พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์

อยู่ระหว่างกระบวนการพิจารณาของ สนช.

พ.ร.บ. ดังกล่าว เป็นกลไกเฝ้าระวัง ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศสำคัญ (CII) และส่งผลเสียหายในระดับประเทศ

- ด้านความมั่นคง
- ด้านบริการภาครัฐที่สำคัญ
- ด้านการเงิน
- ด้านการขนส่งและโลจิสติกส์
- ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- ด้านพลังงานและสาธารณูปโภค
- ด้านสาธารณสุข

คค. เป็นหน่วยงานกำกับดูแล

ส่วนประกอบ ของ พ.ร.บ.

หมวด ๑ จัดตั้งคณะกรรมการ

- คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.)
- คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ (กกช.)
- คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส.)

หมวด ๒ จัดตั้งสำนักงาน

จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับดูแลสำนักงาน

หมวด ๓ กำหนดแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์

- กำหนดกรอบนโยบายและแผน
- แนวทางการบริหารจัดการ
- กำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศและแนวทางการประสานงาน
- แนวทางการรับมือภัยคุกคามทางไซเบอร์

หมวด ๔ กำหนดบทลงโทษ

- บทกำหนดโทษเจ้าหน้าที่และพนักงานสอบสวน
- บทกำหนดโทษหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- บทกำหนดโทษผู้กระทำความผิด ฝ่าฝืน ขัดขวาง และไม่ปฏิบัติตามคำสั่งคณะกรรมการ

จัดทำโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

สาระสำคัญ ของ พ.ร.บ. ที่เกี่ยวข้องกับ คค.

หมวด 1 คณะกรรมการ (มาตรา 5 – มาตรา 18)

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.)

นรม. เป็นประธาน รอง นรม. ฝ่ายความมั่นคง เป็นรองประธาน **รวค. และรัฐมนตรีว่าการกระทรวงที่เกี่ยวข้องเป็นกรรมการ**

- เสนอ ส่งเสริม สนับสนุน และวางแผนนโยบายการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์
- กำหนดนโยบายการบริหารจัดการให้หน่วยงานของรัฐ และหน่วยงาน CII
- จัดทำ และกำกับดูแลแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- ติดตามประเมินผลการปฏิบัติตามนโยบายและแผนปฏิบัติการ
- เสนอแนะ ให้ความเห็นเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ หรือ ครม.
- เสนอแนะ ครม. ในการปรับปรุงประมวลแนวทางปฏิบัติและกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

หมวด 2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (มาตรา 19 – มาตรา 39)

- จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และคณะกรรมการกำกับดูแลสำนักงาน
- รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กปช. และคณะกรรมการเฉพาะด้าน

คณะกรรมการเฉพาะด้าน

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ (กกช.)

รอง นรม. ฝ่ายความมั่นคง เป็นประธาน **ปกค. และปลัดกระทรวงที่เกี่ยวข้องเป็นกรรมการ**

- ติดตามการดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
- ดูแลและดำเนินการรับมือภัยคุกคามทางไซเบอร์
- กำกับดูแลการดำเนินงานเพื่อเป็นศูนย์กลางการประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (THAI CERT) และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์
- กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ประสานงานและให้ความร่วมมือในการจัดตั้งหน่วยงานเฝ้าระวังภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกประเทศ และร่วมประสานงานกับหน่วยงานอื่น ๆ ในการกำหนดกรอบความร่วมมือที่เกี่ยวข้อง
- กำหนดระดับภัยคุกคามทางไซเบอร์ พร้อมรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับ เสนอต่อ กปช.
- วิเคราะห์ ประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ระดับร้ายแรง เสนอต่อ กปช. พิจารณาสั่งการ

คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส.)

รมว.ดศ. เป็นประธาน ปลัดกระทรวงที่เกี่ยวข้อง เป็นกรรมการ

- ดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านการสร้างมาตรการในการปกป้อง CII ของประเทศ และการสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- กำหนดหน้าที่ของหน่วยงาน CII และหน่วยงานกำกับดูแล
- ส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- กำหนดมาตรการและแนวทางในการยกระดับความรู้ความสามารถของเจ้าหน้าที่ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

จัดทำโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม

สาระสำคัญ ของ พ.ร.บ. ที่เกี่ยวข้องกับ คค.

**** คค. เป็นหน่วยงานกำกับดูแล CII ด้านการขนส่งและโลจิสติกส์ ****

หมวด 3 การรักษาความมั่นคงปลอดภัยไซเบอร์ (มาตรา 40 - 68)

ส่วนที่ 1 นโยบายและแผน (มาตรา 40 – 43)

จัดให้มีการกำหนดแนวทางและเป้าหมายของนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดให้หน่วยงานของรัฐ หน่วยงาน CII และหน่วยงานกำกับดูแล ต้องจัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของแต่ละหน่วยงานให้สอดสอดคล้องกับนโยบายและแผนในระดับประเทศโดยเร็ว

ส่วนที่ 3 โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (มาตรา 47 – 56)

กำหนดให้ กปช. มีอำนาจประกาศลักษณะหน่วยงานที่มีภารกิจหรือให้บริการที่เกี่ยวข้องเป็นหน่วยงาน CII และประกาศกำหนดลักษณะ หน้าที่ และความรับผิดชอบของหน่วยงานศูนย์ประสานงานเพื่อความมั่นคงและความปลอดภัยทางไซเบอร์ (CSA) และหรือศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (CERT) สำหรับหน่วยงาน CII

หมวด 4 บทกำหนดโทษ (มาตรา 69 – 76)

พนักงานสอบสวนและเจ้าหน้าที่

เปิดเผยข้อมูลคอมพิวเตอร์ให้บุคคลอื่น (มาตรา 69) - จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ

เปิดเผยข้อมูลคอมพิวเตอร์โดยประมาท (มาตรา 70) - จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ

หน่วยงาน CII

ไม่รายงานภัยคุกคามโดยไม่มีเหตุอันควร (มาตรา 72) ปรับไม่เกิน 200,000 บาท

ส่วนที่ 2 การบริหารจัดการ (มาตรา 44 – 46)

กำหนดให้หน่วยงานของรัฐ หน่วยงาน CII หน่วยงานกำกับดูแล มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามแนวปฏิบัติด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานที่เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึง แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ส่วนที่ 4 การรับมือกับภัยคุกคามทางไซเบอร์ (มาตรา 57 – 68)

กำหนดให้ กปช. และ กกช. พิจารณากำหนดรายละเอียดลักษณะ และมาตรการรับมือภัยคุกคามทางไซเบอร์ทั้ง 3 ระดับ ประกอบด้วย (1) ระดับเฝ้าระวัง (2) ระดับร้ายแรง และ (3) ระดับวิกฤต

โดยกำหนดการดำเนินการสำคัญของหน่วยงาน CII ประกอบด้วย

- ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ ให้ดำเนินการตรวจสอบ ประเมินภัยคุกคาม และดำเนินการป้องกัน รับมือ และลดความเสี่ยงตามแนวปฏิบัติของหน่วยงาน และแจ้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานกำกับดูแลโดยด่วน (มาตรา 57)
- เมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุ ให้รวบรวม ข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ (มาตรา 58)

ผู้กระทำความผิด

- ล่วงรู้ข้อมูลคอมพิวเตอร์จากการสอบสวน (มาตรา 71) - จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ
- ไม่ปฏิบัติตามหนังสือเรียกของพนักงานสอบสวน หรือไม่ส่งข้อมูลคอมพิวเตอร์ (มาตรา 73) - ปรับไม่เกิน 100,000 บาท
- ฝ่าฝืนคำสั่ง กปช. หรือ กกช. (มาตรา 74) - ปรับไม่เกิน 300,000 บาท และปรับอีกไม่เกินวันละ 10,000 บาท จนกว่าจะปฏิบัติให้ถูกต้อง
- ขัดขวางไม่ปฏิบัติตามคำสั่ง หรือไม่อำนวยความสะดวกพนักงานสอบสวน (มาตรา 75) - จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 150,000 บาท หรือทั้งจำทั้งปรับ

จัดทำโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม