรษฐกิจ

๓.๙ มีกรอบหรือแนวทางการใช้ดุลพินิจของเจ้าหน้าที่หรือไม่ อย่างไร

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ได้กำหนดให้ผู้ที่มีหน้าที่สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชน ต้องปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ ในกรณีที่เป็นไปเพื่อป้องกัน รับมือ หรือลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ คณะกรรมการหรือเลขาธิการมีอำนาจออกคำสั่งเท่าที่จำเป็นเพื่อป้องกันหรือบรรเทาความเสียหาย ส่วนในกรณีที่มีผลกระทบต่อบุคคลอื่น เลขาธิการจะต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้สิทธิแก่เจ้าหน้าที่ในการปฏิบัติการที่มีผลกระทบต่อบุคคลอื่น

๓.๑๐ ประเภทของโทษที่กำหนด

☑ **โทษทางอาญา** **โทษทางปกครอง** **ระบบผสม**

๓.๑๑ การกำหนดโทษทางอาญาจะทำให้การบังคับใช้กฎหมายสัมฤทธิ์ผล เพราะเหตุใด

เนื่องจากร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เป็นกฎหมายเกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีความรุนแรงที่จะส่งผลให้เกิดความเสียหายทั้งในระดับบุคคล และระดับประเทศอันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางทหาร ความสงบเรียบร้อยภายในประเทศและความมั่นคงทางเศรษฐกิจ จึงต้องมีการตรากฎหมายที่มีโทษทางอาญามาบังคับใช้เพื่อประโยชน์ในการคุ้มครองปกป้อง และเพื่อสร้างความสงบเรียบร้อยให้เกิดขึ้นทั้งทั้งในโลกไซเบอร์และโลกแห่งความเป็นจริง

๓.๑๒ ความผิดที่กำหนดให้เป็นโทษทางอาญาเป็นความผิดที่มีความร้ายแรงอย่างไร

ในหมวดบทกำหนดตามร่างกฎหมายนี้ ได้กำหนดโทษไว้สองประการ คือ โทษจำคุก โทษปรับ หรือทั้งจำทั้งปรับ ทั้งนี้ ความร้ายแรงของโทษขึ้นอยู่กับพฤติการณ์และความเสียหายที่เกิดขึ้นโดยอ้างอิงและเทียบเคียงอัตราโทษตามประมวลกฎหมายอาญาเป็นสำคัญ

๔. ความซ้ำซ้อนกับกฎหมายอื่น

๔.๑ การดำเนินการตามภารกิจในเรื่องนี้มีกฎหมายอื่นในเรื่องเดียวกันหรือทำนองเดียวกันหรือไม่

ไม่มี

๔.๒ ในกรณีที่มีกฎหมายขึ้นใหม่ เหตุใดจึงไม่ยกเลิก แก้ไขหรือปรับปรุงกฎหมายในเรื่องเดียวกันหรือทำนองเดียวกันที่มีอยู่

ไม่มี

(โปรดพลิก)

๕. ผลกระทบและความคุ้มค่า

๕.๑ ผู้ซึ่งได้รับผลกระทบจากการบังคับใช้กฎหมาย คือ

หน่วยงานของรัฐ ภาคเอกชน และประชาชนทั่วไป

☑ **ผู้มีหน้าที่ตามร่างกฎหมายหรือที่จะได้รับผลกระทบจากร่างกฎหมายนั้นโดยตรง**

หน่วยงานของรัฐ ภาคเอกชน และประชาชนทั่วไปที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ มีหน้าที่ต้องรายงานผลกระทบดังกล่าว ในกรณีเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นในระบบสารสนเทศซึ่งอยู่ในความดูแลของตน เพื่อประโยชน์ในการวิเคราะห์และนำไปสู่การกำหนดมาตรการเพื่อการแก้ไขสถานการณ์อันเกิดจากภัยคุกคามทางไซเบอร์ในอนาคต

☐ **ผู้ที่อยู่ในพื้นที่ที่อาจได้รับผลกระทบจากร่างกฎหมาย**.....

๕.๒ ผลกระทบที่เกิดขึ้นแก่บุคคลดังกล่าว

☑ **ด้านเศรษฐกิจและสังคม**

- เชิงบวก

การกำหนดให้หน่วยงานของรัฐ ภาคเอกชน และประชาชนทั่วไปที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์มีหน้าที่ต้องรายงานผลกระทบดังกล่าว ในกรณีเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นในระบบซึ่งอยู่ในความดูแลของตน เพื่อประโยชน์ในการวิเคราะห์และนำไปสู่การกำหนดมาตรการเพื่อการแก้ไขสถานการณ์อันเกิดจากภัยคุกคามทางไซเบอร์ในอนาคต นั้น ย่อมส่งผลทำให้เกิดการปกป้อง คุ้มครอง ป้องกัน แก้ไข และสามารถรับมือกับสถานการณ์และภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้นทั้งในภาครัฐและเอกชน ซึ่งจะส่งผลดีและช่วยบรรเทาความเสียหายที่จะเกิดขึ้น และนำไปสู่การลดต้นทุนในการแก้ไขปรับปรุงระบบได้ในอนาคต

ผู้ได้รับผลกระทบเชิงบวก.....

ภาครัฐ ภาคเอกชน และประชาชนทุกภาคส่วน

- เชิงลบ

ไม่มี

ผู้ได้รับผลกระทบเชิงลบ

ไม่มี

๕.๓ สิทธิและเสรีภาพของบุคคลในเรื่องใดบ้างที่ต้องถูกจำกัด

ไม่มี

การจำกัดนั้นเป็นการจำกัดเท่าที่จำเป็นหรือไม่ อย่างไร

-

๕.๔ ประโยชน์ที่ประชาชนและสังคมจะได้รับ

๕.๔.๑ ประชาชนจะมีการดำรงชีวิตที่ดีขึ้นในเรื่องใด อย่างไร และเพียงใด หรือเป็นการอำนวยความสะดวกแก่ประชาชนมากน้อยเพียงใด

ประชาชนจะได้รับการปกป้อง คุ้มครอง ป้องกัน แก้ไข และสามารถรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้ อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง

๕.๔.๒ เศรษฐกิจและสังคมมีการพัฒนาอย่างยั่งยืนได้อย่างใด

การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง จะส่งผลดีและสร้างความเชื่อมั่นในการขับเคลื่อนเศรษฐกิจดิจิทัลของประเทศไทยต่อประเทศอื่น และนำไปสู่การพัฒนาเศรษฐกิจสังคมได้อย่างยั่งยืนต่อไป

การประกอบกิจการเป็นไปโดยสะดวกหรือลดต้นทุนของผู้ประกอบการได้มากน้อยเพียงใด

การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีมิให้เกิดความเสียหาย และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง จะส่งผลดีและสามารถลดต้นทุนในการแก้ไขปรับปรุงระบบซึ่งอาจหรือได้รับความเสียหายจากภัยคุกคามดังกล่าว

ยกระดับความสามารถในการแข่งขันของประเทศได้มากน้อย เพียงใด

เมื่อสามารถลดต้นทุนในการแก้ไขปรับปรุงระบบซึ่งอาจหรือได้รับความเสียหายจากภัย คุกคามทางไซเบอร์ได้แล้ว ความเชื่อมั่นในการขับเคลื่อนเศรษฐกิจดิจิทัลก็จะเกิดขึ้นในวงกว้าง และนำไปสู่การยกระดับความสามารถในการแข่งขันของประเทศได้ต่อไป

และส่งเสริมการวิจัยและพัฒนามากน้อยเพียงใด

มีคณะกรรมการซึ่งส่งเสริมการวิจัยและพัฒนาเกี่ยวกับการปกป้อง คุ้มครอง ป้องกัน แก้ไขภัยคุกคามทางไซเบอร์

๕.๔.๓ เสริมสร้างประสิทธิภาพหรือนวัตกรรมในการปฏิบัติราชการอย่างไร

การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง จะช่วยเสริมสร้างประสิทธิภาพในการปฏิบัติราชการ เนื่องจากข้อมูลและระบบที่ใช้เป็นเครื่องมือในการปฏิบัติราชการมีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างสเถียร ทำให้ข้าราชการสามารถใช้ระบบที่มีอยู่ได้อย่างต่อเนื่องไม่ติดขัดซึ่งจะนำไปสู่การต่อยอดและสร้างนวัตกรรมใหม่ ๆ ได้ต่อไป

สามารถลดงบประมาณแผ่นดินได้มากน้อย เพียงใด

เนื่องจากผลกระทบอันเกิดจากภัยทางไซเบอร์เกิดขึ้นได้ภายในระยะเวลาอันรวดเร็ว และ สร้างความเสียหายด้านต่าง ๆ อย่างร้ายแรงและเป็นวงกว้าง ดังนั้น การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง จะช่วยลดงบประมาณแผ่นดินซึ่งจะต้องถูกนำไปใช้ในการปรับปรุงแก้ไข และเยียวยาความเสียหายที่ได้รับจากภัยคุกคามดังกล่าวได้เป็นอย่างมาก

๕.๔.๔ วิธีการและระยะเวลาประเมินผลสัมฤทธิ์ ตลอดจนประโยชน์ที่ประชาชนและสังคมจะได้รับ ได้แก่

ในร่างกฎหมายนี้ได้กำหนดอำนาจหน้าที่เพื่อให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางนโยบายในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ นอกจากนี้ ยังกำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

(โปรดพลิก)

แห่งชาติมีหน้าที่รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติหน้าที่ รวมทั้งปัญหาและอุปสรรค และจัดทำรายงานสรุปผลการดำเนินงานประจำปีให้คณะรัฐมนตรีทราบ ซึ่งจะนำไปสู่การประเมินผลสัมฤทธิ์ตลอดจนประโยชน์ที่ประชาชนและสังคมจะได้รับต่อไป

๕.๕ ความยุ่งยากที่คาดว่าจะเกิดขึ้นจากการปฏิบัติตามกฎหมาย

เนื่องจากผลกระทบอันเกิดจากภัยทางภัยไซเบอร์เกิดขึ้นได้ภายในระยะเวลาอันรวดเร็ว และสร้างความเสียหายด้านต่างๆ อย่างร้ายแรงเป็นวงกว้าง และเป็นเรื่องในเชิงเทคนิคเฉพาะ ดังนั้น อาจทำให้ผู้ที่ได้รับผลกระทบจากภัยดังกล่าวมีเป็นจำนวนมากและจะต้องมีการรายงานอย่างต่อเนื่อง อย่างไรก็ตาม การรายงานอาจกำหนดให้เป็นระบบการรายงานแบบอัตโนมัติด้วยวิธีการทางอิเล็กทรอนิกส์ซึ่งจะช่วยลดความยุ่งยากในการรายงานดังกล่าวลงได้

๕.๖ ความคุ้มค่าของภารกิจเมื่อคำนึงถึงงบประมาณที่ต้องใช้ ภาระหน้าที่ที่เกิดขึ้นกับประชาชนและการที่ประชาชนจะต้องถูกจำกัดสิทธิเสรีภาพเทียบกับประโยชน์ที่ได้รับ

การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพเป็นเอกภาพ อย่างต่อเนื่อง จะช่วยเสริมสร้างความมั่นคงปลอดภัยให้เกิดขึ้นและลดความเสียหายที่จะเกิดขึ้นกับ ข้อมูลและระบบต่างๆ ในทุกภาคส่วน ซึ่งจะช่วยลดงบประมาณที่จะต้องถูกนำไปใช้ในการปรับปรุงแก้ไข และ เยียวยาความเสียหายที่ได้รับจากภัยคุกคามดังกล่าวได้เป็นอย่างมาก ทั้งนี้ เมื่อเปรียบเทียบระหว่างประโยชน์ ที่ประชาชนจะได้รับกับภาระหน้าที่และการถูกจำกัดสิทธิ์ซึ่งกำหนดไว้แล้วถือได้ว่าภารกิจนี้มีความคุ้มค่าเป็น อย่างยิ่ง

๖. ความพร้อมของรัฐ

๒.๑ ความพร้อมของรัฐ

(ก) กำลังคนที่คาดว่าต้องใช้

ประมาณ ๓๐๐ อัตรา และภายใน ๓ ปี นับจากจัดตั้งให้เพิ่มเติมเฉลี่ยร้อยละ ๒๐ ต่อไป

(ข) คุณวุฒิและประสบการณ์ของเจ้าหน้าที่ที่จำเป็นต้องมี

กำหนดให้กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้อเป็นผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(ค) งบประมาณที่คาดว่าต้องใช้ในระยะห้าปีแรกของการบังคับใช้กฎหมาย

โดยเป็นงบดำเนินงานจำนวน .... และงบลงทุนจำนวน ...

ในปีแรกของการจัดตั้ง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจำเป็นต้องใช้เงินเงินประมาณรวมทั้งสิ้นประมาณ ๓๐๐ ล้านบาท และภายในระยะเวลาห้าปีแรกของการบังคับใช้กฎหมายน่าจะต้องของบประมาณเพิ่มเติม จำนวนไม่เกินประมาณ ๒,๐๐๐ ล้านบาท

๖.๒ ในกรณีที่เป็นร่างกฎหมายที่มีผลกระทบต่อการจัดตั้งหน่วยงานหรืออัตรากำลัง มีความเห็นของหน่วยงานที่เกี่ยวข้องกับการกำหนดอัตรากำลังและงบประมาณ หรือไม่ อย่างไร

ยังไม่มีความเห็นของหน่วยงานที่เกี่ยวข้องดังกล่าว

๖.๓ วิธีการที่จะให้ผู้อยู่ภายใต้บังคับของกฎหมายมีความเข้าใจและพร้อมที่จะปฏิบัติตาม กฎหมาย

☑ **วิธีการสร้างความรับรู้ความเข้าใจแก่ประชาชนผู้อยู่ภายใต้กฎหมาย**

ได้มีการสร้างความรู้ความเข้าใจผ่านกลไกต่าง ๆ ที่มีอยู่ เช่น การประชุมรับฟังความคิดเห็นของหน่วยงานที่เกี่ยวข้อง โดยเฉพาะหน่วยงานด้านความมั่นคง

☑ **การเข้าถึงข้อมูลของประชาชน**

ในระหว่างกระบวนการจัดทำร่างพระราชบัญญัตินี้ได้จัดให้มีช่องทางในการเผยแพร่และรับฟังความคิดเห็นจากประชาชนอย่างกว้างขวาง โดยเผยแพร่บนเว็บไซต์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม http://www.mdes.go.th และเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย http://www.lawamendment.go.th รวมถึงการเปิดเวทีเผยแพร่ข้อมูลและรับฟังความคิดเห็นจากประชาชนและผู้มีส่วนเกี่ยวข้องด้วย

๗. หน่วยงานที่รับผิดชอบและผู้รักษาการตามกฎหมาย

๗.๑ มีหน่วยงานอื่นใดที่ปฏิบัติภารกิจซ้ำซ้อนหรือใกล้เคียงกันหรือไม่ มีข้อเสนอแนะในการดำเนินการกับหน่วยงานนั้นอย่างไร

ไม่มี

๗.๒ มีความเกี่ยวข้องหรือมีผลกระทบต่อการปฏิบัติงานของหน่วยงานอื่นหรือไม่ อย่างไร

ไม่มี

๗.๓ มีการบูรณาการการทำงานร่วมกับหน่วยงานอื่นหรือไม่ อย่างไร

ภารกิจของหน่วยงานกลางในระดับประเทศที่จะต้องผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการบูรณาการและประสานการปฏิบัติร่วมกันทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน เพื่อป้องกันและรับมือได้ทันสถานการณ์ เพื่อป้องกันภัยทางไซเบอร์ในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ได้อย่างมีประสิทธิภาพและเป็นเอกภาพ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

๗.๔ ผู้รักษาการตามกฎหมาย ได้แก่

นายกรัฐมนตรี

การกำหนดให้ผู้ดำรงตำแหน่งดังกล่าวเป็นผู้รักษาการตามกฎหมาย เนื่องจาก

นายกรัฐมนตรี เป็นผู้มีอำนาจสูงสุดในฝ่ายบริหารและสามารถสั่งการหน่วยงานของรัฐที่เกี่ยวข้องได้

๘. วิธีการทำงานและตรวจสอบ

๘.๑ ระบบการทำงานที่กำหนดสอดคล้องกับหลักการบริหารกิจการบ้านเมืองที่ดีหรือไม่

☑ เกิดประโยชน์สุขของประชาชน
☑ เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ
☑ มีประสิทธิภาพและและเกิดความคุ้มค่าในเชิงภารกิจของรัฐ
☑ ไม่มีขั้นตอนการปฏิบัติงานเกินความจำเป็น

(โปรดพลิก)

☑ มีการปรับปรุงภารกิจของส่วนราชการให้ทันต่อสถานการณ์
☑ ประชาชนได้รับการอำนวยความสะดวกและได้รับการตอบสนองความต้องการ
☑ มีการประเมินผลการปฏิบัติราชการอย่างสม่ำเสมอ

๘.๒ การเปิดเผยการปฏิบัติหน้าที่ของเจ้าหน้าที่รัฐ

๘.๒.๑ ในกฎหมายมีการกำหนดขั้นตอนการดำเนินการของเจ้าหน้าที่ของรัฐในเรื่องใดบ้าง แต่ละขั้นต้องใช้เวลาดำเนินการเท่าใด

ร่างกฎหมายนี้ได้กำหนดระดับของภัยคุกคามทางไซเบอร์ ออกเป็น ๓ ระดับ ได้แก่ ระดับเฝ้าระวัง ระดับร้ายแรง และระดับวิกฤติ โดยได้กำหนดวิธีการดำเนินการในกรณีปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในดับร้ายแรง ให้คณะกรรมการดำเนินการหรือมอบหมายให้คณะกรรมการเฉพาะด้านออกคำสั่งให้สำนักงานดำเนินการตามกฎหมายกำหนดเพื่อวิเคราะห์สถานการณ์ ประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งในการดำเนินการดังกล่าวคณะกรรมการเฉพาะด้านอาจสั่งให้พนักงานเจ้าหน้าที่มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด ขอข้อมูลและเอกสารที่อยู่ในความครอบครอง สอบถามบุคคล รวมถึงเข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้อง และในกรณีมีความจำเป็นอาจขอให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๒.๒ หากมีการใช้ดุลพินิจ การใช้ดุลพินิจสอดคล้องกับหลักธรรมาภิบาลและหลักนิติธรรมอย่างไร

ไม่มี

๘.๒.๓ ในการพิจารณาของเจ้าหน้าที่ใช้หลักกระจายอำนาจ หรือมอบอำนาจเพื่อให้ประชาชนได้รับการบริการที่สะดวก รวดเร็ว และมีประสิทธิภาพ อย่างไร

ไม่มี

๘.๓ มีระบบการตรวจสอบและคานอำนาจ อย่างไรบ้าง

๘.๓.๑ มีระบบการตรวจสอบการปฏิบัติงานภายในหรือไม่ อย่างไร

๑) ระบบตรวจสอบในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เพื่อป้องกันภัยคุกคามทางไซเบอร์ เพื่อประโยชน์ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง มีการกำหนดให้คณะกรรมการหรือคณะกรรมการเฉพาะด้าน โดยเลขาธิการ ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง หรือผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ ดำเนินการตามคำร้อง

๒) ร่างกฎหมายนี้ได้กำหนดให้มีระบบตรวจสอบการปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้สำนักงานฯ จัดทำรายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติการตามพระราชบัญญัติ รวมทั้งปัญหาอุปสรรค และจัดทำรายงานสรุปผลการดำเนินงานประจำปีให้คณะรัฐมนตรีทราบ

๓) ร่างกฎหมายนี้ได้กำหนดให้มีระบบตรวจสอบการปฏิบัติงานของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้คณะกรรมการฯ จัดทำรายงานสรุปผลการดำเนินงานของการ

รักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางนโยบายการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

๘.๓.๒ มีกระบวนการร้องเรียนจากบุคคลภายนอกหรือไม่ อย่างไร

มีกระบวนการร้องเรียนจากบุคคลภายนอก โดยกำหนดกลไกเพื่อให้มีช่องทางการร้องเรียนโดยสะดวกและรวดเร็วจากบุคคลภายนอกที่พบว่าการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือพนักงานเจ้าหน้าที่ไม่ถูกต้องหรือไม่เป็นไปตามกฎหมาย บุคคลภายนอกอาจแจ้งเรื่องร้องเรียนให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ทราบ

๙. การจัดทำกฎหมายลำดับรอง

๙.๑ ได้จัดทำแผนในการจัดทำกฎหมายลำดับรอง กรอบระยะเวลา ตลอดจนกรอบสาระสำคัญของกฎหมายลำดับรองนั้น หรือไม่

มีแผนการจัดทำกฎหมายลำดับรองแล้ว

ได้ยกร่างกฎหมายลำดับรองในเรื่องใดบ้าง

- การกำหนดคุณสมบัติของบุคคลที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่
- การกำหนดคุณสมบัติและองค์ประกอบของคณะกรรมการผู้ทรงคุณวุฒิในคณะกรรมการ รวมถึงวิธีการได้มาซึ่งกรรมการผู้ทรงคุณวุฒิ เพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระ
- การกำหนดคุณสมบัติ ลักษณะต้องห้าม องค์ประกอบ วิธีปฏิบัติหน้าที่ วาระการดำรงตำแหน่ง และการพ้นจากตำแหน่งของคณะที่ปรึกษา

การกำหนดคุณสมบัติและองค์ประกอบของคณะกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเฉพาะด้าน รวมถึงวิธีการได้มาซึ่งกรรมการผู้ทรงคุณวุฒิ เพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระ

- การกำหนดคุณสมบัติและองค์ประกอบของอนุกรรมการที่เป็นชาวต่างประเทศ
- การกำหนดหลักเกณฑ์หรือแนวทางเกี่ยวกับวิธีการประชุมของคณะกรรมการ
- การกำหนดหลักเกณฑ์รายละเอียดเกี่ยวกับการได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นของคณะกรรมการ
- การกำหนดรายละเอียดเกี่ยวกับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่และลักษณะรูปแบบของบัตรประจำตัวพนักงานเจ้าหน้าที่
- การกำหนดหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
- การกำหนดคุณสมบัติและองค์ประกอบของคณะกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์
- การกำหนดคุณสมบัติและองค์ประกอบของผู้ทรงคุณวุฒิเพื่อเป็นที่ปรึกษาของคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์
- การกำหนดหลักเกณฑ์รายละเอียดเกี่ยวกับการได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นของคณะกรรมการเฉพาะด้าน
- การกำหนดอัตราเงินเดือนและค่าตอบแทนอื่นของเลขาธิการ
- การกำหนดระยะเวลาและวิธีการประเมินผลการปฏิบัติงานของเลขาธิการ
- การกำหนดรายละเอียดเกี่ยวกับการมอบอำนาจในการปฏิบัติหน้าที่ให้บุคคลใดในสังกัดของสำนักงาน

(โปรดพลิก)

- การกำหนดแบบและหลักเกณฑ์เกี่ยวกับการบัญชีของสำนักงาน ให้เป็นไปตามหลักสากลและมาตรฐานการบัญชี

- การกำหนดรายละเอียดเกี่ยวกับคุณลักษณะ ความรู้ความเชี่ยวชาญของผู้เชี่ยวชาญที่สามารถได้รับการว่าจ้างเฉพาะงานได้

- การกำหนดประเภทหรือชื่อหน่วยงานที่มีภารกิจหรือบริการที่มีลักษณะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- การกำหนดรายละเอียดเพื่อจะนำมาใช้พิจารณาทบทวนความพร้อมของหน่วยงานที่มีภารกิจหรือบริการที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- กำหนดรายละเอียดเกี่ยวกับการรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- กำหนดรายละเอียดเกี่ยวกับลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

๙.๒ มีกรอบในการตราอนุบัญญัติเพื่อป้องกันการขยายอำนาจหน้าที่ของรัฐหรือเพิ่มภาระแก่บุคคลเกินสมควรอย่างไร

มี โดยการตราอนุบัญญัติจะต้องไม่ขัดต่อกฎหมาย และไม่เกินไปกว่าขอบเขตอำนาจตามที่กำหนดไว้ในร่างพระราชบัญญัตินี้

๑๐. การรับฟังความคิดเห็น

☑ มีการรับฟังความคิดเห็น ☐ ไม่ได้รับฟังความคิดเห็น

๑๐.๑ ผู้ที่เกี่ยวข้องหรืออาจได้รับผลกระทบที่รับฟังความคิดเห็น

หน่วยงานภาครัฐ

☑ **สำนักงบประมาณ** ☑ **สำนักงาน ก.พ.**

☑ **สำนักงาน ก.พ.ร.** ☐ **สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ**

หน่วยงานที่เกี่ยวข้องกับภารกิจ ได้แก่

ภาคประชาชน/องค์กรอื่นที่เกี่ยวข้อง

☑ **ประชาชนที่ได้รับหรืออาจได้รับผลกระทบ**

☑ **ประชาชนทั่วไป**

☑ **องค์กรอื่น** ได้แก่ บุคคลที่เกี่ยวข้องกับโลกไซเบอร์ หน่วยงานเอกชน ภาคประชาสังคม ภาควิชาการและผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์

๑๐.๒ มีการเปิดเผยผลการรับฟังความคิดเห็นต่อประชาชนหรือไม่ อย่างไร

มี

๑๐.๓ จัดทำสรุปผลการรับฟังรับฟังความคิดเห็นและเสนอมาประกอบการพิจารณาของคณะรัฐมนตรี

☑ จัดทำ ☐ ไม่มีการจัดทำ

ในกรณีจัดทำสรุปผลการรับฟังความคิดเห็น มีสาระสำคัญในเรื่องดังต่อไปนี้ หรือไม่

☑ วิธีการในการรับฟังความคิดเห็น

มีการเผยแพร่ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ... เพื่อให้ประชาชนสามารถแสดงความคิดเห็นได้ในเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม http://www.mdes.go.th และเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย http://www.lawamendment.go.th เปิดเวทีรับฟังความคิดเห็น รวมถึงจัดตั้งคณะทำงานปรับปรุงร่างพระราชบัญญัติ และรับฟังความคิดเห็นผ่านทางจดหมายและจดหมายอิเล็กทรอนิกส์

☑ จำนวนครั้งและระยะเวลาในการรับฟังความคิดเห็นแต่ละครั้ง

๑. รับฟังความคิดเห็นผ่านเว็บไซต์ www.lawamendment.go.th ระหว่างวันที่ ๒๗ กันยายน ถึง ๑๒ ตุลาคม ๒๕๖๑ และวันที่ ๑๖ พฤศจิกายน ถึง ๑ ธันวาคม ๒๕๖๑

๒. จัดงานประชุมสัมมนาและการประชุมหารือเพื่อรับฟังความคิดเห็นจำนวน ๘ ครั้ง ดังนี้

(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

(๕) การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๗ – ๒๘ ตุลาคม ๒๕๖๑ ณ โรงแรมแคนทารี จังหวัดพระนครศรีอยุธยา โดยผู้เข้าร่วมเป็นกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้มีส่วนเกี่ยวข้อง

(๖) การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีผู้เข้าร่วมเป็นส่วนราชการ เอกชน และผู้มีส่วนเกี่ยวข้อง

(๗) การประชุมคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยพลอากาศเอก ประจิน จั่นตอง เข้าร่วมการประชุม และคณะทำงานประกอบด้วยภาครัฐ ภาคเอกชน และภาคประชาสังคม

(๘) การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๐ พฤศจิกายน ๒๕๖๑ โดยผู้เข้าร่วมเป็นกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(โปรดพลิก)

☑ **พื้นที่ในการรับฟังความคิดเห็น**

บนเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมhttp://www.mdes.go.th และเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย http://www.lawanmendment.go.th และเวทีการประชุมสัมมนาและการรับฟังความคิดเห็น

☑ **ประเด็นที่มีการแสดงความคิดเห็น**

มีการแสดงความคิดเห็นอย่างแพร่หลายในหลายประเด็น โดยมีประเด็นที่สำคัญหลักๆ ได้แก่

๑) การกำหนดองค์ประกอบและอำนาจหน้าที่ของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒) การกำหนดลักษณะของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓) การกำหนดหน้าที่และอำนาจของพนักงานเจ้าหน้าที่

๔) วันที่มีผลใช้บังคับ

๕) ขอบเขตของกฎหมาย ความซ้ำซ้อน และการเชื่อมโยงกับกฎหมายอื่น

๖) คำนิยาม

๗) การกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๘) การรับมือภัยคุกคามทางไซเบอร์

๙) บทกำหนดโทษ

☐ **ข้อคัดค้านหรือความเห็นของหน่วยงานและผู้เกี่ยวข้องในแต่ละประเด็น**

ไม่มี

☐ **คำชี้แจงเหตุผลรายประเด็นและการนำผลการรับฟังความคิดเห็นมาประกอบการพิจารณาจัดทำร่างกฎหมาย**

ได้นำผลการรับฟังความคิดเห็นจากทุกภาคส่วนมาปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

ขอรับรองว่าการเสนอร่างพระราชบัญญัติได้ดำเนินการตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรีฯ และระเบียบว่าด้วยหลักเกณฑ์และวิธีการเสนอเรื่องต่อคณะรัฐมนตรีแล้ว

ลงชื่อ .....

(นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย)

ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑๒ ธันวาคม ๒๕๖๑

หน่วยงานผู้รับผิดชอบ กองกฎหมาย สำนักงานปลัดกระทรวงฯ

เจ้าหน้าที่ผู้รับผิดชอบ นางสาวกอบสิริ เอี่ยมสุรีย์, นายสถาพร สอนเสนา

หมายเลขติดต่อ ๐ ๒๑๔๑ ๖๗๖๓, ๖๖

สรุปผลการรับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้จัดให้มีการรับฟังความคิดเห็นและข้อเสนอแนะต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกา (เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑) เพื่อให้เป็นไปตามมติคณะรัฐมนตรี วันที่ ๔ เมษายน ๒๕๖๐ เรื่อง แนวทางการจัดทำและการเสนอร่างกฎหมายตามบทบัญญัติมาตรา ๗๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอสรุปผลการรับฟังความคิดเห็นและข้อเสนอแนะต่อร่างพระราชบัญญัติดังกล่าว ดังนี้

๑. วิธีการในการรับฟังความคิดเห็น

ในการดำเนินการตามหลักเกณฑ์และวิธีการที่กำหนดในมติคณะรัฐมนตรีเมื่อวันที่ ๔ เมษายน ๒๕๖๐ โดยเห็นชอบให้หน่วยงานของรัฐถือปฏิบัติตามแนวทางการจัดทำและการเสนอร่างกฎหมายตามบทบัญญัติตามมาตรา ๗๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยและหลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist) ในการเปิดรับฟังความคิดเห็นต่อ ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดให้มีการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... โดยมีวิธีการรับฟังความคิดเห็นดังนี้

๑.๑ การรับฟังความคิดเห็นผ่านทางเว็บไซต์เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และการรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th โดยกระทรวงฯ ได้จัดให้มีการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ ระหว่างวันที่ ๒๗ กันยายน ถึงวันที่ ๑๒ตุลาคม ๒๕๖๑ และฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง ระหว่างวันที่ ๑๖ พฤศจิกายน ถึงวันที่ ๑ ธันวาคม ๒๕๖๑

๑.๒ การจัดการประชุมสัมมนาและการประชุมหารือเพื่อรับฟังความคิดเห็นจำนวน ๘ ครั้ง ดังนี้

(๑) การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๓ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

(๒) การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๕ ตุลาคม ๒๕๖๑ เวลา ๑๔.๐๐ ถึง ๑๖.๐๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.(องค์การมหาชน) โดยเป็นการเชิญผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการและหน่วยงานที่เกี่ยวข้องกับระบบการให้บริการ

(โปรดพลิก)

ที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศเข้าร่วมรับฟังสรุปสาระสำคัญของกฎหมายและแสดงความคิดเห็นต่อร่างกฎหมายดังกล่าว

(๓) การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๙ ตุลาคม ๒๕๖๑ เวลา ๑๕.๐๐ ถึง ๑๗.๓๐ น. ณ วิทยาลัยป้องกันราชอาณาจักรเขตดินแดง กรุงเทพมหานคร โดยเป็นการรับฟังความคิดเห็นจากกลุ่มสายงานความมั่นคงเข้าร่วมแสดงความคิดเห็น

(๔) การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๑๑ ตุลาคม ๒๕๖๑ เวลา ๑๐.๐๐ ถึง ๑๒.๓๐ น. ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นการเปิดรับฟังความคิดเห็นเป็นการทั่วไป

(๕) การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 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

(๖) การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีผู้เข้าร่วมเป็นส่วนราชการ เอกชน และผู้มีส่วนเกี่ยวข้อง ทั้งนี้ ได้นำผลสรุปจากการประชุมเมื่อวันที่ ๒๗ – ๒๘ ตุลาคม ๒๕๖๑ มาเป็นข้อมูลในการพิจารณาเพื่อปรับปรุงร่างดังกล่าว

(๗) การประชุมคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งประกอบด้วยผู้แทนจากภาครัฐ ภาคเอกชน และภาคประชาสังคม และผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยที่ประชุมได้นำผลจากการพิจารณาและปรับปรุงร่างรวมทั้งประเด็นข้อห่วงใยและความคิดเห็นจากภาคส่วนที่เกี่ยวข้องที่ส่งมาเพิ่มเติมมาพิจารณาปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบันมากยิ่งขึ้น

(๘) การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๐ พฤศจิกายน ๒๕๖๑ ณ วิทยาลัยป้องกันราชอาณาจักร โดยผู้เข้าร่วมเป็นกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้แทนจากคณะกรรมการจัดทำยุทธศาสตร์ชาติ โดยได้นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่คณะทำงานฯ ได้ร่วมกันพิจารณาปรับปรุงเมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ ตามข้อ ๒.๓ มาปรับปรุงให้เหมาะสมยิ่งขึ้น

๑.๓ การรับฟังความคิดเห็นเป็นหนังสือและจดหมายอิเล็กทรอนิกส์

๒. จำนวนครั้งและระยะเวลาในการรับฟังความคิดเห็น

กระทรวงฯได้จัดให้มีการรับฟังความคิดเห็นต่อ ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... จำนวน ๑๐ ครั้ง ดังนี้

๒.๑ การรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ ผ่านทางเว็บไซต์เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และการรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th ระหว่างวันที่ ๒๗ กันยายน ถึงวันที่ ๑๒ ตุลาคม ๒๕๖๑

๒.๒ การรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง ผ่านทางเว็บไซต์เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และการรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th ระหว่างวันที่ ๑๖ พฤศจิกายน ถึงวันที่ ๑ ธันวาคม ๒๕๖๑

๒.๓ การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๓ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๒.๔ การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๕ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๒.๕ การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๙ ตุลาคม ๒๕๖๑ ณ วิทยาลัยป้องกันราชอาณาจักร

๒.๖ การประชุมสัมมนารับฟังความคิดเห็น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ เมื่อวันที่ ๑๑ ตุลาคม ๒๕๖๑ ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๒.๗ การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๗ – ๒๘ ตุลาคม ๒๕๖๑ ณ โรงแรมแคนทารี จังหวัดพระนครศรีอยุธยา

๒.๘ การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๒.๙ การประชุมคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๒.๑๐ การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๐ พฤศจิกายน ๒๕๖๑ ณ วิทยาลัยป้องกันราชอาณาจักร

๓. พื้นที่หรือกลุ่มเป้าหมายในการรับฟังความคิดเห็น

๓.๑ การรับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จเรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ ผ่านทาง

(โปรดพลิก)

เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และการรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th โดยกระทรวงฯ ได้เปิดให้มีการรับฟังความคิดเห็นเป็นการทั่วไป มีผู้เข้าร่วมแสดงความคิดเห็น ๑๓ ราย

๓.๒ การรับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง ผ่านทางเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และการรับฟังความคิดเห็นกฎหมายไทย www.lawamendment.go.th โดยกระทรวงฯ ได้เปิดให้มีการรับฟังความคิดเห็นเป็นการทั่วไป ซึ่งมีผู้เข้ามาอ่านจำนวน ๑,๑๓๒ ราย

๓.๓ การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๗ – ๒๘ ตุลาคม ๒๕๖๑ ณ โรงแรมแคนทารี จังหวัดพระนครศรีอยุธยา โดยเป็นการเชิญผู้มีส่วนได้เสียในกลุ่มผู้ประกอบการและหน่วยงานที่เกี่ยวข้องกับระบบการให้บริการที่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) เข้าร่วมพิจารณาสรุปผลการรับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกา (เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑) เพื่อนำมาพิจารณาและจัดทำเป็นข้อสรุปในการปรับปรุงร่างในประเด็นที่สำคัญ โดยแยกเป็น ๗ ประเด็น คือ (๑) วันที่มีผลใช้บังคับ (๒) ขอบเขตของกฎหมาย ความซ้ำซ้อน และการเชื่อมโยงกับกฎหมายอื่น (๓) คำนิยาม อาทิ ทรัพย์สินสารสนเทศ (๔) รูปแบบของสำนักงาน (๕) การกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๖) การรับมือภัยคุกคามทางไซเบอร์ และ (๗) บทกำหนดโทษ เพื่อให้ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบัน โดยมีเข้าร่วมการประชุมหารือจำนวน ๕๖ คน

๓.๔ การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยเป็นการเชิญส่วนราชการจำนวน ๒๐ กระทรวง รวมทั้งหน่วยงานความมั่นคง และภาคเอกชน เข้าร่วมรับฟังสรุปสาระสำคัญของร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุงขึ้นจากข้อสรุปเมื่อวันที่ ๒๗ – ๒๘ ตุลาคม ๒๕๖๑ เพื่อรับฟังความคิดเห็นต่อร่างกฎหมายดังกล่าว และนำไปปรับปรุงให้มีความเหมาะสมยิ่งขึ้นและสอดคล้องกับสถานการณ์ปัจจุบัน โดยมีผู้เข้าร่วมการประชุมหารือจำนวน ๘๘ คน

๓.๕ การประชุมคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๑ ณ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งประกอบด้วยผู้แทนจากภาครัฐ ภาคเอกชน และภาคประชาสังคม และผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เข้าร่วมประชุมพิจารณาร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุงตามข้อ ๓.๔ เพื่อรับฟังความคิดเห็นต่อร่างกฎหมายดังกล่าว และนำไปปรับปรุงให้มีความเหมาะสมยิ่งขึ้นและสอดคล้องกับสถานการณ์ปัจจุบัน โดยมีผู้เข้าร่วมการประชุมจำนวน ๙๐ คน

๓.๖ การประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เมื่อวันที่ ๒๐ พฤศจิกายน ๒๕๖๑ ณ วิทยาลัยป้องกันราชอาณาจักร โดยผู้เข้าร่วมเป็นผู้บริหารกระทรวง ฝ่ายกฎหมายของกระทรวง กรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคง

ปลอดภัยไซเบอร์แห่งชาติ และผู้แทนจากคณะกรรมการจัดทำยุทธศาสตร์ชาติ เพื่อนำความเห็นของคณะทำงานตามข้อ ๓.๔มาปรับปรุง โดยมีผู้เข้าร่วมการประชุมหารือจำนวน ๑๔ คน

๔. ประเด็นที่มีการแสดงความคิดเห็น / คำชี้แจงเหตุผลรายประเด็น

จากการที่กระทรวงฯ ได้จัดให้มีการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้วเสร็จ เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑ และฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง ผ่านทางเว็บไซต์ และโดยการจัดสัมมนาและการประชุมหารือเพื่อรับฟังความคิดเห็น รวมถึงทางหนังสือและจดหมายอิเล็กทรอนิกส์ สามารถสรุปประเด็นที่มีการแสดงความคิดเห็นได้ตามเอกสารแนบท้ายนี้

๕. ข้อคัดค้านหรือความเห็นของหน่วยงานและผู้เกี่ยวข้องในแต่ละประเด็น

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง โดยนำความคิดเห็นจากผลการรับฟังความคิดเห็นต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่ผ่านการตรวจพิจารณาจากสำนักงานคณะกรรมการกฤษฎีกา (เรื่องเสร็จที่ ๑๔๙๐/๒๕๖๑) มาพิจารณาและปรับปรุง และได้ผ่านการรับฟังความคิดเห็นจากหน่วยงานและผู้ที่เกี่ยวข้องในแต่ละประเด็นแล้วนั้น หน่วยงานและผู้เกี่ยวข้องไม่มีข้อคัดค้านในประเด็นที่ได้ปรับปรุงทั้ง ๗ ประเด็น คือ (๑) วันที่มีผลใช้บังคับ (๒) ขอบเขตของกฎหมาย ความซ้ำซ้อน และการเชื่อมโยงกับกฎหมายอื่น (๓) คำนิยาม อาทิ ทรัพย์สินสารสนเทศ (๔) รูปแบบของสำนักงาน (๕) การกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๖) การรับมือภัยคุกคามทางไซเบอร์ และ (๗) บทกำหนดโทษ

๖. การนำผลการรับฟังความคิดเห็นมาประกอบการพิจารณาจัดทำร่างกฎหมาย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้นำความคิดเห็นมาประกอบการพิจารณาจัดทำร่างกฎหมายตามขั้นตอนการปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ดังนี้

(๑) นำข้อสรุปการประชุมหารือเพื่อปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 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 โดยนำมาปรับปรุงเป็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ณ วันที่ ๑๕ พฤศจิกายน ๒๕๖๑ เพื่อนำไปรับฟังความคิดเห็นเพิ่มเติมจากหน่วยงานและผู้เกี่ยวข้อง

(๒) ได้นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ปรับปรุง ณ วันที่ ๑๕ พฤศจิกายน ๒๕๖๑ มาประชุมหารือร่วมกับส่วนราชการเอกชน และผู้มีส่วนเกี่ยวข้อง พร้อมทั้ง ได้นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

(โปรดพลิก)

ฉบับปรับปรุงเมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๑ ขึ้นรับฟังความคิดเห็นทางเว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th และเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทยwww.lawamendment.go.th เป็นระยะเวลา ๑๕ วัน ระหว่างวันที่ ๑๖ พฤศจิกายน ๒๕๖๑ ถึงวันที่ ๑ ธันวาคม ๒๕๖๑

(๓) นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ปรับปรุง ณ วันที่ ๑๕ พฤศจิกายน ๒๕๖๑ มาปรับปรุงตามความเห็นจากส่วนราชการและเอกชน และผู้มีส่วนเกี่ยวข้อง และนำเสนอต่อที่ประชุมคณะทำงานปรับปรุงร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแต่งตั้งขึ้น โดยมีองค์ประกอบจากผู้แทนจากภาครัฐ ภาคเอกชน และภาคประชาสังคม และผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบันมากยิ่งขึ้น

(๔) นำร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ปรับปรุง ณ วันที่ ๑๕ พฤศจิกายน ๒๕๖๑ และปรับปรุงตามความเห็นของคณะทำงานฯ ตาม (๓) มาปรับปรุงร่วมกับกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้แทนจากคณะกรรมการจัดทำยุทธศาสตร์ชาติ ให้เหมาะสมยิ่งขึ้น เพื่อนำเสนอต่อคณะรัฐมนตรีพิจารณา

เอกสารแนบท้ายสรุปผลการรับฟังความคิดเห็น
ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง

ตารางสรุปประเด็นที่มีการแสดงความคิดเห็นและคำชี้แจงเหตุผลรายประเด็น

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
๑.	วันมีผลใช้บังคับ	- ไม่ควรให้มีผลบังคับใช้ทันที อย่างน้อยควรเว้นระยะเวลา ๑๘๐ วัน นับแต่วันประกาศในราชกิจจานุเบกษา อย่างไรก็ตาม ความเห็นของส่วนราชการส่วนใหญ่เห็นสมควรให้มีผลใช้บังคับทันที เนื่องจากเป็นเรื่องเร่งด่วนที่อาจส่งผลกระทบและสร้างความเสียหายให้แก่ส่วนรวม หากโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกคุกคามจากภัยทางไซเบอร์ - ร่างกฎหมายฉบับนี้กำหนดหน้าที่ให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ต้องดำเนินการในหลายสิ่ง จึงควรเว้นระยะเวลา ให้หน่วยงานต่าง ๆ ได้เตรียมตัว เตรียมความพร้อมสำหรับการปฏิบัติตามกฎหมาย ไม่ควร ให้กฎหมายมีผลบังคับใช้ทันที - มาตรา ๒ “พระราชบัญญัตินี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป”	กระทรวงฯ พิจารณาแล้ว เห็นสมควรกำหนดวันที่มีผลใช้บังคับในร่างที่กระทรวงฯ ปรับปรุง เหมือนกับร่างฯ ที่ สคก. ตรวจพิจารณาฯ เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องเร่งด่วนที่อาจส่งผลกระทบและสร้างความเสียหายให้แก่ส่วนรวม หากโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกคุกคามจากภัยทางไซเบอร์ จึงสมควรให้มีผลใช้บังคับทันที (ร่าง มาตรา ๒)

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		ทางภาคเอกชนมี ความกังวลในเรื่องพร้อมของผู้ประกอบการในการปฏิบัติตามกฎหมาย	
๒.	ขอบเขตของกฎหมาย ความซ้ำซ้อน และการเชื่อมโยงกับกฎหมายอื่น	- มีความซ้ำซ้อนกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ หรือไม่ - ขอบเขตของกฎหมายนี้มีลักษณะคล้ายกับเป็นการกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอยู่ในตัว ซึ่งหน่วยงานดังกล่าวอาจเป็นหน่วยงานที่อยู่ภายใต้การกำกับดูแลของหน่วยงานอื่นอยู่แล้ว นอกจากนี้การใช้อำนาจของพนักงานเจ้าหน้าที่มีลักษณะเช่นเดียวกันกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงมีข้อพิจารณาว่าจะทำให้เกิดความซ้ำซ้อนหรือไม่ - กรณีของข้อมูล มีกฎหมายอื่นกำกับอยู่แล้ว ดังนั้น กฎหมายนี้ควรจำกัดขอบเขต เฉพาะเรื่องของโครงสร้างและเครือข่าย ทั้งนี้ ข้อมูลน่าจะเป็นเรื่องผลกระทบจากภัยคุกคามมากกว่า หากพิจารณาบนกรอบมาตรฐานดูแลความมั่นคงปลอดภัยในการเข้าถึงข้อมูลจึงน่าจะเป็นผลของการเกิด Cyber attack ดังนั้น การกำกับข้อมูลจึงน่าจะไม่เหมาะสมและตรงตามเจตนารมณ์ของกฎหมาย	ร่างฯ ที่กระทรวงฯ ปรับปรุง ไม่ขัดแย้งกับกฎหมายอื่นที่มีอยู่แล้ว แต่จะช่วยเสริมและสนับสนุนกฎหมายอื่นเพื่อทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ของประเทศ ดังจะเห็นได้จากการที่ร่างกฎหมายนี้มิได้กำหนดฐานความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ หรือฐานความผิดเกี่ยวกับการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ เนื่องจากมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใช้บังคับอยู่แล้ว นอกจากนี้ ขอบเขตของร่างกฎหมายนี้ยังสอดคล้องตามยุทธศาสตร์ชาติ แผนปฏิบัติงาน บุคลากร กรอบงบประมาณ เพื่อดูแลปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ CII ให้สามารถให้บริการต่อเนื่อง

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- ภาพรวมของโครงสร้างกฎหมาย น่าจะมี ลักษณะเหมือนกฎหมายในสถานการณ์พิเศษ จึงควรมีการกำหนดนิยามให้ชัดเจนว่าอะไรคือสถานการณ์พิเศษ ขอบเขต และห้วงเวลา	
๓.	คำนิยาม	- มีข้อคิดเห็นว่าคำนิยามมีความไม่ชัดเจน ดังนี้ o "ภัยคุกคามทางไซเบอร์" ไม่ชัดเจนว่าแค่ไหนเพียงใดจึงจะเป็นภัยคุกคามทางไซเบอร์ o "ระดับของภัยคุกคาม" o "ทรัพย์สินสารสนเทศ" - ถ้อยคำในกฎหมายยังขาดความชัดเจนอันจะก่อให้เกิดปัญหาการตีความ และทำให้ผู้ปฏิบัติไม่สามารถปฏิบัติได้อย่างถูกต้อง ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง, อย่างมีนัยสำคัญ ที่สำคัญมีจำนวนมาก, ผู้ดูแลระบบ ดังนั้น ในหลายกรณีที่ปรากฏ ความไม่ชัดเจนในร่างกฎหมายฉบับนี้ ควรมีการกำหนดประกาศหรือหลักเกณฑ์ที่มี ขอบเขตและความชัดเจน เพื่อให้ผู้ที่ต้อง ปฏิบัติตามกฎหมายสามารถดำเนินการไปได้ อย่างราบรื่น - ตามมาตรา ๓ "การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า "มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อ ป้องกัน รับมือ	ร่างฯ ที่กระทรวงฯ ปรับปรุง ได้แก้ไขเพิ่มเติม บทนิยาม (ร่าง มาตรา ๓) ดังนี้ (๓.๑) แก้ไขนิยามคำว่า "ภัยคุกคามทางไซเบอร์" เพื่อกำหนดกรอบของภัยไซเบอร์ให้ชัดเจนว่าภัยไซเบอร์หมายถึงภัยไซเบอร์ที่มีผลกระทบต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) เป็นหลัก มิใช่ภัยไซเบอร์ที่เกิดกับประชาชนทั่วไป และไม่รวมถึง Content หรือ เนื้อหาสาระ ข้อความซึ่งใช้ติดต่อสื่อสารกันโดยทั่วไป แต่เป็นเรื่องที่ส่งผลกระทบต่อโครงสร้างระบบ หรือโครงข่าย ทั้งนี้ จะต้องเป็นการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (๓.๒) ตัดนิยามคำว่า "ทรัพย์สินสารสนเทศ" ออก เพื่อให้มีความชัดเจนว่า กฎหมายนี้ต้องการคุ้มครอง ข้อมูล ระบบ และโครงข่าย แต่ไม่รวมถึง Content หรือ เนื้อหาสาระ ข้อความซึ่งใช้ติดต่อสื่อสารกันโดยทั่วไป แต่เป็นเรื่องที่ส่งผลกระทบต่อโครงสร้างระบบ หรือโครงข่าย

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์" ขอเสนอแนะให้เพิ่มคำว่า เฝ้าระวังภัยคุกคามทางไซเบอร์ด้วย - ขอเสนอแนะว่า คำนิยามคำว่า ไซเบอร์ ให้รวมถึงวิธีการทางอิเล็กทรอนิกส์ด้วย เพราะตามมาตรา ๓ บัญญัติว่า "ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือเหตุการณ์ที่กระทำด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์ - คำนิยาม "ทรัพย์สินสารสนเทศ" นั้นกว้างเกินไป เมื่อประกอบกับ "ภัยคุกคามทางไซเบอร์" นั้นอาจตีความได้ว่า รวมไปถึงทรัพย์สินสารสนเทศของประชาชนทั่วไปด้วย จึงเสนอให้ระบุให้ชัดเจนและกระชับ - คำนิยาม "ภัยคุกคามทางไซเบอร์" ควรใช้ข้อความที่รัดกุมของคำว่า "พยายามเข้าถึง" เพราะจะเป็นการกำหนดผู้กระทำความผิด	(๓.๓) เพิ่มเติมนิยามคำว่า "ประมวลแนวทางปฏิบัติ"(Code of Practice)" เพื่อให้ กปช. กำหนดเป็นมาตรฐานกลาง (๓.๔) เพิ่มเติมนิยามคำว่า "เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident)" เพื่อให้มีความชัดเจนในความหมายซึ่งเป็นคำเทคนิคเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓.๕) เพิ่มเติมนิยามคำว่า "มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Solution)" เพื่อให้มีความชัดเจนในความหมายซึ่งเป็นคำเทคนิคเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓.๖) เพิ่มเติมนิยามคำว่า "หน่วยงานควบคุมหรือกำกับดูแล" เพื่อให้มีความชัดเจนในการบังคับใช้สำหรับหน่วยงานหรือผู้ที่มีหน้าที่ควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) นอกจากนี้ เพื่อให้เกิดความชัดเจนของระดับภัยคุกคามทางไซเบอร์ ร่างฯ ที่กระทรวงฯ ปรับปรุง จึงกำหนดหลักการให้การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ กปช. และหรือ กกช. จะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ คือ ระดับเฝ้าระวัง ระดับร้ายแรง และระดับวิกฤต ทั้งนี้ รายละเอียดของลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้ กปช. เป็นผู้ประกาศกำหนด (ร่าง มาตรา ๕๙)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
๔.	องค์กร	- ควรมีเลขาธิการ สนง.คณะกรรมการสิทธิมนุษยชนแห่งชาติและผู้ตรวจการแผ่นดินเข้าร่วมเป็นกรรมการเพื่อเป็นหลักประกันการพิจารณาเรื่องสิทธิและเสรีภาพส่วนบุคคล - เนื่องจากการดำเนินกิจการบางอย่างภายใต้ขอบเขตของกฎหมายฉบับนี้เป็นการดำเนินการโดยเอกชนแต่ฝ่ายเดียว จึงควรมีตัวแทนจากภาคเอกชนเข้าร่วมในคณะกรรมการดังกล่าวด้วย - ตามมาตรา ๕ “ให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cybersecurity Committee” เรียกโดยย่อว่า “NCSC” ประกอบด้วยนายกรัฐมนตรีเป็นประธานกรรมการ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและ สังคม ปลัดกระทรวงยุติธรรม ผู้บัญชาการตารวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย ...” จึงมีข้อเสนอแนะว่า เนื่องจากกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรมีหน้าที่ในเรื่องยุทธศาสตร์ชาติ ซึ่งในยุทธศาสตร์ชาติก็มีเรื่อง cyber security ด้วย จึงประสงค์จะขอร่วมใน	ร่างฯ ที่กระทรวงฯ ปรับปรุง ได้กำหนดให้มี คณะกรรมการ กปช. และคณะกรรมการเฉพาะด้าน ซึ่งแตกต่างจากร่างฯ ที่ สคก. ตรวจพิจารณาฯ เพื่อดำเนินการตามอำนาจหน้าที่ ดังนี้ **(๔.๑) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”(กปช)** มีนายกรัฐมนตรี เป็นประธาน เหมือนเช่นร่างฯ ที่ สคก. ตรวจพิจารณาฯ แต่ได้ปรุงองค์ประกอบของกรรมการโดยตำแหน่งให้ครอบคลุมหน่วยงานที่เกี่ยวข้องมากขึ้นได้แก่รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รัฐมนตรีว่าการกระทรวง การคลัง รัฐมนตรีว่าการกระทรวงการต่างประเทศ รัฐมนตรีว่าการกระทรวงคมนาคม รัฐมนตรีว่าการกระทรวงพลังงาน รัฐมนตรีว่าการกระทรวงมหาดไทย รัฐมนตรีว่าการกระทรวงยุติธรรม เลขาธิการ กอ.รมน. ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินเจ็ดคนซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญและประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมายหรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นกรรมการซึ่งยังคงจำนวนและ

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		คณะกรรมการโดยตำแหน่งด้วย นอกจากนี้ คณะกรรมการโดยตำแหน่ง ๖ ท่านนี้ เสนอแนะให้พิจารณาใหม่ให้รอบคอบ โดยทุกส่วนราชการที่เกี่ยวข้อง ควรเพิ่ม เข้ามาในคณะกรรมการโดยตำแหน่งตามมาตรานี้ด้วย - ขอเสนอแนะให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติควรใช้อำนาจผ่านทางคณะอนุกรรมการ โดยคณะอนุกรรมการจะเป็นผู้ทำงานในรายละเอียด และ คณะกรรมการทำหน้าที่เป็นผู้กำกับดูแล - การจัดทำนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ควรจัดให้มีการรับฟังความคิดเห็นด้วยรวมถึงควรเปิดเผยและสร้างความเข้าใจในแผนดังกล่าวต่อสาธารณะ - องค์ประกอบของ กปช. ยังขาดผู้เกี่ยวข้องที่เป็นส่วนกลางน้ำของกระบวนการยุติธรรม จึงเสนอให้เพิ่มเติม (๑) อัยการสูงสุด (๒) เลขาธิการสำนักงานศาลยุติธรรม เข้าเป็นองค์ประกอบในคณะกรรมการระดับชาติด้วย - ไม่ปรากฏองค์ประกอบของ DSI และ ศูนย์ไซเบอร์ทางทหาร ก.กลาโหม - การกำหนดหน้าที่เรื่อง CERT ซึ่งจะ ทำงานประสานกันระหว่าง National CERT กับ Sector	ความเชี่ยวชาญในด้านต่างๆ ของกรรมการผู้ทรงคุณวุฒิไว้เช่นเดิมตามร่างฯ ที่ สคก.ตรวจพิจารณาฯ (ร่าง มาตรา ๕) โดย กปช. มีหน้าที่และอำนาจดังนี้ (๑) เสนอนโยบาย ส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้คณะรัฐมนตรีให้ความเห็นชอบ (๒) กำหนดนโยบายให้หน่วยงานรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) กำกับดูแลการจัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงานเพื่อเสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ (๔) แต่งตั้งและถอดถอนเลขาธิการ (๕) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ อำนาจหน้าที่และกรอบการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๖) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ (๗) เสนอแนะและ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		CERT นั้น ควรมีการกำหนดกลไก อำนาจหน้าที่ของทั้งสองฝ่ายไว้ในกฎหมายด้วย - ในการกำหนดนโยบายและแผนซึ่งร่างมาตรา ๙ (๓) และมาตรา ๓๘ กำหนดให้กปช. กำหนดแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่ง เป็นข้อกำหนดขั้นต่ำสำหรับหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีขอเสนอว่าอาจกำหนดเพิ่มเติมในเรื่องดังนี้ O ควรกำหนดอุปกรณ์และเครื่องมือขั้นต่ำที่หน่วยงานควรต้องมี เพื่อให้สำนักงานสามารถนำไปกำหนดนโยบายและงบประมาณเพื่อรับการจัดสรรเงินได้ ทั้งนี้ ควรเพิ่มเติมเรื่องดังกล่าวไว้ในมาตรา ๙ (๒) และเพิ่มไว้ในคำนิยาม "ทรัพย์สินสารสนเทศ"ด้วย O ควรกำหนดมาตรฐานการทำงานและต้องมีการอบรมพนักงานเจ้าหน้าที่ของหน่วยงาน O ควรกำหนดให้หน่วยงานทำการ encrypt ข้อมูล - การตรวจสอบและการประเมินความเสี่ยงตามร่างฯ มาตรา ๓๘ มีการกำหนดมาตรฐานของผู้ตรวจสอบหรือไม่	ให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๘) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงประมวลแนวทางปฏิบัติ และกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (๙) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางนโยบายในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ (ร่าง มาตรา ๙) **(๔.๒) คณะกรรมการเฉพาะด้าน ได้แก่** **(๔.๒.๑) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกซ.)** โดยมีรองนายกรัฐมนตรีฝ่ายความมั่นคงเป็นประธานกรรมการ และกรรมการโดยตำแหน่ง ประกอบด้วย รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงกลาโหม ปลัดกระทรวงการคลัง ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคม ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินสี่คนซึ่ง กปช. แต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญประสบการณ์เป็นที่ประจักษ์และ

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- การรับฟังความคิดเห็นในการจัดทำนโยบายและแผน ตามมาตรา ๓๗ ถ้ารัฐมองว่าเป็นเรื่องกระทบหลายภาคส่วน ก็ควรเปิดให้รับฟังความคิดเห็นสาธารณะไม่น้อยกว่า ๓๐ วัน - ตามมาตรา ๙ (๒) "คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ" หรือ "กปช." มีหน้าที่และอำนาจ จัดทำ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงานเพื่อเสนอต่อคณะรัฐมนตรีสำหรับเป็น แผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคง ของสภาความมั่นคงแห่งชาติ นั้น เห็นว่า ต้องมีกรอบการทำงาน ก่อนที่จะมียุทธศาสตร์ แผนแม่บท แผนงาน ต้องหากรอบการทำงานด้าน Cyber เพื่อให้สอดคล้องกับยุทธศาสตร์ชาติแล้วจึงตรากฎหมายรองรับสิ่งเหล่านี้ จะได้เป็นเรื่องเดียวกัน	เป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ (ร่าง มาตรา ๑๑ (๑)) โดย กกซ. มีหน้าที่และอำนาจดังนี้ (๑) ติดตามการดำเนินการตามนโยบายและแผนในส่วนที่เกี่ยวข้อง (๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ (๓) กำกับดูแลการดำเนินงานเพื่อเป็นศูนย์กลางการประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (THAI CERT) และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ (๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน (๕) ประสานงานและให้ความร่วมมือในการตั้งหน่วยงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (CERT) ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ (๖) ร่วมกันประสานงานกับหน่วยงานอื่นๆ ในการกำหนดกรอบและความร่วมมือที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- การให้บริการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการใช้ผู้เชี่ยวชาญ ในมุมมองที่เป็นบริการสาธารณะ ประกอบกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องจัดเก็บรายได้ จะมีการคิดค่าใช้จ่ายอย่างไร - มาตรา ๑๔ บัญญัติว่า "ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหาร ราชการแผ่นดิน หรือรัฐวิสาหกิจตาม กฎหมายว่าด้วยวิธีการงบประมาณ หรือ กฎหมายอื่น" และมาตรา ๑๗ บัญญัติว่า "ในการปฏิบัติหน้าที่ตามมาตรา ๑๖ ให้สำนักงานมีหน้าที่และอำนาจดังต่อไปนี้ (๔) ถือหุ้นหรือเข้าเป็นหุ้นส่วนหรือเข้าร่วม ทุนกับนิติบุคคลอื่นในกิจการที่เกี่ยวกับ วัตถุประสงค์ของสำนักงานและมาตรา ๑๘ ทุนและทรัพย์สินในการดำเนินงานของสำนักงาน ประกอบด้วย ๕) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการหรือรายได้อันเกิดจากการ ดำเนินการตามหน้าที่และอำนาจของ สำนักงาน" จากบทบัญญัติข้างต้นเห็นว่าเป็นการขัดต่อหลักธรรมาภิบาล	กับหน่วยงานในประเทศและต่างประเทศ (๗) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกันรับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อ กปช. (๘) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อ กปช. พิจารณาสั่งการเมื่อมีภัยคุกคามระดับร้ายแรงขึ้น (ร่าง มาตรา ๑๒) **(๔.๒.๒) คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส)** โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ กรรมการโดยตำแหน่ง ประกอบด้วยปลัดกระทรวงการคลัง ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพาณิชย์ กรรมการคนหนึ่งในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติที่คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติแต่งตั้งผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินสี่คนซึ่ง กปช. แต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ (ร่าง มาตรา ๑๑ (๒)) โดย กกส. มีหน้าที่และอำนาจ ดังนี้ (๑) ติดตามการดำเนินการตามนโยบายและแผนในส่วนที่เกี่ยวข้อง (๒) ดำเนินการเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓) กำหนดหน้าที่ของหน่วยงานโครงสร้าง

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- การทำงานด้านการประสานงานเนื่องจากศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์ (Computer Emergency Response Team : CERT) ของประเทศไทยมีด้วยกันหลาย CERT เช่น National CERT ของ สพธอ. หรือ Sector based CERT ในแต่ละกลุ่มบริการ เช่น ธนาคารหรือสถาบันการเงินซึ่งมี CERT ของกลุ่มเอง จึงมีความกังวลว่าจะมีความทับซ้อนในการทำงานระหว่างกันหรือไม่	พื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของผู้ควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้ผู้ควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๔) ส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดมาตรฐานบังคับขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมใบรับรองมาตรฐานความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชน (๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานรัฐและหน่วยงานเอกชน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ **(๔.๒.๓) คณะกรรมการเฉพาะด้านอื่น** ซึ่ง กปช. แต่งตั้งโดยความเห็นชอบของคณะรัฐมนตรีเพื่อปฏิบัติหน้าที่ตามที่ กปช. กำหนด (ร่าง มาตรา ๑๑ (๓)) ทั้งนี้ ให้เลขาธิการเป็นกรรมการและเลขานุการโดยตำแหน่งในคณะกรรมการฯ ทุกคณะเหมือนเช่นร่างฯ ที่ สคก.ตรวจพิจารณาฯ สำหรับหลักการที่กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งรูปแบบสำนักงานและการกำหนดให้มีคณะกรรมการกำกับสำนักงานฯ นั้น ร่างฯ ที่กระทรวงฯ ปรับปรุงยังคงใช้หลักการตามร่างฯ ที่ สคก.ตรวจพิจารณาเช่นเดิม เพียงแต่มีการปรับปรุง

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
			องค์ประกอบที่สำคัญ คือ ให้เรียกคณะกรรมการดังกล่าวโดยย่อว่า “คกส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลางเลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคน และให้เลขาธิการเป็นกรรมการและเลขานุการของ คกส. และให้แต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ตามความจำเป็น สำหรับกรรมการผู้ทรงคุณวุฒิ ให้รัฐมนตรีแต่งตั้งจากบุคคล ซึ่งมีความรู้ความเชี่ยวชาญและความสามารถเป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการดำเนินงานของ คกส. ตามหลักเกณฑ์และวิธีการที่ กปช. กำหนด โดยกำหนดให้เป็นหน่วยงานของรัฐมีฐานะเป็นนิติบุคคล ที่ไม่เป็นส่วนราชการและรัฐวิสาหกิจ รับผิดชอบงานธุรการ งานวิชาการ และงานเลขานุการของ กปช. และคณะกรรมการเฉพาะด้าน และมีหน้าที่หลักในการจัดทำนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กปช. และสำนักงาน จัดทำแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เฝ้าระวังความเสี่ยงในการเกิด

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
			ภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ปฏิบัติการประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เสริมสร้างความรู้ความเข้าใจและความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชนเป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐและหน่วยงานเอกชนทั้งในประเทศและต่างประเทศศึกษาและวิจัยส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
			โดยกำหนดให้สำนักงาน กปช. เป็นองค์กรที่จัดตั้งขึ้นใหม่เป็นส่วนราชการลักษณะพิเศษเพื่อให้เกิดความคล่องตัวในการบริหารงาน และสามารถกำหนดค่าตอบแทนที่ดึงดูดคนที่มีความรู้ความสามารถเข้ามาร่วมทำงาน โดยองค์กรนี้จะไม่ไปลงทุนและหารายได้ หรือให้บริการ หรือดำเนินการในภารกิจอื่นใดที่ไม่เกี่ยวข้องกับอำนาจหน้าที่ (ร่าง มาตรา ๑๙ มาตรา ๒๐ มาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๓)
๕.	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)	- กรณีที่มีข้อโต้แย้งเกี่ยวหน่วยงานที่จะถือเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ควรให้ กปช. เป็นผู้วินิจฉัยชี้ขาด - เรื่องการขอข้อมูลจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีข้อสังเกตเกี่ยวกับข้อยกเว้นตามความใน มาตรา ๔๖ วรรคสอง ว่าเรื่องสัญญา ส่วนมากจะมีเรื่องการรักษาความลับของ ลูกค้า ทรัพย์สินทางปัญญา และเรื่อง privacy ซึ่งการเขียนห้ามยกเอาหน้าที่ ตามกฎหมายหรือตามสัญญาขึ้นอ้างเพื่อ ไม่เปิดเผยข้อมูลเท่ากับว่ากฎหมายนี้ยกเว้นกฎหมายอื่นทั้งหมด - การขอข้อมูลโครงสร้างของระบบควรผ่านกระบวนการตรวจสอบโดยศาล และควรดำเนินการเฉพาะเท่าที่จำเป็นและตามสมควรแก่กรณี	- ร่างฯ ที่กระทรวงฯ ปรับปรุง จะกำหนดให้มี คณะกรรมการส่งเสริมด้านโครงสร้างพื้นฐานสำคัญทางเทคโนโลยีสารสนเทศแห่งชาติ (“กสส.”) เพื่อทำหน้าที่ดูแลเรื่องมาตรฐานขั้นต่ำของระบบไซเบอร์และส่งเสริมพัฒนา สร้างมาตรฐาน ยกระดับทักษะความรู้ และกำหนดหน้าที่ของ CII และ Regulator โดยเน้นให้ CII ในแต่ละ Sector กำกับและดูแลกันเอง โดยยังคงให้ กปช. มีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็น ๗ ด้าน ดังเช่นร่างฯ ที่ สคก. ตรวจพิจารณาฯ โดยมีหลักการกำกับดูแล CII ดังนี้ (๑) ไม่ขัดข้องกับการ regulate จากส่วนกลาง การกำหนด minimum requirement (๒) ดูแลแบบ sector-based regulator (๓) การให้ incentive ในขณะเดียวกัน ให้มี consultation เพื่อส่งเสริมภาคเอกชนด้วยมาตรการต่างๆ ที่เหมาะสม

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- การประเมินความเสี่ยงตามมาตรา ๔๘ เปิดโอกาสให้เลขาธิการฯ ใช้ดุลพินิจได้อย่าง กว้างขวาง เนื่องจากกำหนดว่า หากการประเมินความเสี่ยง "ไม่เป็นที่น่าพอใจ" เลขาธิการฯ อาจมีคำสั่งให้ดำเนินการใหม่ได้ จึงควรมีการกำหนดกรอบและหลักเกณฑ์ ที่มีความชัดเจน - การได้ไปซึ่งข้อมูลโครงสร้างการทำงาน ของระบบคอมพิวเตอร์นั้น ยังขาดบทกำกับหน้าที่และความรับผิดของพนักงานเจ้าหน้าที่และสำนักงานที่ได้ไปซึ่งข้อมูลดังกล่าว - จะทราบได้อย่างไรว่าเมื่อใดจึงจะถือว่าเป็นภัยคุกคามทางไซเบอร์อย่างร้ายแรงแม้ในร่างกฎหมายจะกำหนดลักษณะของคำว่า ร้ายแรง ไว้แต่ก็ยังขาดความชัดเจนพอที่จะทำให้เข้าใจได้ อันจะส่งผลต่อการดำเนินการตามภาระหน้าที่ที่กฎหมายกำหนด - การรายงานเหตุภัยคุกคาม ควรมีรูปแบบ และวิธีการที่ชัดเจน - จำเป็นต้องรายงานเหตุในทุกกรณีหรือไม่ เนื่องจากโดยปกติ การโจมตีทั่วไปๆ สามารถเกิดขึ้นได้ทุกวันและเกิด เป็นประจำ หากว่าการโจมตีเยอะมากและมีลักษณะเดียวกันทุกวันจะต้องรายงานอย่างไร	

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- นอกจากนี้ ปัจจุบันในบาง sector มี CERT แล้ว และมีประสิทธิภาพในการทำงานด้วย แต่ไม่มีการพูดถึงในกฎหมายนี้ แนวทาง ของรัฐมีแนวทางในการประสานงานกับ CERT และ Sector CERT อย่างไร เพราะเอกชนนั้นมีภาระต้องใช้งบประมาณในการเตรียมตัวรวมถึงการวางแผนการทำงาน - รัฐมีแนวทางในการส่งเสริมสนับสนุน Sector CERT อย่างไร - ในร่างมาตรา ๔๖ ในการขอข้อมูล เห็นว่า กองบัญชาการ กองทัพไทย ไม่อาจให้ข้อมูลได้ เนื่องจากเป็นข้อมูลด้านความปลอดภัย และความลับระดับชาติ ดังนั้น หากจะขอข้อมูลอะไรควรยกเว้น ข้อมูลของกระทรวงกลาโหม เนื่องจากกองทัพไทยได้ดำเนินการด้านนี้ มาแล้ว ๒ ปี จึงมีความเชี่ยวชาญมากกว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นหน่วยงานตั้งขึ้นใหม่ จึงเป็นไปได้ยากที่กองทัพไทยจะให้ข้อมูลแก่สำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จนกว่าจะมีการพิสูจน์ได้ว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีความเชี่ยวชาญมากกว่า (กระทรวงกลาโหม)	

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- ในร่างมาตรา ๕๔ กำหนดว่า ผู้ดูแลระบบผู้ใดฝ่าฝืนหรือไม่ ปฏิบัติตามมาตรา ๔๗ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบ กำหนดระยะเวลาที่พนักงานเจ้าหน้าที่ออกคำสั่งให้ปฏิบัติจนกว่าจะ ปฏิบัติให้ถูกต้อง เห็นว่า ไม่ควรมีบทลงโทษ ผู้ดูแลระบบเพราะจะทำให้ไม่มีใครอยากทำหน้าที่นี้ - ถ้าดูในยุทธศาสตร์ทั้ง ๔ ด้านแล้ว เน้นโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ เน้นการบังคับใช้กฎหมาย ซึ่งใกล้เคียงกับ คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มี ๔ ด้าน เช่นเดียวกัน ปัจจุบันสำนักงานตำรวจ แห่งชาติทราบดี มีหลายหน่วยงานที่เกี่ยวข้อง ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น ศูนย์ปราบปรามอาชญากรรม ด้านเทคโนโลยีสารสนเทศ - ภาคเอกชนกังวลใจในร่างมาตรา ๔๖ วรรคท้าย ที่กำหนดว่า หน่วยงานที่ได้รับหนังสือตามวรรคหนึ่งไม่อาจยกเอาหน้าที่ตาม กฎหมายอื่นหรือตามสัญญามาเป็นข้ออ้างเพื่อไม่เปิดเผยข้อมูล ทั้งนี้ มิให้ถือว่าการกระทำตามความในมาตรานี้โดยสุจริต	

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		เป็น การผิดกฎหมายหรือผิดสัญญา จึงขอเสนอให้ตัดออกร่างมาตรา ๔๖ วรรคท้าย ออก - ควรแยกประเภทการรักษาความมั่นคงปลอดภัยไซเบอร์ ในแต่ละด้าน เช่น ให้ทหารดูแลความมั่นคงปลอดภัยไซเบอร์เฉพาะด้านทหาร พลเรือนดูแลความมั่นคงปลอดภัยไซเบอร์เฉพาะด้านพลเรือน และเอกชนดูแลความมั่นคงปลอดภัยไซเบอร์เฉพาะด้านเอกชน น่าจะเหมาะสมกว่า - ผู้แทนสำนักงาน กลต. เห็นว่าการกำหนด กลุ่มภารกิจหรือการให้บริการที่เป็นโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ ในมาตรา ๔๓ (๓) ด้านการเงินการธนาคาร ถ้อยคำยังไม่ครอบคลุม ตลาดทุน และประกัน จึงเสนอให้ ใช้คำว่า "ภาคการเงิน" ซึ่งจะกว้างและ ครอบคลุมมากกว่า (Financial Sector ประกอบด้วย ๓ ส่วน การเงินและการ ธนาคาร ตลาดทุน ประกัน จึงกังวลว่าจะไม่ ครอบคลุม ตลาดทุน และประกัน) - มาตรา ๔๕ ที่กำหนดให้มีการแจ้งรายชื่อ “ผู้ดูแลระบบ” นั้น ยังขาดความชัดเจนว่า หมายถึงบุคลากรในระดับใดขององค์กร เพราะแม้จะกำหนดว่า ผู้ดูแลระบบอย่างน้อย ต้องเป็นบุคคลผู้ซึ่งรับผิดชอบในการ บริหารงาน แต่ในองค์กรขนาดใหญ่มีผู้บริหาร หลายระดับ จึงมีการเสนอให้	

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		มีช่องทางการ ติดต่อมากกว่า ๑ ช่องทาง โดยให้มีทั้งระดับบริหาร และ ระดับปฏิบัติการ - ตามมาตรา ๔๖ การขอข้อมูลการ ออกแบบหรือข้อมูลการทำงานของระบบ o การขอข้อมูลค่อนข้างกว้างและข้อมูลดังกล่าวเป็นเรื่องที่มีความอ่อนไหวอย่างมาก ซึ่งควรมีกระบวนการในการดูแลข้อมูล และกำหนดความรับผิดของพนักงานเจ้าหน้าที่ที่ได้รับข้อมูลนั้นไป o นอกจากนี้ข้อยกเว้นตามความในวรรคสองมีข้อสังเกตว่า เรื่องสัญญาส่วนมากจะมีเรื่องการรักษาความลับของลูกค้า ทรัพย์สินทางปัญญา และเรื่อง privacy ซึ่งการเขียนห้ามยกเอาหน้าที่ตามกฎหมายหรือตามสัญญาขึ้นอ้างเพื่อไม่เปิดเผยข้อมูลเท่ากับว่ากฎหมายนี้ยกเว้นกฎหมายอื่นทั้งหมด	
๖.	การรับมือภัยคุกคามทางไซเบอร์	- มาตรา ๕๗ ให้อำนาจเลขาธิการในการหยุดการใช้งานระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วน และในมาตรา ๕๘ ให้อำนาจเลขาธิการให้ทำการหรือสั่งให้พนักงานเจ้าหน้าที่ทำการยึดคอมพิวเตอร์หรืออุปกรณ์ใด ๆ ที่มีเหตุอันควรว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์แม้จะมีการจ่ายค่าชดเชย หากมี ค่าจำกัดสูงสุดก็มีความเสี่ยงที่ค่าชดเชยนั้นจะน้อยเกินไปสำหรับผลกระทบทางเศรษฐกิจของผู้ประกอบการ นอกจากนี้ ยังส่งผลเรื่อง	ร่างฯ ที่กระทรวงฯ ปรับปรุง มิได้เปลี่ยนแปลงหลักการในการรับมือภัยคุกคามทางไซเบอร์ โดยยังคงใช้หลักการไว้เช่นเดิมตามร่างฯ ที่ สคก.ตรวจพิจารณาฯ แต่ได้ปรับปรุงหลักเกณฑ์ในการใช้อำนาจในการรับมือกับภัยคุกคามทางไซเบอร์ของเลขาธิการและพนักงานเจ้าหน้าที่ซึ่งต้องอยู่ภายใต้การควบคุมของคณะกรรมการ กปช. และคณะกรรมการ กกช. โดยปรับปรุงถ้อยคำบางส่วนเพื่อให้มีความชัดเจนเพิ่มขึ้นและสอดรับกับบทนิยาม และการปรับเลขมาตราใหม่ ดังนี้

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		ความไม่เชื่อใจจากผู้ใช้และผู้ลงทุน ต่างประเทศ ในความเป็นส่วนตัว ดังนั้น จึงควรพิจารณาอย่างรอบคอบว่ามีอุปกรณ์หรือกระบวนการใดบ้างที่ควรเป็น "ที่พึ่งสุดท้าย" ในกรณีเร่งด่วนและสำคัญที่สุด และมีอุปกรณ์หรือกระบวนการใดบ้าง ที่ควรเป็นวิธีการแรก ๆ ที่ถูกใช้ที่จะไม่ก่อให้เกิดปัญหาความเสียหายของอุปกรณ์ และข้อมูล หรือความเสียหายต่อภาพลักษณ์ และเศรษฐกิจ - มีวิธีการใดที่จะทำให้มั่นใจว่าเลขาธิการ หรือพนักงานเจ้าหน้าที่ที่ได้รับอำนาจจาก มาตรา ๕๗ และ ๕๔ ไม่นำอำนาจนี้มาใช้ เพื่อค้นข้อมูลหรือบังคับการกระทำใดๆ โดยมิชอบ หรือเพื่อผลประโยชน์นอกเหนือจากการปกป้องสังคมและประเทศจากภัยคุกคามทางไซเบอร์ที่แท้จริงหรือไม่ - มีข้อเสนอให้แก้ไขเพิ่มเติมโดยขอให้เพิ่ม วรรคสาม (วรรคท้าย) ว่า "การดำเนินของ เลขาธิการตามวรรคหนึ่ง ต้องรายงานให้คณะกรรมการ กปช.ทราบโดยเร็ว" เพื่อให้คณะกรรมการ กปช. รับทราบถึงการใช้อำนาจของ เลขาธิการ และเป็นการตรวจสอบโดยคณะกรรมการ กปช. ถึงการใช้ดุลยพินิจของเลขาธิการฯ - ควรกำหนดลักษณะหรือรูปแบบของการกระทำความผิดที่เข้าข่ายต่อการกระทำความผิดหรือมีผล	**ส่วนที่ ๑ นโยบายและแผน** กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ และต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ กำหนดให้ กปช. จัดทำนโยบายส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามเป้าหมายและแนวทางที่กฎหมายกำหนด เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้จัดให้มีการรับฟังความคิดเห็นด้วย และกำหนดให้หน่วยงานที่เกี่ยวข้องจัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนดังกล่าว (ร่าง มาตรา ๔๐ มาตรา ๔๑ มาตรา ๔๒ มาตรา ๔๓) **ส่วนที่ ๒ การบริหารจัดการ** กำหนดให้หน่วยงานที่เกี่ยวข้องมีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน (ร่าง มาตรา ๔๔ มาตรา ๔๕ มาตรา ๔๖) **ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ** กำหนดความสำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		ต่อความมั่นคงของประเทศ เพื่อให้เจ้าหน้าที่ร้องขอต่อศาลเพื่อให้ได้หมายศาลก่อน แล้วจึงเข้าไปตรวจสอบคอมพิวเตอร์ของผู้สงสัยได้ - การปฏิบัติงานของพนักงานเจ้าหน้าที่ แม้จะกำหนดให้มีบัตรประจำตัวและต้องแสดงบัตรในการปฏิบัติหน้าที่ แต่จะทราบได้อย่างไรว่าเป็นพนักงานเจ้าหน้าที่ตาม กฎหมายจริง ควรกำหนดให้มีช่องทางในการตรวจสอบหรือยืนยันตัวบุคคลได้ - ในร่างมาตรา ๖๒ และมาตรา ๖๓ ให้อำนาจเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมากเกินไป ควรมีกลไกมาถ่วงดุลอำนาจของเลขาธิการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ - พนักงานเจ้าหน้าที่ ถือว่าเป็นพลเรือนหน่วยหนึ่ง แต่กลายเป็น Law enforcement หน่วยงานของรัฐคุมเอกชน เช่น ขอข้อมูลจาก ดีแทค หรือ เอไอเอส ถ้าดีแทค หรือ เอไอเอส ไม่ให้ข้อมูล รัฐจะมีบทลงโทษ จึงอยากสอบถามว่าพนักงานเจ้าหน้าที่จำกัดเฉพาะของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือไม่ เนื่องจากในกฎหมายฉบับอื่นเปิดกว้างให้แต่งตั้งพนักงานเจ้าหน้าที่ที่มีความชำนาญด้านคอมพิวเตอร์ และดูแลด้านความมั่นคงปลอดภัยด้าน Cyber ด้วย	กปช. มีอำนาจประกาศกำหนดให้หน่วยงานที่มีลักษณะดังต่อไปนี้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๑) ด้านความมั่นคงของรัฐ (๒) ด้านบริการภาครัฐที่สำคัญ (๓) ด้านการเงินการธนาคาร (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (๕) ด้านการขนส่งและโลจิสติกส์ (๖) ด้านพลังงานและสาธารณูปโภค (๗) ด้านสาธารณสุข (๘) ด้านอื่นตามที่ กปช.ประกาศกำหนดเพิ่มเติม รวมทั้งให้ กปช. มีอำนาจประกาศกำหนดลักษณะหน้าที่และความรับผิดชอบของหน่วยงานศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหมดหรือบางส่วนก็ได้ โดยในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าไม่ได้มาตรฐานให้ส่งเรื่องให้ กปช. หรือ กสส. พิจารณา ทั้งนี้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจ

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- การบริหารจัดการ ม.๓๙ หน่วยงานของรัฐมีหน้าที่ต้องทำตนให้เท่ากับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งในทางปฏิบัติหน่วยงานรัฐบางแห่งอาจมีการบริการที่ไม่จำเป็นต้องดูแลเข้มข้นในทำนองเดียวกันก็เป็นได้ แต่กลับปรากฏว่าเรื่องของการรับมือหน่วยงานรัฐกลับมีโทษเท่ากับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ - การกำหนด Point of Contact ตาม มาตรา ๔๐ ควรกำหนดจำนวนเจ้าหน้าที่ เพื่อให้องค์กรเกิดความตระหนัก - การคัดเลือกบุคลากรเข้ามาทำงานด้านนี้ มีกระบวนการอย่างไร นอกจากนี้ กระบวนการมีความเกี่ยวข้องกับข้อมูลความลับจะมีมาตรการดูแลบุคลากรอย่างไร คนที่เข้ามาแล้วมีสิทธิลาออกหรือไม่ หากลาออกแล้วจะกลายสภาพเป็นอย่างไร หากเอาข้อมูลไปเปิดเผยแล้วเสียหายจะดำเนินการอย่างไร จะมั่นใจได้อย่างไร ว่าชั้นความลับจะไม่สูญเสีย - ในร่างมาตรา ๑๗ (๖) กำหนดให้ สำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจเรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน	ประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง (ร่าง มาตรา ๔๗ มาตรา ๔๘ มาตรา ๔๙ มาตรา ๕๐ มาตรา ๕๑ มาตรา ๕๒ มาตรา ๕๓ มาตรา ๕๔ มาตรา ๕๕ มาตรา ๕๖) **ส่วนที่ ๔ การรับมือกับภัยคุกคามทางไซเบอร์** กำหนดให้ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุม หรือกำกับดูแลของตนโดยเร็ว ทั้งนี้ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานซึ่งทำหน้าที่เป็นศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์

47

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		นอกจากนี้ ร่างมาตรา ๑๘ ยังกำหนดว่า รายได้ยังไม่ต้องนำส่งต่อคลังเป็นรายได้แผ่นดิน เห็นว่าในเรื่องของความมั่นคงของชาติ ไม่ควรมีรายได้อาจต้องของบประมาณพิเศษหรือไม่ - การใช้อำนาจในการออกคำสั่ง หรือเพื่อการปฏิบัติการต่าง ๆ ตามมาตรา ๕๒, ๕๘ ควรมีกระบวนการกลั่นกรองความเหมาะสมและจำเป็น โดยควรให้ศาลเป็นผู้ตรวจสอบการใช้อำนาจ จึงควรขอหมายศาลก่อนการดำเนินการ ทั้งนี้เนื่องจากเป็นการใช้อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ จึงควรดำเนินการที่ “ศาลอาญา” - ตามร่างกฎหมายฉบับนี้พนักงาน เจ้าหน้าที่มีอำนาจในการขอและเข้าถึงข้อมูลซึ่งไม่ปรากฏว่ามีการกำหนดหน้าที่และความรับผิดของพนักงานเจ้าหน้าที่ในการดูแลข้อมูลที่ได้มาแต่อย่างใด - นอกจากนี้ หากเกิด data breach กับข้อมูลที่ได้มา ความรับผิดชอบจะตกกับใคร ซึ่งรับผิดตามประมวลกฎหมายอาญา อาจจะไม่เพียงพอ สำหรับกรณีความรับผิดของพนักงานเจ้าหน้าที่ เนื่องจากความเสียหายที่เกิดขึ้นอาจจะสูงมาก ยกตัวอย่าง เช่น พ.ร.บ. โรคติดต่อฯ หากเจ้าหน้าที่ขอข้อมูลโรคติดต่อได้ เมื่อได้มาแล้วรั่วไหล ก็เป็นความรับผิดชอบ ของพนักงานเจ้าหน้าที่	เพื่อสนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และแจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว (ร่าง มาตรา ๕๗ มาตรา ๕๘) นอกจากนี้ เพื่อให้เกิดความชัดเจนของระดับภัยคุกคามทางไซเบอร์ ร่างฯ ที่กระทรวงฯ ปรับปรุง จึงกำหนดหลักการให้การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ กปช. และหรือ กกช. จะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้ (ร่าง มาตรา ๕๙) (๑) ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง (๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้ (ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูล คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ข) เป็น

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- การแสดงตัวพนักงานเจ้าหน้าที่ จะรู้ได้อย่างไรว่าเป็นพนักงานเจ้าหน้าที่จริงแล้ว หากบุคคลดังกล่าวเข้าไปทำอะไรสักอย่างที่ก่อให้เกิดความเสียหาย จะทำอย่างไร จะมีกระบวนการตรวจสอบได้อย่างไรว่าเป็นพนักงานเจ้าหน้าที่จริง - การเรียกให้ส่งข้อมูล ควรมีการกำหนดมาตรการการจัดเก็บ ระยะเวลาในการจัดเก็บ กระบวนการทำลายข้อมูล มาตรการป้องกัน การรั่วไหล การรักษาความลับของข้อมูล และ เปิดโอกาสให้ชี้แจงในกรณีที่ไม่สามารถส่งข้อมูลให้ได้ - ในร่างมาตรา ๕๘ (๔) ให้อำนาจพนักงานเจ้าหน้าที่ ยึดคอมพิวเตอร์หรืออุปกรณ์ใด ๆ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ จึงต้องฝึกพนักงานเจ้าหน้าที่ให้ยิงปืนด้วย หากให้ตำรวจหรือทหารเข้าไปช่วยดำเนินการน่าจะเหมาะสมกว่า - ตามมาตรา ๑๔ "ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะ เป็นนิติบุคคลและไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ หรือกฎหมายอื่น" ในฐานะที่สำนักงานคณะกรรมการการรักษา	ภัยคุกคามที่ก่อให้เกิดความเสี่ยงภัยจนอาจทำให้คอมพิวเตอร์ ระบบคอมพิวเตอร์ที่ให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงของรัฐ การป้องกันประเทศ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน ถูกแทรกแซงอย่างมีนัยสำคัญหรือถูกระงับการทำงาน (ค) เป็นภัยคุกคามที่มีความรุนแรงที่ก่อหรืออาจก่อให้เกิดความเสียงภัยหรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่สำคัญหรือมีจำนวนมาก (๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้ (ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน (ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์จำนวนมากถูกทำลายในวงกว้างในระดับประเทศ (ค) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่ง

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		ความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นนิติบุคคล มีใช่ส่วนราชการ อำนาจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะมีความเพียงพอหรือไม่ และถ้าไม่ใช่หน่วยงานของรัฐจะบังคับใช้กฎหมายได้หรือไม่ ควรขึ้นกับสำนักนายกรัฐมนตรีจะมีสะดวกรวดเร็วกว่าหรือไม่ - อยากให้รัฐทำ Cloud เป็นหน่วยงานกลางเพื่อดูแลระบบกลางของ Cyber Security ของทุกหน่วยงาน - สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะขอบุคลากรมาจากไหน - กรณีที่กำหนดให้เป็นหน้าที่หน่วยงานต้องทำแผนปฏิบัติการ และดำเนินการป้องกัน รับมือ และ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งหากมีข้อติดขัดหรืออุปสรรคอาจร้องขอความช่วยเหลือไปยังสำนักงานได้นั้น หากปรากฏว่าหน่วยงานทำเต็มที่ตามความสามารถที่มีแล้วและร้องขอความช่วยเหลือไปยังสำนักงาน แต่ปรากฏว่าก็ยังโดนโจมตีหรือมีภัยคุกคามเกิดขึ้น เช่นนี้จะต้องรับผิดอย่างไร ควรจะต้องให้สำนักงานแชร์ความรับผิดด้วยหรือไม่ - เนื่องจากมีประเด็นเรื่องการรายงานให้แก่หลายหน่วยงาน เช่น กลุ่มธนาคาร โดยหน้าที่หลักต้อง	การปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง รายละเอียดของลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้ กปช. เป็นผู้ประกาศกำหนดทั้งนี้ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ (๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง (๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ (๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่ (๔) รักษาสถานะของข้อมูล

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		รายงานไปยัง ธปท. ซึ่งเป็นหน่วยงานกำกับดูแล และยังต้องรายงานไปยัง กปช. ตามร่างกฎหมายนี้ จึงควรกำหนดมาตรการที่ไม่ก่อให้เกิดภาระให้กับ หน่วยงานที่มีหน้าที่ต้องรายงาน และในการรายงานเหตุภัยคุกคามไซเบอร์ - เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจมาก แต่ยังขาดกระบวนการตรวจสอบการใช้อำนาจ ซึ่งอาจก่อให้เกิดการใช้ดุลพินิจไปในทางที่มิชอบได้ - การขอข้อมูลของพนักงานเจ้าหน้าที่ ซึ่งใช้กับกรณีที่คาดว่าจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์นั้น เสนอให้ตัดคำว่า “คาดว่าน่าจะเกิด” เนื่องจากเปิดช่องให้มีการใช้ดุลพินิจและอำนาจอย่างกว้างขวาง จึงมีการเสนอให้ใช้คำว่า “มีเหตุอันควรเชื่อได้ว่า” แทน เพื่อให้มีความชัดเจนมากขึ้น - ความละเอียดของข้อมูลที่จะต้องส่งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ต้องระบุรายละเอียดมากน้อยเพียงใด อีกทั้งในองค์กรหนึ่งจะมีโครงข่ายหลายส่วน มีทั้งโครงข่ายที่มีความเสี่ยงสูงและโครงข่ายที่ไม่มีความเสี่ยง โครงข่ายที่ไม่มีความเสี่ยง นั้นต้องส่งข้อมูลให้ด้วยหรือไม่	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์ (๕) เข้าถึงข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยให้ กปช. หรือ กกช. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง หรือผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรงในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว (ร่าง มาตรา ๖๔) ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ในเรื่อง (๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ (๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศ

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- ข้อมูลที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติร้องขอควรกำหนดให้ชัดเจนว่าเป็นข้อมูลอะไรบ้าง เพราะบางกรณีข้อมูลที่ส่งให้เป็น ข้อมูลส่วนบุคคลของผู้ที่ได้รับความเสียหาย - การขอข้อมูลนั้น ยังขาดเรื่องการควบคุม การทำลาย การจัดเก็บข้อมูล	หรือโปรแกรมคอมพิวเตอร์ 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 (ร่าง มาตรา ๖๕) ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายนี้ (ร่าง มาตรา ๖๖) ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ กปช. มีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็น

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
			เพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้ทันทีโดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าวแล้วเสร็จให้ กปช. หรือ กกซ. แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว (ร่าง มาตรา ๖๗) สำหรับผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้(ร่าง.มาตรา ๖๘)
๗.	บทกำหนดโทษ	- ความรับผิดกรณีไม่แจ้งเหตุภัยคุกคามทาง ไซเบอร์ ○ จะรู้ได้อย่างไรว่าเป็นภัยคุกคามทางไซเบอร์ และอย่างไรจะถือว่าร้ายแรง ○ จะระบุได้อย่างไรว่าระดับไหนต้องแจ้ง ระดับไหนไม่ต้องแจ้ง ○ หากสามารถป้องกันเหตุภัยคุกคามทางไซเบอร์ได้ ยังมีหน้าที่ต้องรายงานอีกหรือไม่ ○ ควรกำหนดแบบรายงาน - การกำหนดบทลงโทษ ควรพิจารณาความพร้อมของหน่วยงานด้วย เนื่องจากเรื่องนี้ถือ เป็นเรื่องใหม่และต้องให้เวลาในการปรับตัวซึ่งแต่ละหน่วยงานมีความสามารถและความรู้ ความเข้าใจไม่เท่าเทียมกัน - การกำหนดผู้ต้องรับโทษ ในร่างกฎหมายประกอบด้วยคำว่า “ผู้ดูแลระบบ /หน่วยงาน / เจ้าของ / ผู้ครอบครอง / ผู้ใช้” ซึ่งในบางกรณียังขาดความชัดเจน ดังนั้นจึงควรกำหนดตัวบุคคลผู้ที่ ต้องรับผิดให้ชัดเจน	ร่างฯ ที่กระทรวงฯ ปรับปรุง ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับพร้อมทั้งได้ให้ความหมายเกี่ยวกับระดับภัยทั้งสามระดับไว้ แล้ว โดยให้ กปช. และหรือ กกซ. เป็นผู้พิจารณา ทั้งนี้ รายละเอียดของลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้ กปช. เป็นผู้ประกาศกำหนด (ร่าง มาตรา ๕๙) นอกจากนี้ ยังได้เพิ่มเติมกลไกในการควบคุมและตรวจสอบการใช้อำนาจโดยกำหนดให้มีบทกำหนดโทษห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามพระราชบัญญัติฉบับนี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการที่ได้มาตามพระราชบัญญัติฉบับนี้ให้แก่บุคคลใด และในกรณีกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่ได้มาตามพระราชบัญญัติฉบับนี้และผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่

(โปรดพลิก)

ลำดับ	ประเด็น	ความเห็น/ข้อเสนอแนะ	การดำเนินการ / คำชี้แจงเหตุผลรายประเด็น
		- ความรับผิดควรรับผิดเฉพาะในกรณีที่เป็นการกระทำโดยจงใจหรือประมาทเลินเล่อเท่านั้น หากได้ดำเนินการตามที่กฎหมายกำหนดแล้ว แต่ก็ยังไม่สามารถป้องกันได้ เช่นนี้ไม่ควรจะต้องรับโทษ - ม.๖๓ ถ้าไม่อำนวยความสะดวก หมายถึงอย่างไร หากว่าเป็นการขัดขวางเพราะมีหน้าที่ต้องทำตามกฎหมายอื่นจะทำอย่างไร	พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามพระราชบัญญัติฉบับนี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดต้องได้รับโทษทางอาญาตามที่กำหนดไว้ (ร่างมาตรา ๖๙ มาตรา ๗๐ มาตรา ๗๑)

การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก
ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง เป็นการพิจารณาผลกระทบของบทบัญญัติตามร่างพระราชบัญญัตินี้ ที่อาจส่งผลทั้งในเชิงบวกและเชิงลบ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้รวบรวมประเด็นและนำผลสรุป การรับฟังความคิดเห็นและข้อเสนอแนะจากผู้ที่เกี่ยวข้องทั้งภาครัฐ ภาคเอกชน ตลอดจนประชาชนทั่วไป มาเป็นข้อมูลประกอบการพิจารณาวิเคราะห์ผลกระทบที่อาจเกิดขึ้น เพื่อใช้เป็นข้อมูลประกอบการพิจารณร่างพระราชบัญญัติต่อไป

๑. ผู้ซึ่งอาจได้รับผลกระทบจากการบังคับใช้กฎหมาย

จากผลการวิเคราะห์พบว่า ผู้ซึ่งได้รับผลกระทบจากการบังคับใช้กฎหมาย ดังนี้

๑.๑ หน่วยงานภาครัฐ

๑.๒ ภาคเอกชน

๑.๓ ประชาชนทั่วไป

โดยผู้ที่จะได้รับผลกระทบจากร่างกฎหมายโดยตรง ได้แก่ หน่วยงานของรัฐ และหน่วยงานที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ทั้งที่เป็นหน่วยงานภาครัฐและภาคเอกชน ในการดำเนินมาตรการที่จำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ผลกระทบที่อาจได้รับจากร่างกฎหมาย

โดยการวิเคราะห์ผลกระทบแยกออกเป็น ๒ ส่วน คือ ผลกระทบเชิงบวกและผลกระทบเชิงลบ ดังนี้

<u>ส่วนที่ ๑</u> ผลกระทบเชิงบวก

(๑) ผลกระทบต่อสิทธิและเสรีภาพของประชาชน

เพื่อให้การใช้บังคับกฎหมายฉบับนี้มีความชัดเจนและลดข้อห่วงกังวลและข้อห่วงใยจากประชาชนและภาคประชาสังคม ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง จึงได้เพิ่มเติมหลักการเพื่อให้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) และ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกช.) กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิดความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับร้ายแรง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงภัยจนอาจทำให้คอมพิวเตอร์ ระบบคอมพิวเตอร์ที่ให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงของรัฐ

(โปรดพลิก)

การป้องกันประเทศ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน ถูกแทรกแซงอย่างมีนัยสำคัญหรือถูกระงับการทำงาน

(ค) เป็นภัยคุกคามที่มีความรุนแรงที่ก่อหรืออาจก่อให้เกิดความเสียงภัย หรือความเสียหายต่อบุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่สำคัญหรือมีจำนวนมาก

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

(ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์จำนวนมากถูกทำลายในวงกว้างในระดับประเทศ

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

นอกจากนี้ ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง ได้เพิ่มเติมกลไกในการควบคุมและตรวจสอบการใช้อำนาจโดยกำหนดให้มีบทกำหนดโทษห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามพระราชบัญญัติฉบับนี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการที่ได้มาตามพระราชบัญญัติฉบับนี้ให้แก่บุคคลใด และในกรณีผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่ได้มาตามพระราชบัญญัติฉบับนี้ ต้องได้รับโทษทางอาญาตามที่กำหนดไว้ สำหรับการรับมือกับภัยคุกคามทางไซเบอร์ของเลขาธิการและพนักงานเจ้าหน้าที่นั้น ต้องอยู่ภายใต้การควบคุมของคณะกรรมการ กปช. และ คณะกรรมการ กกช. ทั้งนี้ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กปช. หรือ กกช. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันการคุกคามทางไซเบอร์ในเรื่อง (๑) เข้าตรวจสอบสถานที่โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ (๒) เข้าถึงทรัพย์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ (๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใดๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบ

คอมพิวเตอร์นั้น (๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็น ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์ สำหรับการดำเนินการตาม (๓) และ (๔) ให้ กปช. หรือ กกช. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงาน เจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

สำหรับผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้

(๒) ผลกระทบด้านความมั่นคงของประเทศ

เพื่อให้การใช้บังคับกฎหมายฉบับนี้มีความเชื่อมโยงกับกฎหมายฉบับอื่นและอำนาจหน้าที่ของหน่วยงานด้านความมั่นคงของประเทศ ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมปรับปรุง จึงได้เพิ่มเติมหลักการในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายนี้

(๓) ผลกระทบด้านเศรษฐกิจและสังคม

(๓.๑) การยกระดับความสามารถในการแข่งขันของประเทศ

จากผลการสำรวจระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์โดยสหภาพ โทรคมนาคมระหว่างประเทศ (ITU) ที่สำรวจระดับความเอาจริงเอาจัง (Commitment) ด้านความมั่นคง ปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ ๕ ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity building) และด้านความร่วมมือ (Cooperation) ในปี พ.ศ. ๒๕๖๐ พบว่า Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ ๒๒ จาก ๑๙๔ ประเทศ นอกจากนี้ เมื่อเปรียบเทียบกับประเทศสมาชิก ในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ ๓ รองจากสิงคโปร์และมาเลเซีย ซึ่งผลการสำรวจดังกล่าวเป็น ส่วนหนึ่งที่แสดงให้เห็นถึงแนวโน้มความน่าเชื่อถือของประเทศในการประกอบธุรกิจ รวมถึงกลไกลดความเสี่ยง ในการทำธุรกรรมทางอิเล็กทรอนิกส์ การยกอันดับ GCI ของประเทศจึงเป็นหนึ่งในนโยบายของกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมที่ตั้งเป้าหมายในการยกอันดับของประเทศให้อยู่ใน ๒๐ อันดับแรก เพื่อเพิ่ม ระดับความน่าเชื่อถือของประเทศไทยอันจะส่งผลต่อการพิจารณาเรื่องการค้าการลงทุนด้วย ดังนั้น ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... จึงเป็นโครงสร้างพื้นฐานทางกฎหมาย สำคัญฉบับหนึ่งที่มีส่วนช่วยในการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตาม Global Cybersecurity Index (GCI) รวมทั้งมีส่วนช่วยในการยกระดับการดูแลความมั่นคงปลอดภัยไซเบอร์ ของประเทศในทุกมิติ โดยเฉพาะบริการที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructures) ของประเทศให้สามารถให้บริการแก่ ประชาชน ผู้ประกอบธุรกิจ และหน่วยงานของรัฐ ได้อย่างต่อเนื่อง

นอกจากนี้ ร่างกฎหมายดังกล่าวยังเป็นการส่งเสริมกระบวนการบริหารจัดการ ความเสี่ยงและกำหนดแผนรองรับทั้งด้านความพร้อมใช้งาน การฟื้นตัว การกู้คืนระบบ และความต่อเนื่อง ในการให้บริการของกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเป็นผลดีต่อการรักษาประสิทธิภาพ และความสามารถ

(โปรดพลิก)

ในการให้บริการสำคัญเมื่อเกิดเหตุขัดข้องจากภัยคุกคามในระบบนิเวศทางดิจิทัล เพื่อให้มี สภาพพร้อมใช้งานที่สามารถดำเนินการได้อย่างต่อเนื่องแม้เมื่อเกิดสถานการณ์ด้านภัยคุกคามไซเบอร์ อันจะช่วยสร้างความเชื่อมั่นให้แก่นักลงทุนในการตัดสินใจเข้ามาประกอบธุรกิจในประเทศไทย ซึ่งส่งผลสำคัญต่อการส่งเสริมให้ขีดความสามารถด้านการแข่งขันของประเทศดีขึ้น

(๓.๒) การเสริมสร้างประสิทธิภาพหรือนวัตกรรมในการปฏิบัติราชการ

ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์จำเป็นต้องมีการสร้าง กลไกสำหรับประสานความร่วมมือระหว่างภาครัฐและเอกชนที่สะท้อนการมีความรับผิดชอบต่อสังคม ในการรักษาความมั่นคงปลอดภัยไซเบอร์ของทุกภาคส่วน โดยจำต้องอาศัยรูปแบบการมีส่วนร่วมใน กระบวนการตัดสินใจ (Multi-stakeholders) การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ การรับมือสถานการณ์ ฉุกเฉินอย่างรอบด้าน ซึ่งการสร้างกลไกดังกล่าวจะส่งเสริมการทำงานและประสิทธิภาพของหน่วยงานของรัฐ ทำให้มีระบบการให้บริการแก่ประชาชนที่มีความมั่นคงปลอดภัย และสามารถช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นกับหน่วยงานของรัฐ

นอกจากนี้ หน่วยงานของรัฐสามารถลดค่าใช้จ่ายที่เป็นต้นทุนในการดำเนินการเพื่อรับมือภัยคุกคามทางไซเบอร์ได้ เนื่องจากเป็นการวางโครงสร้างในภาพรวม ทำให้ไม่เกิดการลงทุนที่ซ้ำซ้อน การมีหน่วยงานกลางทำหน้าที่ประสานงานทำให้การดำเนินงานมีประสิทธิภาพมากยิ่งขึ้น

(๓.๓) การยกระดับคุณภาพชีวิตของประชาชน

เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นกลไกสำคัญในยุคปัจจุบันเพื่อแก้ไขปัญหาที่มีผลกระทบทั้งประเทศ หรือต่อประชาชนจำนวนมาก และนำไปสู่การประสานความร่วมมือและหน้าที่ที่จำเป็นสำหรับหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่พร้อมปกป้อง รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันจะทำให้สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งมีหน่วยงานและกลไกในการให้ความช่วยเหลือ สนับสนุน ในการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น ส่งผลให้ประเทศ ไทยมีระบบนิเวศ หรือ Ecosystem ที่ช่วยสร้างความเชื่อมั่นในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลเพื่อดำเนินกิจกรรมต่าง ๆ อาทิ การให้บริการสำคัญภาครัฐในรูปแบบดิจิทัล การทำธุรกรรมผ่านช่องทางออนไลน์ต่าง ๆ ที่ต้องมีกลไกสำหรับการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง กลไกดังกล่าวจึงทำให้ประชาชนได้รับบริการจากระบบที่เป็นบริการอันเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) อย่างต่อเนื่อง นำไปสู่การยกระดับคุณภาพชีวิตของประชาชนที่สามารถได้รับบริการที่ดี มีคุณภาพ มีคุณภาพชีวิตที่ดีขึ้นจากระบบบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ดี

นอกจากนี้ การกำหนดมาตรการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นการสร้างความเข้มแข็งทั้งระบบ และยกระดับการดูแลความมั่นคงปลอดภัยไซเบอร์ในทุกมิติ เนื่องจากการดำเนินกิจกรรมต่าง ๆ อาศัยเทคโนโลยีเป็นเครื่องมือในการพัฒนาบริการและเพิ่มมูลค่าทางเศรษฐกิจ การให้บริการอันเป็นโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญซึ่งต้องให้บริการได้อย่างต่อเนื่อง จึงก่อให้เกิดประโยชน์แก่ภาคเอกชนที่สามารถประกอบกิจกรรมหรือดำเนินธุรกิจได้อย่างสะดวกและราบรื่น ซึ่งหากไม่มีมาตรการดูแลที่ดีเพียงพอ อาจกลายเป็นข้อจำกัดและอุปสรรคในการดำเนินธุรกิจของภาคเอกชน เนื่องจากขาดความน่าเชื่อถือ และภาคเอกชนอาจเสียโอกาสในการประกอบธุรกิจ ทั้งยังกระทบต่อระบบเศรษฐกิจในภาพรวมได้ อีกทั้งเมื่อประเทศไทยมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ จะทำให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) มีมาตรการในการดูแลความมั่นคงปลอดภัยไซเบอร์ของทรัพย์สินสารสนเทศของตน

ตาม มาตรฐานขั้นต่ำที่กฎหมายกำหนด ซึ่งจะมีส่วนช่วยให้การให้บริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้น หน่วยงานต่าง ๆ จะมีแนวปฏิบัติในการทำงานร่วมกัน ซึ่งจะทำให้การจัดการ เยียวยา แก้ปัญหา กู้คืน และฟื้นฟู สามารถดำเนินการได้อย่างทันท่วงที

(๔) ผลกระทบต่อประเทศโดยรวม

การที่ร่างพระราชบัญญัติดังกล่าวกำหนดโครงสร้างการทำงานเพื่อการบูรณาการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งครอบคลุมการทำงานทั้งภาครัฐและภาคเอกชนนั้น ส่งผลให้ประเทศไทยมีความพร้อม สามารถปกป้อง ป้องกัน และรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ทั้งในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ทั้งนี้ การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Governance) การเตรียมแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ยังก่อให้เกิดประโยชน์ในการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness) เพื่อรับมือและป้องกันภัยคุกคามไซเบอร์ได้อย่างทันท่วงที ถือเป็นกลไกสำคัญที่ให้สามารถแก้ไขสถานการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพและเป็นเอกภาพ สร้างความเชื่อมั่นในการดำเนินกิจกรรมต่าง ๆ ภายใต้สถานการณ์ภัยคุกคามไซเบอร์ และบริหารจัดการความเสี่ยงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ อันส่งผลต่อการดำเนินชีวิตประจำวันของ ประชาชน เสถียรภาพทางเศรษฐกิจ และความมั่นคงของชาติ

การขับเคลื่อนเรื่องความมั่นคงปลอดภัยไซเบอร์ยังจำเป็นต้องอาศัยการศึกษา วิจัยและ พัฒนาอย่างต่อเนื่อง เนื่องจากการวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเป้าหมายสำคัญของนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ต้องกำหนดให้มีขึ้นเพื่อหาแนวโน้มความเสี่ยงของภัยคุกคามไซเบอร์ และพัฒนาต่อยอดเทคโนโลยีในการป้องกันรับมือ และตอบโต้ภัยคุกคาม จะส่งผลให้ประเทศสามารถพึ่งพาตัวเองทางเทคโนโลยีได้อย่างยั่งยืน ไม่ยึดติดกับเทคโนโลยีต่างประเทศซึ่งอาจมีช่องโหว่ด้านความมั่นคงปลอดภัยทั้งแบบที่ตั้งใจและ ไม่ตั้งใจ

นอกจากนี้ การดำเนินงานตามร่างพระราชบัญญัตินี้จะช่วยลดงบประมาณแผ่นดินในระยะยาว และทำให้เกิดความคุ้มค่า เนื่องจากเป็นการดำเนินการแบบองค์รวมในการเสริมสร้างความเข้มแข็งในการดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างเป็นระบบ ทั้งมาตรการเชิงรุกที่ต้องมีการสร้างความแข็งแรงทั้งด้านนโยบาย องค์กร คน และองค์ความรู้ และมาตรการเชิงรับที่ต้องรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ซึ่งการดำเนินการดังกล่าวยังช่วยสร้างความเชื่อมั่นด้านการค้าและการลงทุนอันส่งผลดีต่อระบบเศรษฐกิจโดยรวม ส่วนการจำกัดสิทธิเสรีภาพของประชาชนนั้น ร่างพระราชบัญญัติฉบับนี้จำกัดเฉพาะการดำเนินการเพื่อปกป้อง และรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เพื่อประโยชน์ในการ รวบรวมข้อมูลและวิเคราะห์เพื่อหาแนวทางการรับมือได้อย่างมีประสิทธิภาพ

<u>ส่วนที่ ๒</u> ผลกระทบเชิงลบ

- ไม่มี -

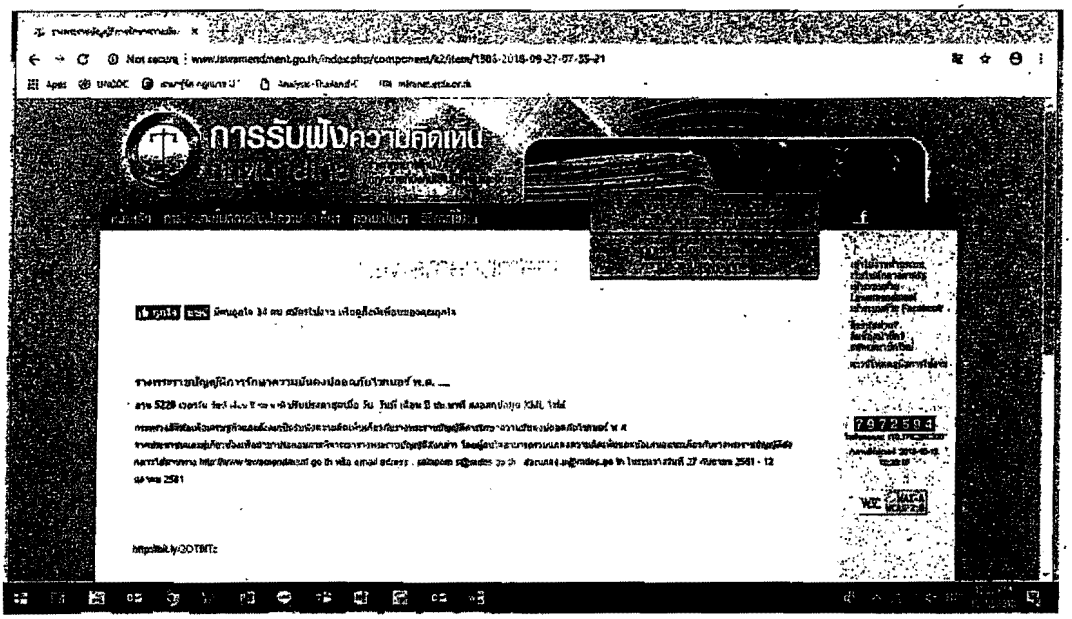
(โปรดพลิก)

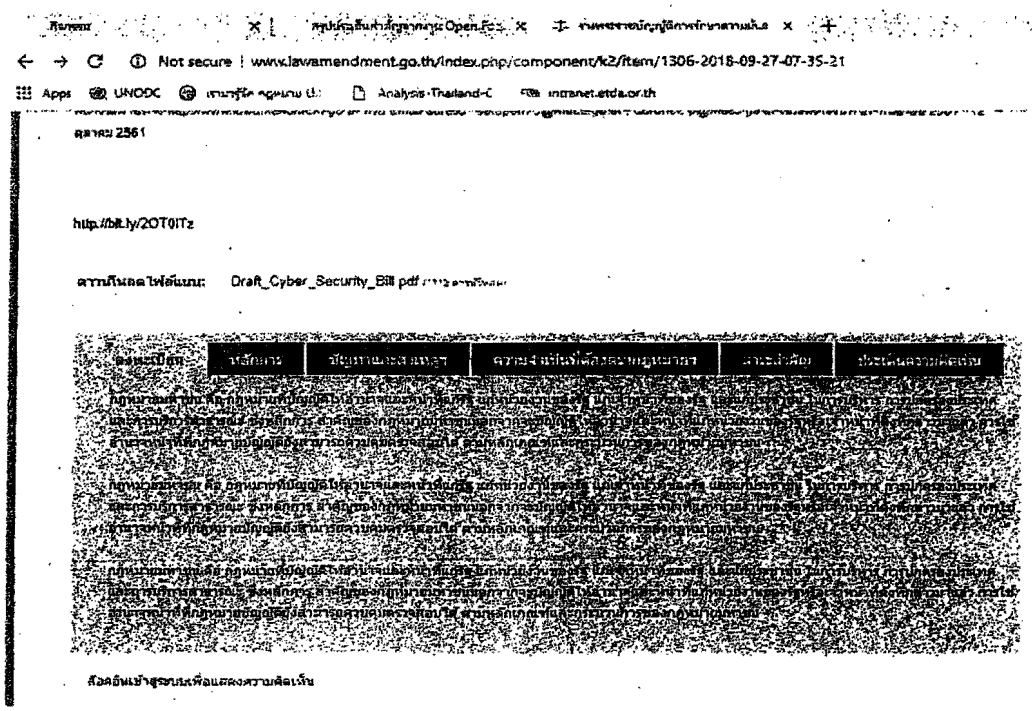
๓. ประโยชน์ที่ประชาชนและสังคมจะได้รับ

การที่สามารถปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ด้านภัยคุกคามทาง ไซเบอร์ได้อย่างทันท่วงที และสามารถแก้ไขสถานการณ์อันเกิดจากภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ เป็นเอกภาพ อย่างต่อเนื่อง จะส่งผลดีและสร้างความเชื่อมั่นในการขับเคลื่อนเศรษฐกิจดิจิทัลของประเทศไทยต่อประเทศอื่น และนำไปสู่การพัฒนาเศรษฐกิจสังคมได้อย่างยั่งยืนต่อไป โดยเฉพาะอย่างยิ่งจะทำให้ประชาชนได้รับบริการจากระบบที่เป็นบริการอันเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัย รวมทั้งมีหน่วยงานและกลไกในการให้ความช่วยเหลือ สนับสนุน ในการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... มีเจตนารมณ์เพื่อเป็นการป้องกัน รับมือ และลดความเสี่ยงภัยจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบ เรียบร้อยภายในประเทศ รวมทั้งเป็นการสร้างความเข้มแข็งให้ระบบการให้บริการผ่านออนไลน์ของหน่วยงานรัฐและเอกชนให้ดียิ่งขึ้น โดยมีหน่วยงานรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการให้บริการเป็นไป อย่างมีประสิทธิภาพและต่อเนื่อง

หลักฐานการรับฟังความคิดเห็นและการเปิดเผยผลการรับฟังความคิดเห็นและการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก (ร่าง) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

การรับฟังความคิดเห็นผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย
www.lawamendment.go.th
ระหว่างวันที่ ๒๗ กันยายน ถึงวันที่ ๑๒ ตุลาคม ๒๕๖๑





(โปรดพลิก)

การเผยแพร่สรุปผลการรับฟังความคิดเห็น
หลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist)
และการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก
(ร่าง) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

๑. เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

https://ictlawcenterdev.etda.or.th/de_laws

การดำเนินการตามมาตรา 77 ของ รธน.

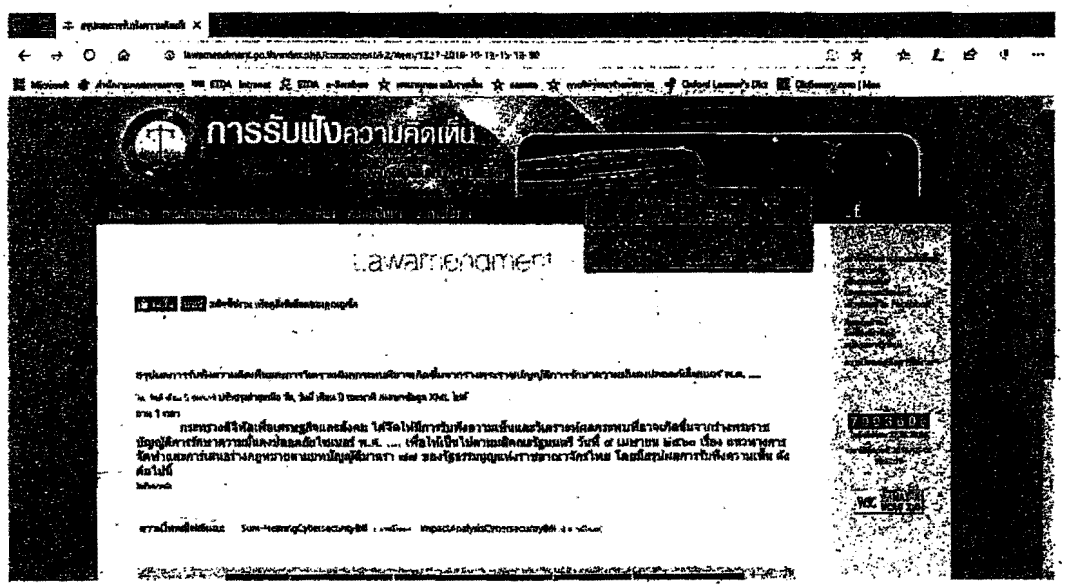
ร่าง พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. ....
- ร่าง พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. ....
- หลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist)
- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. ....
- สรุปผลการรับฟังความคิดเห็น

ร่าง พ.ร.บ. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....
- ร่าง พ.ร.บ. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....
- หลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist)
- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก ร่างพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....
- สรุปผลการรับฟังความคิดเห็น

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
- ร่าง พ.ร.บ. ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
- หลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist)
- สรุปผลการรับฟังความคิดเห็น
- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

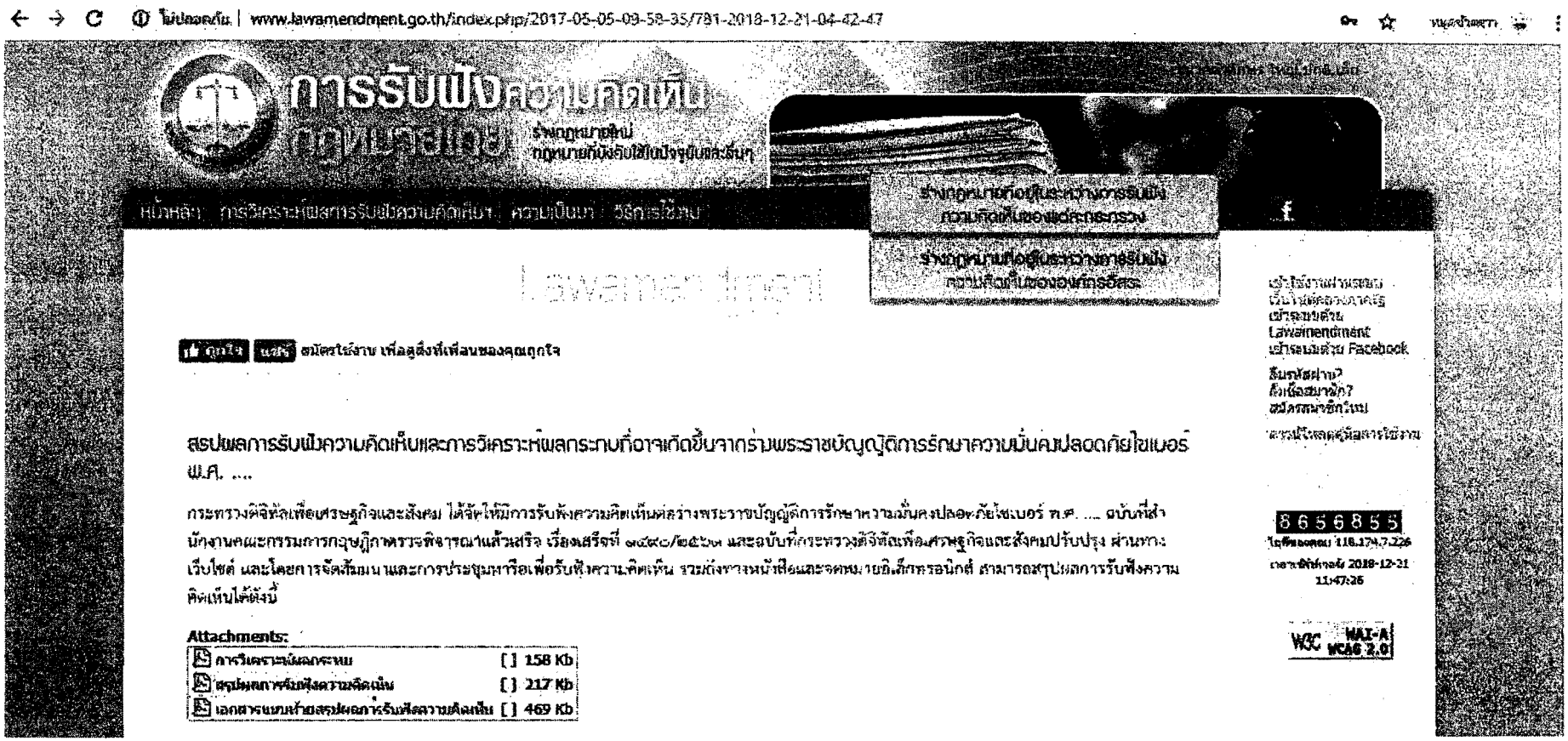
ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....
- ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....
- หลักเกณฑ์ในการตรวจสอบความจำเป็นในการตราพระราชบัญญัติ (Checklist)
- สรุปผลการรับฟังความคิดเห็น
- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

๒. เว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย (www.lawamendment.go.th)



ภาพแสดงการนำเอกสารสรุปผลการรับฟังความคิดเห็นและการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ขึ้นเผยแพร่ทางเว็บไซต์ www.lawamendment.go.th

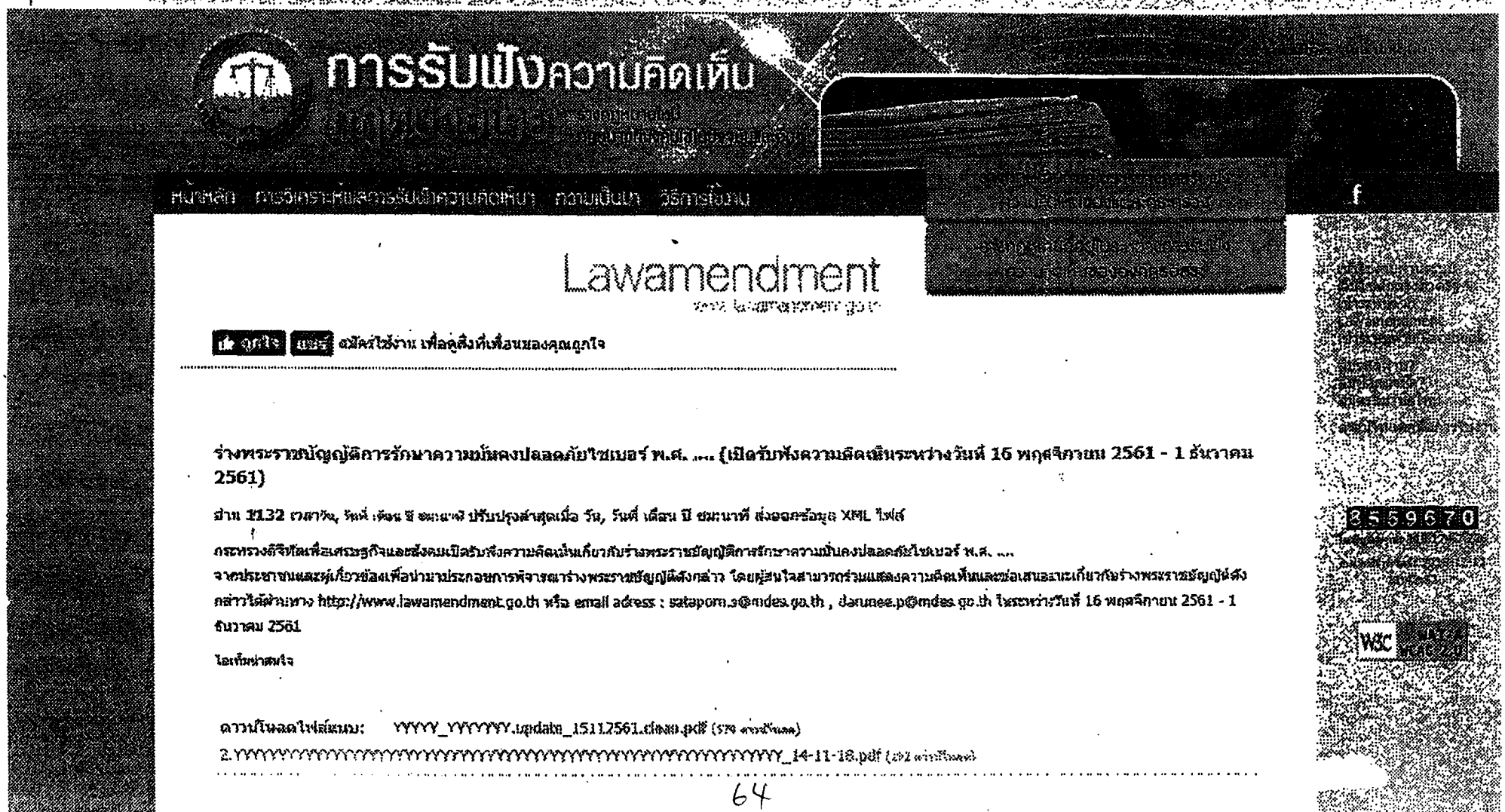


(โปรดพลิก)

การรับฟังความคิดเห็นผ่านทางเว็บไซต์การรับฟังความคิดเห็นกฎหมายไทย

www.lawamendment.go.th

ระหว่างวันที่ ๑๖ พฤศจิกายน ถึง ๑ ธันวาคม ๒๕๖๑



ไม่ปลอดภัย | www.lawamendment.go.th/index.php/component/k2/item/1356-2018-11-16-02-33-00

ธันวาคม 2561

ดาวน์โหลดไฟล์แนบ: YYYYY_YYYYYY?.update_15112561.clean.pdf

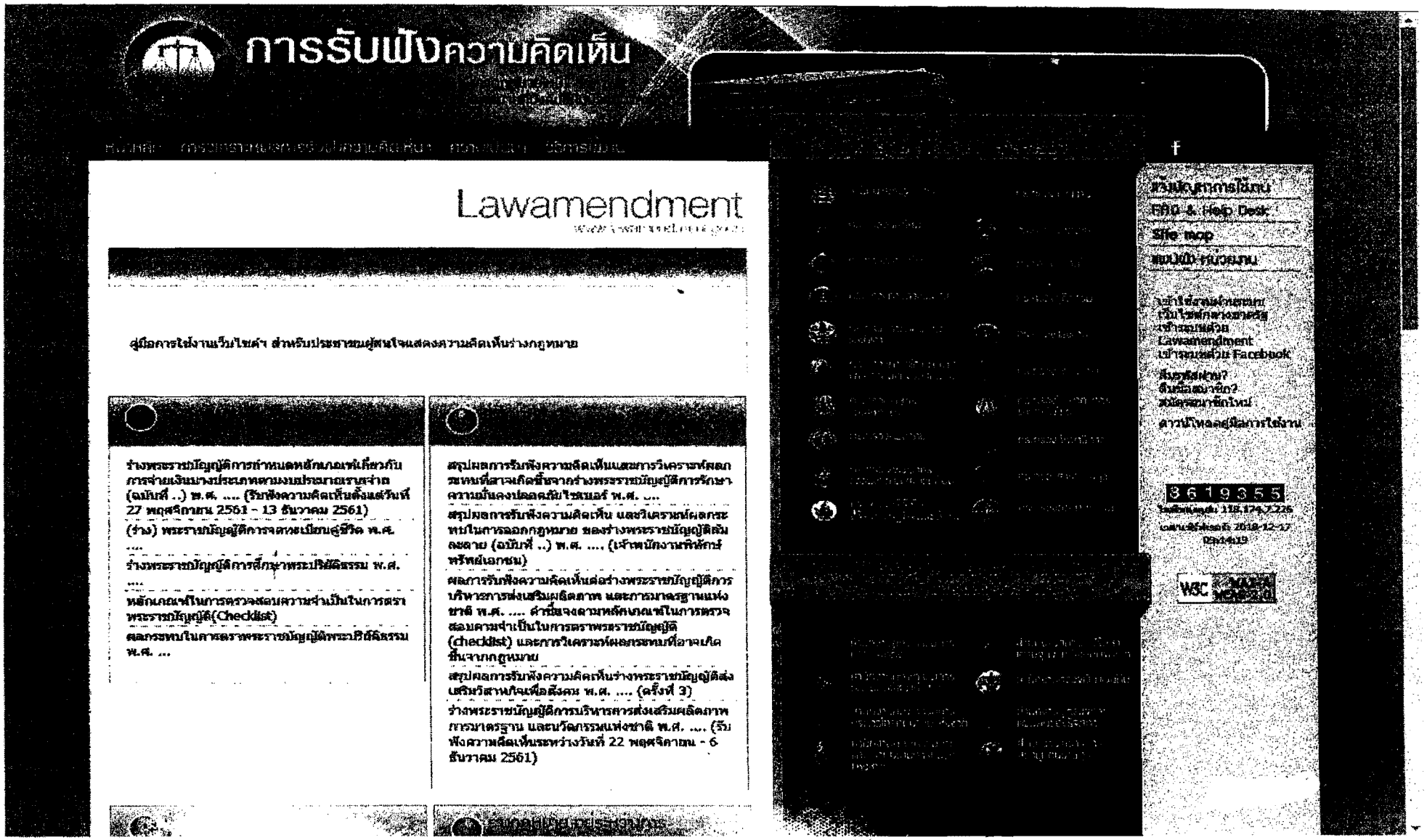
2.YYYYYYYYYYYYYYYY?YYYYYYYYYY?YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_14-11-18.pdf

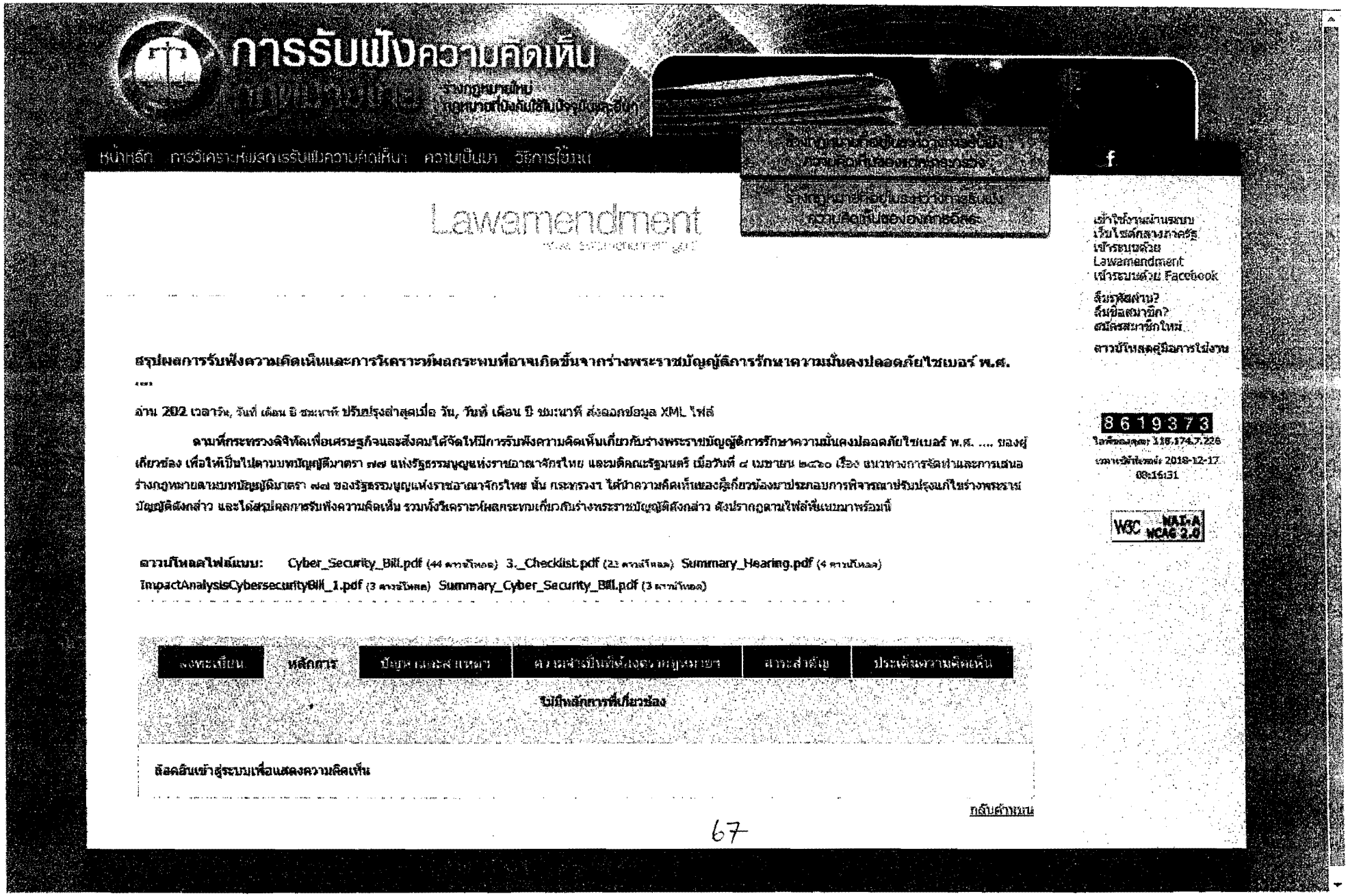
ล็อคอินเข้าสู่ระบบเพื่อแสดงความคิดเห็น

กลับด้านบน

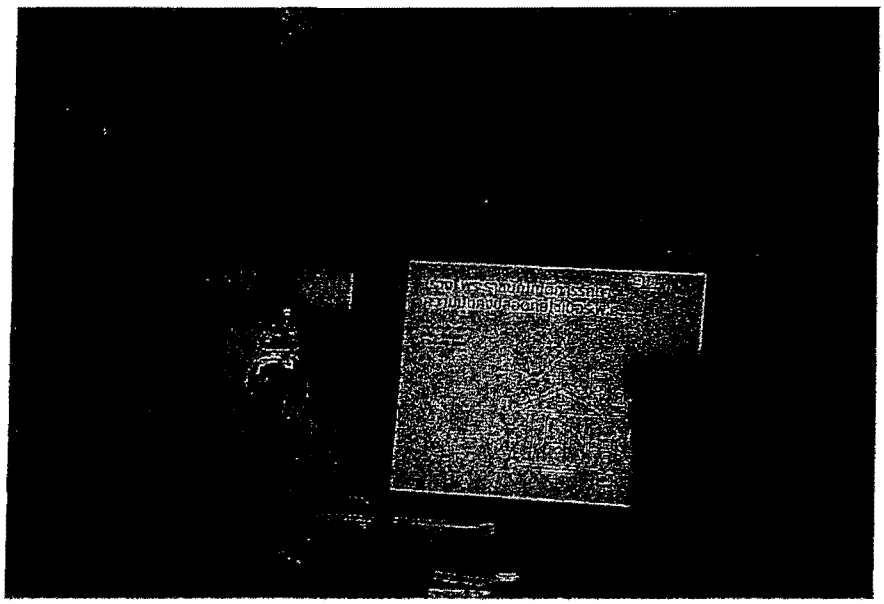
(โปรดพลิก)

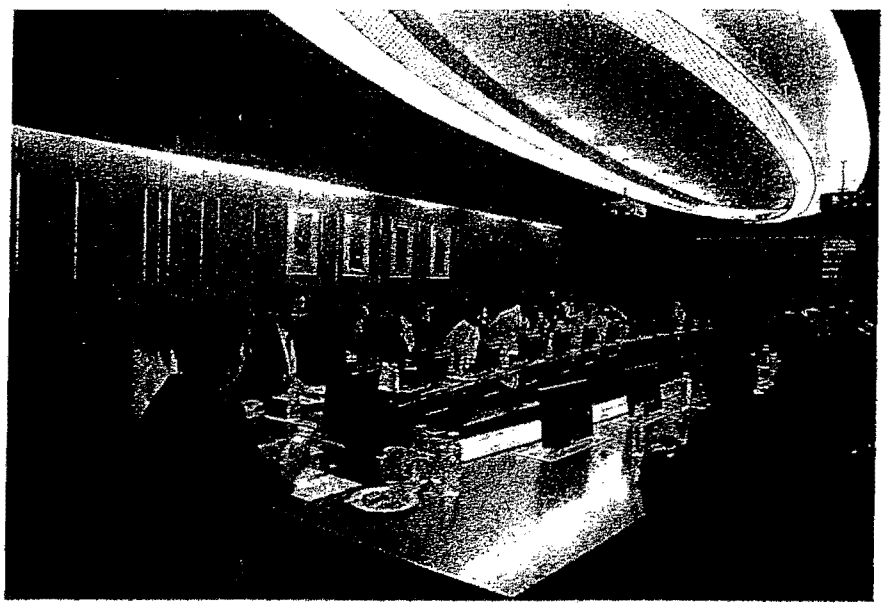
ภาพสรุปผลการรับฟังความคิดเห็นและการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก
ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....



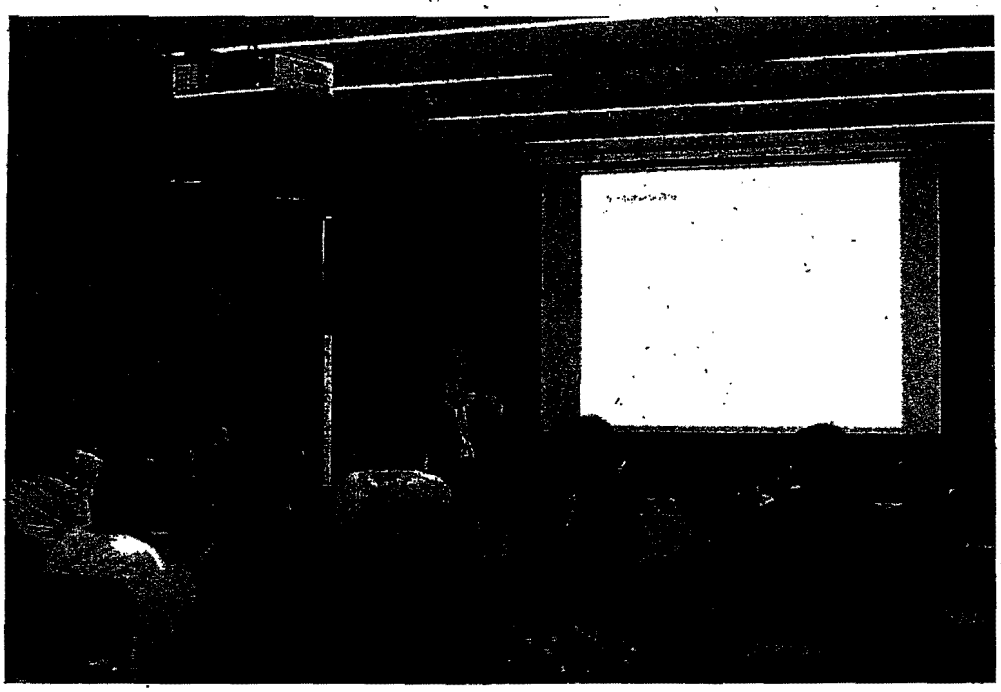

การรับฟังความคิดเห็น
หน้าหลัก
Lawamendment
เข้าใช้งานผ่านระบบ
เว็บไซต์กลางภาครัฐ
เข้าระบบด้วย
Lawamendment
เข้าระบบด้วย Facebook
ลืมรหัสผ่าน?
ลืมชื่อสมาชิก?
สมัครสมาชิกใหม่
ดาวน์โหลดคู่มือการใช้งาน
สรุปผลการรับฟังความคิดเห็นและการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
ดาวน์โหลดไฟล์แบบ:
Cyber_Security_Bill.pdf
3._Checklist.pdf
Summary_Hearing.pdf
ImpactAnalysisCybersecurityBill_1.pdf
Summary_Cyber_Security_Bill.pdf
ไม่มีหลักการที่เกี่ยวข้อง
ล็อคอินเข้าสู่ระบบเพื่อแสดงความคิดเห็น
กลับด้านบน
67

การประชุมสัมมนารับฟังความคิดเห็นร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ...
ที่ผ่านการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา
เมื่อวันที่ ๓ ตุลาคม ๒๕๖๑ เวลา ๑๔.๓๐ ถึง ๑๖.๓๐ น.
ณ ศูนย์ส่งเสริมพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)





การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
ที่ผ่านการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา
เมื่อวันที่ ๕ ตุลาคม ๒๕๕๘ เวลา ๑๔.๐๐ ถึง ๑๖.๐๐ น.
ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)



การประชุมสัมมนารับฟังความคิดเห็น (ร่าง) พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....
ที่ผ่านการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา
เมื่อวันที่ ๑๑ ตุลาคม ๒๕๕๘ เวลา ๑๐.๐๐ ถึง ๑๒.๓๐ น.
ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)